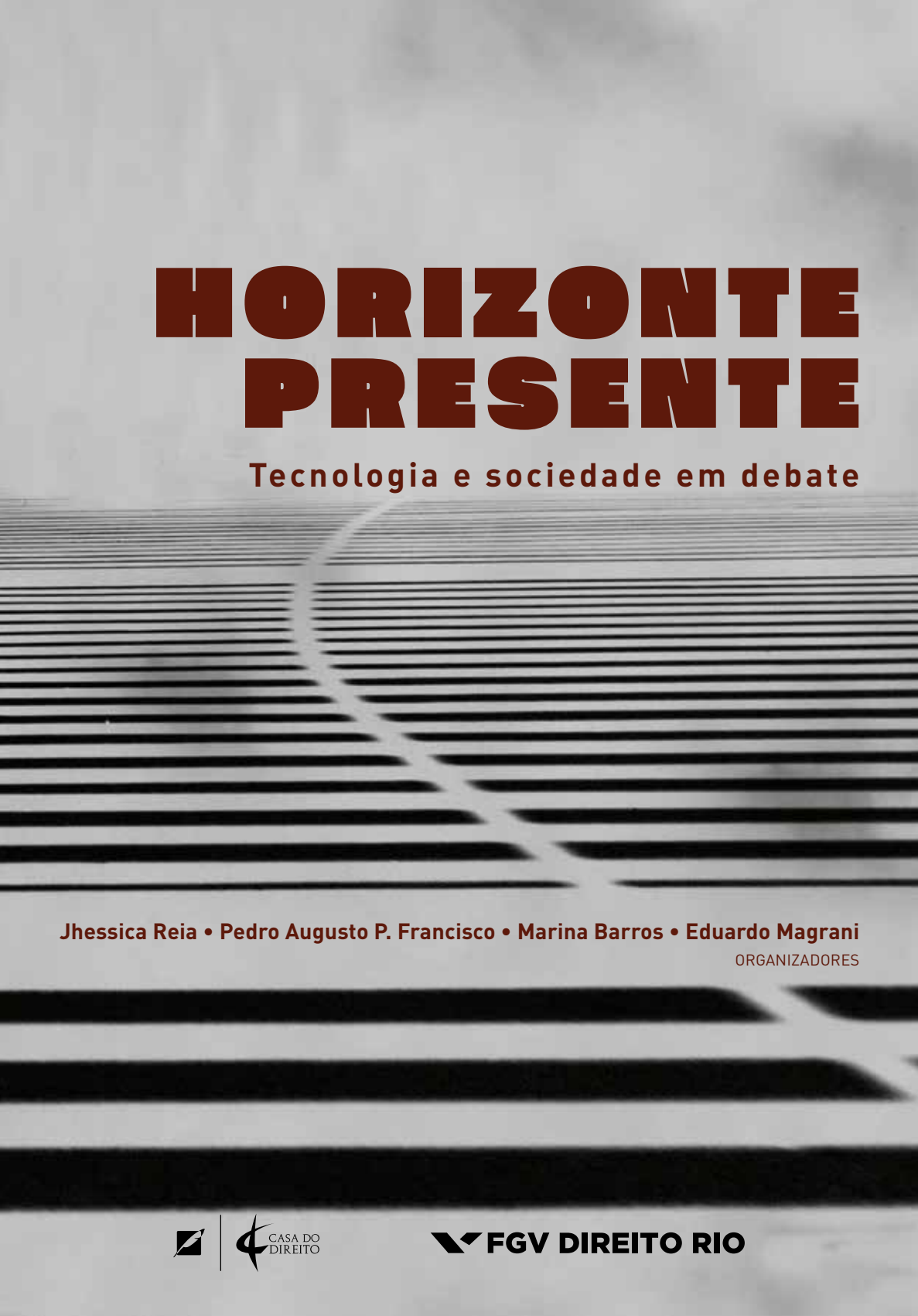


HORIZONTE PRESENTE

Tecnologia e sociedade em debate

Jhessica Reia • Pedro Augusto P. Francisco • Marina Barros • Eduardo Magrani
ORGANIZADORES

CASA DO DIREITO
FGV DIREITO RIO

HORIZONTE PRESENTE
TECNOLOGIA E SOCIEDADE EM DEBATE

ORGANIZADORES

JHESSICA REIA

PEDRO AUGUSTO P. FRANCISCO

MARINA BARROS

EDUARDO MAGRANI

CASA DO DIREITO

FGV DIREITO RIO

Diretor Editorial | Gustavo Abreu
Diretor Administrativo | Júnior Gaudereto
Diretor Financeiro | Cláudio Macedo
Logística | Vinícius Santiago
Designer Editorial | Luís Otávio Ferreira
Assistente Editorial | Giulia Staar e Laura Brand
Revisão | Lorena Camilo
Capa | Wellinton Lenzi
Diagramação | Isabela Brandão

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

H811 Horizonte presente: tecnologia e sociedade em debate / Alberto Silva ... [et al.] ; organizado por Jhessica Reia ... [et al.]. - Belo Horizonte : Casa do Direito ; FGV – Fundação Getúlio Vargas, 2019.
588 p. : il. ; 15,5cm x 22,5cm.

ISBN: 978-85-9530-081-1

1. Comunicação. 2. Tecnologia. 3. Sociedade. I. Silva, Alberto. II. Evsukoff, Alexandre G. III. Aprigio, André. IV. Andrade, Andressa Bizutti. V. Gutierrez, Andriei. VI. Freitas, Bruna Castanheira de. VII. Bioni, Bruno. VIII. Mulhollan, Caitlin Sampaio. IX. Therrien, Cristiano. X. Vicentin, Diego. XI. Magrani, Eduardo. XII. Peixoto, Eduardo. XIII. Carvalho, Gabriel Stumpf Duarte de. XIV. Knupp, Gabriela. XV. Matos, Helena Ferreira. XVI. Venturini, Jamila. XVII. Reia, Jhessica. XVIII. Chaves, Julio César. XIX. Rodrigues, Karina Furtado. XX. Hurel, Louise Marie. XXI. Belli, Luca. XXII. Abrahão, Luiz. XXIII. Sousa, Marcos de. XXIV. Barros, Marina. XXV. Campagnani, Mario. XXVI. Silva, Melissa Garcia Blagitz de Abreu e. XXVII. Silva, Moacyr Alvim Horta Barbosa da. XXVIII. Damazio, Natalia. XXIX. Unterstell, Natalie. XXX. Foditsch, Nathalia. XXXI. Patrício, Nathalia Sautchuk. XXXII. Oliveira, Neide M. C. Cardoso de. XXXIII. Cavalli, Olga. XXXIV. Cerdeira, Pablo. XXXV. Francisco, Pedro Augusto P. XXXVI. Ramos, Pedro Henrique Soares. XXXVII. Mizukami, Pedro Nicoletti. XXXVIII. Oliveira, Renan Medeiros de. XXXIX. Monteiro, Renato Leite. XXXX. Souza, Renato Rocha. XXXXI. Ribeiro, Ricky. XXXXII. Shanapinda, Stanley. XXXXIII. Wissenbac, Tomás. XXXXIV. Fortes, Vinicius Borges. XXXXV. Título.

CDD 302.2
2019-375 CDU 316.77

Elaborado por Vagner Rodolfo da Silva - CRB-8/9410

Índice para catálogo sistemático:
1. Comunicação 302.2
2. Comunicação 316.77

Belo Horizonte - MG
Rua Magnólia, 1086
Bairro Caiçara
CEP 30770-020
Fone 31 3327-5771
contato@editoraletramento.com.br
grupoeditorialletramento.com
casadodireito.com

Grupo Editorial LETRAMENTO
CASA DO DIREITO
Casa do Direito é o selo jurídico do Grupo Editorial Letramento

SUMÁRIO

parte ii — Privacidade e proteção de dados

parte iii — Tutela das comunicações e segurança na era digital

parte iv — Neutralidade de rede: acesso, autonomia e inovação

parte v — O futuro das coisas

AUTORES E ORGANIZADORES

ALBERTO SILVA Sociólogo, mestre em Gestão de Cidades pela London School of Economics, pós-graduado em Sociologia Urbana pela Universidade do Estado do Rio de Janeiro (UERJ) e Ciências Sociais no Trabalho em Comunidades pela Universidade Federal Rural do Rio de Janeiro (UFRRJ). É Vice-Presidente de Gestão Urbana Instituto Smart Cities Business Américas e Consultor em Estratégias para o desenvolvimento urbano sustentável para ONU Habitat e o Banco Mundial no Brasil e vários outros países. Foi presidente da Companhia de Desenvolvimento Urbano da Região do Porto do Rio de Janeiro (CDURP), empresa Municipal responsável pela Operação Urbana Porto Maravilha e o VLT Carioca, no Rio de Janeiro, entre novembro de 2012 a dezembro de 2016.

ALEXANDRE G. EVSUKOFF Concluiu a graduação em Engenharia Mecânica na Universidade Federal do Rio de Janeiro (UFRJ) em 1990, mestrado em Engenharia Mecânica na Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa em Engenharia (Coppe) da Universidade Federal do Rio de Janeiro (UFRJ) em 1992 e doutorado em Automação e Controle no Institut National Polytechnique de Grenoble, França, em 1998. Desde 2002 é professor do programa de Engenharia Civil da Coppe/UFRJ, com foco de pesquisa em desenvolvimento de técnicas de inteligência computacional para modelagem de sistemas complexos em aplicações de mineração de dados, de texto e da *web*. Nos últimos anos, vem trabalhando ativamente em projetos de PD em colaboração com a indústria, nas áreas de petróleo, energia, meio ambiente e telefonia. Recentemente, tem atuado também no tema de Cidades Inteligentes.

ANDRÉ APRIGIO Doutorando e pesquisador em Ciência Política e Relações Internacionais pela Universidade do Minho, Portugal, com período sanduíche no Instituto de Relações Internacionais (IRI) da Universidade de São Paulo (USP). Mestre e especialista em Relações Internacionais pela Universidade do Minho com intercâmbio no Technological Educational Institute of Crete/Grécia e MBA em Gestão Estratégica de Serviços pela ESPM. É membro consultor da Comissão Especial de Direito das telecomunicações da Conselho Federal da Ordem dos Advogados do Brasil (OAB) de São Paulo (SP).

ANDRESSA BIZUTTI ANDRADE Mestranda em Direito Comercial pela Universidade de São Paulo (USP), com graduação em Direito pela mesma universidade, onde também atua como monitora. Desenvolve desde 2014 trabalhos na área de Regulação da Arquitetura da Rede, com foco em temas como neutralidade da rede e regulação do setor de *video on demand*. É advogada associada do Baptista Luz Advogados na área de transações de tecnologia e propriedade intelectual, e professora convidada do Interactive Advertising Bureau Brasil em cursos voltados para publicidade online e regulação de novas tecnologias.

ANDRIEI GUTIERREZ Doutor em Ciência Política pela Universidade Federal de Campinas (Unicamp) e em Sociologia pela Université de Provence. Atua há mais de quinze anos no setor privado e acadêmico em diferentes áreas, como tecnologia (IBM), mineração (VALE) e bens de capital (ABIMAQ). É gerente de Relações Governamentais e Assuntos Regulatórios da IBM desde 2015. Foi pesquisador da Unicamp por cerca de dez anos em Ciência Política. É um dos idealizadores e coordenador do Movimento Brasil, País Digital, iniciativa multissetorial liderada pela Associação Brasileira das Empresas de Software (ABES) para discutir e divulgar os benefícios das inovações baseadas em dados para a sociedade brasileira.

BRUNA CASTANHEIRA DE FREITAS Doutoranda em Políticas Públicas, Estratégias e Desenvolvimento na Universidade Federal do Rio de Janeiro (UFRJ), onde desenvolve pesquisa a respeito da inserção de Gênero na Ciência e Tecnologia. É advogada e atuou como Pesquisadora no Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (CTS – FGV), em projetos sobre Propriedade Intelectual e Novas Tecnologias.

BRUNO BIONI Doutorando em Direito Comercial e Mestre com louvor em Direito Civil na Faculdade de Direito da Universidade de São Paulo (USP), foi *study visitor* do Departamento de Proteção de Dados Pessoais do Conselho da Europa e pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa e no Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação da USP. Atualmente é pesquisador do Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (LAVITS) e advogado do Núcleo de Informação e Coordenação do Ponto Br (NIC.br).

CAITLIN SAMPAIO MULHOLLAND Doutora (2006) e Mestre (2002) em Direito Civil, pela Universidade do Estado do Rio de Janeiro (UERJ). É professora de Direito Civil do Departamento de Direito da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), onde atualmente coordena a graduação em Direito. É professora do programa de pós-graduação em Direito Constitucional e Teoria do Estado da PUC-Rio, é também coordenadora do Instituto de Direito do Departamento de Direito da PUC-Rio. Atua na área do direito privado, através da metodologia do chamado direito civil constitucional, com ênfase nas relações jurídicas de natureza não patrimonial. É presidente da Comissão de Ensino Jurídico da OAB, Seccional Rio de Janeiro. Associada ao Instituto Brasileiro de Direito Civil (IBDCivil) e à Association Henri Capitant des Amis de la Culture Juridique Française. Pesquisadora do INCT Proprietas.

CRISTIANO THERRIEN Pesquisador do Centre de Recherche en Droit Public (CRDP). Doutorando em Direito na Université de Montréal e bolsista do programa Ciência sem Fronteiras da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Mestre em Direito e Informática pela Universidad de Madrid e bacharel em Direito pela Universidade Federal do Ceará. Advogado e consultor jurídico em tecnologia da informação. Foi coordenador geral de Tecnologia da Informação da Prefeitura Municipal de Fortaleza.

DIEGO VICENTIN Doutor e Mestre em Sociologia, Universidade Federal de Campinas (Unicamp). Professor colaborador do Laboratório de Estudos Avançados em Jornalismo (LABJOR/Unicamp). Seus interesses de pesquisa se concentram na relação entre Tecnologia e Política desde seu estatuto filosófico até a interface com políticas públicas. Redes comunitárias, propaganda computacional, regulação e apropriação do espectro radioelétrico e governança da Internet são alguns dos temas específicos. Foi pesquisador visitante no Center for Information Technology Policy (CITP) da Universidade de Princeton e pesquisador associado ao Instituto Tecnológico de Aeronáutica (ITA).

EDUARDO MAGRANI Coordenador do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). *Senior Fellow* na Universidade Humboldt de Berlim. Pesquisador da Law Schools Global League. Doutor e Mestre em Direito Constitucional pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Bacharel em Direito pela PUC-Rio, com intercâmbio na Universidade de Coimbra e Université Stendhal-Grenoble. Professor de Direito e Tecnologia e Propriedade Intelectual na FGV, IBMEC e PUC-Rio. Advogado atuante nos campos de Direitos Digitais, Direito Societário e Propriedade Intelectual. Autor de diversos livros e artigos na área de Tecnologia e Propriedade Intelectual, dentre eles os livros: *Democracia conectada* e *Digital Rights: Latin America and the Caribbean* e *A Internet das Coisas*.

EDUARDO PEIXOTO Executivo Chefe de Negócios do CESAR. Tem mais de 30 anos de experiência na área de Tecnologia da Informação e Comunicação, com atuação na Holanda, Suíça e Brasil, em empresas como Nederlandse PHILIPS Bedrijven B.V., ASCOM Business System AG e CESAR, respectivamente. Consultor de inovação de várias empresas e instituições, possui mestrado em Comunicação de Dados com distinção pela Technical University of Eindhoven-Holanda e diplomas de pós-MBA pela Kellog School of Management, Evanston-EUA e Digital Business Leadership pela Columbia Business School, Manhattan-EUA.

GABRIEL STUMPF DUARTE DE CARVALHO Doutorando em Sistemas de Transportes pelo programa MITPortugal no Instituto Superior Técnico de Lisboa e Mestre em Engenharia de Transportes pelo Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa em Engenharia (COPPE) da Universidade Federal do Rio de Janeiro (UFRJ). Atuou como consultor na área de mobilidade urbana na FGV Projetos e posteriormente como pesquisador no Centro de Estudos em Regulação e Infraestrutura (CERI) da Fundação Getulio Vargas (FGV).

GABRIELA KNUPP Advogada graduada pela Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ) e especialista em Direito de Empresas pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Especializada em nível de aperfeiçoamento em Competition Law in Telecoms pela Cullen International, em Bruxelas, e em nível de extensão em Direito Digital pela Escola Superior de Advocacia do Rio de Janeiro. É membro da Comissão de Direito e Tecnologia da Informação do Conselho da Ordem dos Advogados do Brasil (OAB) do Rio de Janeiro.

HELENA FERREIRA MATOS Foi pesquisadora no Centro de Tecnologia e Sociedade (CTS) da Fundação Getúlio Vargas (FGV). LLM candidate na Harvard Law School. Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ) e membro da Clínica de Direitos Fundamentais da Universidade do Estado do Rio de Janeiro (UERJ).

JAMILA VENTURINI Jornalista e pesquisadora com experiência em governança da Internet e direitos humanos. Mestranda na Faculdade Latinoamericana de Ciências Sociais (Flacso Argentina). É autora dos livros *Recursos Educacionais Abertos no Brasil: o campo, os recursos e sua apropriação em sala de aula* e *Terms of Service and Human Rights: an Analysis of Online Platform Contracts*. Foi Google Policy Fellow na organização internacional Access Now em 2016 e pesquisadora do Centro de Tecnologia e Sociedade da FGV Direito Rio (CTS/FGV) de 2014 a 2016. Foi membro da assessoria técnica às atividades do CGI.br.

JHESSICA REIA Pesquisadora e líder de projetos do Centro de Tecnologia e Sociedade (CTS) da Fundação Getulio Vargas (FGV). Pós-doutoranda no Programa de Pós-Graduação em Comunicação Social (PPGCOM) da Universidade do Estado do Rio de Janeiro (UERJ). Doutora e Mestre em Comunicação pelo Programa de Pós-Graduação em Comunicação e Cultura da Universidade Federal do Rio de Janeiro (UFRJ). Bacharel em Gestão de Políticas Públicas pela Universidade de São Paulo (USP). Foi Graduate Research Trainee na McGill University e pesquisadora visitante no McGill Institute for the Study of Canada entre 2015 e 2016. Pesquisadora colaboradora do Núcleo de Estudos e Projetos em Comunicação (NEPCOM) da Universidade Federal do Rio de Janeiro.

JULIO CÉSAR CHAVES Doutor em Inteligência Computacional na Universidade Federal do Rio de Janeiro (UFRJ), concluindo a tese sobre estimativa de matrizes de origem-destino a partir de dados de telefonia móvel. Administrador de banco de dados há mais de vinte anos. No momento iniciando uma frente de governança de infraestrutura computacional para pesquisas na Fundação Getulio Vargas (FGV). Líder do grupo vocal de canto gregoriano na Igreja de Nossa Senhora da Glória do Outeiro.

KARINA FURTADO RODRIGUES Doutora e Mestre em Administração Pública pela Escola Brasileira de Administração Pública e de Empresas (EBAPE) da Fundação Getulio Vargas (FGV). É pesquisadora no Programa de Transparência Pública da FGV e no grupo SOCIUS da Faculdade de Administração e Ciências Contábeis da Universidade Federal de Juiz de Fora (UFJF). Foi pesquisadora sobre transparência e anticorrupção no Centro de Tecnologia e Sociedade da FGV Direito Rio, além de pesquisadora-visitante na Universidade da Califórnia, em San Diego, e no Centro de Investigación y Docencia Económicas, na Cidade do México. Também atuou como consultora para a National Security Archive em projeto sobre o acesso civil a informações de defesa nacional.

LOUISE MARIE HUREL Mestre em Mídia e Comunicações com especialização em governança de dados com distinção pela London School of Economics and Political Science. Bacharel em Relações Internacionais pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Pesquisadora e coordenadora de projetos da área de segurança cibernética e liberdades digitais no Instituto Igarapé. Sua experiência inclui consultoria para a UNESCO, pesquisa no Núcleo de Análise de Conjuntura da Escola de Guerra Naval (NAC-EGN) e no Centro de Tecnologia e Sociedade da FGV.

LUCA BELLI PhD e professor e pesquisador sênior do Centro de Tecnologia e Sociedade, da Escola de Direito da Fundação Getúlio Vargas no Rio de Janeiro e pesquisador associado no Centro de Direito Público Comparado da Universidade Paris 2. Trabalhou como agente na Unidade sobre Governança da Internet do Conselho da Europa. É autor de mais de trinta publicações científicas que foram utilizadas, entre outros, pelo Conselho da Europa, pela Organização dos Estados Americanos e citadas por diversos jornais brasileiros e estrangeiros. Luca é mestre em direito pela Università degli Studi di Torino e Doutor em Direito Público pela Université Panthéon-Assas Paris 2.

LUIZ ABRAHÃO Pós-doutor, Doutor e Mestre em Filosofia pela Universidade Federal de Minas Gerais (UFMG). Professor do Centro Federal de Educação Tecnológica de Minas Gerais (CEFET/MG) credenciado no programa de pós-graduação em Educação Profissional e Tecnológica. Membro do GT Filosofia da Tecnologia e da Técnica da ANPOF. Pesquisador visitante no Institut Wiener Kreis (Áustria), Center for Philosophy of Science of University of Lisbon (Portugal) e Zentralen Einrichtung für Wissenschaftstheorie Wissenschaftsethik (Alemanha). Desenvolve pesquisas nas áreas de Filosofia da Ciência; Filosofia da Técnica e da Tecnologia; Filosofia da Engenharia e do Design de Artefatos.

MARCOS DE SOUSA Jornalista, Diretor Editorial e Coordenador de campanhas do portal Mobilize Brasil. Graduado em Comunicação Social pela Escola de Comunicações e Artes (ECA) da Universidade de São Paulo (USP) em 1985. Atuou nos jornais *Folha de S.Paulo*, *Jornal da Tarde* e nas revistas *Construção Pini*, *Téchne*, *Arquitetura e Urbanismo*, e *Projeto Design*, entre outras publicações e *sites* especializados. Editou livros nas áreas de artes, engenharia, arquitetura e urbanismo.

MARINA BARROS Administradora pela Fundação Getulio Vargas (FGV), Mestre em Comunicação pela Escola de Comunicação da Universidade Federal do Rio de Janeiro (UFRJ). Trabalhou como Líder de projeto do Centro de Tecnologia e Sociedade da FGV Direito Rio entre 2013 e 2018. Coordenou pesquisas sobre a implementação da Lei de Acesso à Informação no Brasil, transparência no Poder Judiciário e no Ministério Público e sobre a disponibilidade de dados de compras públicas no Brasil. Mais recentemente vem investigando o uso de dados públicos e privados para a formulação e avaliação de políticas públicas.

MARIO CAMPAGNANI Jornalista, com passagens pelas redações dos jornais *Folha Dirigida* e *Extra*. Atualmente trabalha como comunicador da organização de Direitos Humanos Justiça Global. Também milita como comunicador em redes e movimentos sociais, como o Comitê Popular da Copa e Olimpíadas do Rio de Janeiro.

MELISSA GARCIA BLAGITZ DE ABREU E SILVA Procuradora da República em São Paulo, membro do Grupo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo e do Grupo de Trabalho sobre Crimes Cibernéticos da 2ª. Câmara de Coordenação e Revisão do Ministério Público Federal. Mestre em Direito pela Universidade de Chicago.

MOACYR ALVIM HORTA BARBOSA DA SILVA Possui mestrado em Matemática pela Associação Instituto Nacional de Matemática Pura e Aplicada (1998) e doutorado em Matemática pela Associação Instituto Nacional de Matemática Pura e Aplicada (2004). Atualmente é professor da Escola de Matemática Aplicada da Fundação Getulio Vargas (FGV). Seus temas de interesse incluem redes complexas, teoria dos jogos e mobilidade urbana.

NATALIA DAMAZIO Advogada, Mestre em Teoria e Filosofia do Direito na Universidade do Estado do Rio de Janeiro (UERJ) com dissertação sobre o tema auto de resistência. Doutoranda em Direito na Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) pesquisando o tema sistema interamericano e políticas de gênero e raça nas decisões do sistema interamericano. É consultora em direito internacional no Instituto de Defensores de Direitos Humanos e suplente pela organização no Comitê Estadual de Prevenção e Combate à tortura. Co-coordenadora do Grupo de Estudos Permanente sobre Sistema Interamericano de Direitos Humanos do Núcleo de Direitos Humanos da PUC-Rio. Foi advogada e pesquisadora da organização não-governamental Justiça Global na área violência institucional e segurança pública.

NATALIE UNTERSTELL Mestre em Administração Pública pela Universidade de Harvard. Graduada em Administração de Empresas pela Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas (EAESP-FGV). É Secretária Adjunta do Fórum Brasileiro de Mudança do Clima, chefiado pela Presidência da República e coordenado pela sociedade civil organizada.

NATHALIA FODITSCH Advogada especialista em regulação e políticas de comunicação. Trabalhou no Brasil nos setores público e privado, e nos Estados Unidos em organismos internacionais e centros de pesquisa relacionados ao tema. Publicou variados artigos e relatórios e em 2016 lançou, como co-editora e co-autora, o livro *Banda Larga no Brasil: passado, presente e futuro* pela Editora Novo Século, que foi finalista do Premio Jabuti em 2017. Atualmente está baseada em Washington D.C.

NATHALIA SAUTCHUK PATRÍCIO Graduada e Mestra em Engenharia de Computação pela Escola Politécnica da Universidade de São Paulo (USP). É professora da disciplina "Governança da Internet" no Curso de Pós-Graduação em Assessoria de Comunicação e Mídias Digitais na Universidade Anhembi Morumbi e no curso de Pós-Graduação em Segurança da Informação no Centro Universitário SENAC. Também atua como Assessora Técnica do Comitê Gestor da Internet no Brasil (CGI.br). Faz parte do Núcleo de Coordenação da Rede de Pesquisa em Governança da Internet.

NEIDE M. C. CARDOSO DE OLIVEIRA Procuradora Regional da República na Procuradoria Regional da República da 2ª Região. Membro do Núcleo Criminal de Combate à Corrupção da PRR da 2ª Região e da Força Tarefa da Lava Jato na 2ª Instância. Coordenadora do Grupo de Apoio sobre Criminalidade Cibernética do MPF. Coordenadora do projeto Ministério Público pela Educação Digital nas Escolas. Graduada em Direito pela Universidade do Estado do Rio de Janeiro (UERJ) e especialista em Direitos Humanos pela Universidade Federal do Rio de Janeiro (UFRJ).

OLGA CAVALLI Co-fundadora e diretora acadêmica da South School on Internet Governance e Dominios Latinoamerica. Durante sete anos, foi membro do MAG, Advisory Group do Secretariado Geral da ONU para o Fórum de Governança da Internet. Desde 2006, como conselheira do Ministério das Relações Exteriores da Argentina, ela é a representante argentina no Governmental Advisor Committee da ICANN, onde é vice-presidente. Professora na Universidade de Buenos Aires, presidente do capítulo argentino da ISOC e membro do Board of Trustees da ISOC.

PABLO CERDEIRA Professor da Fundação Getulio Vargas (FGV) Direito Rio e advogado formado pela Faculdade de Direito do Largo São Francisco pela Universidade de São Paulo (USP). Foi um dos coordenadores do Centro de Tecnologia e Sociedade da Fundação Getulio Vargas (CTS/FGV). Foi também chefe de gabinete no Conselho Nacional de Justiça (CNJ), criador do Projeto Supremo em Números, da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (FGV), Subsecretário de Defesa do Consumidor do Rio de Janeiro e Chefe do Escritório de Dados da Prefeitura da Cidade do Rio de Janeiro (Big Data: PENSA – Sala de Ideias), da Prefeitura do Rio de Janeiro.

PEDRO AUGUSTO P. FRANCISCO Doutorando em Antropologia Cultural na Universidade Federal do Rio de Janeiro (UFRJ). É Mestre em Antropologia Cultural e possui graduação em Direito. Trabalhou como Líder de Projetos e Pesquisador no Centro de Tecnologia e Sociedade da Escola de Direito da FGV, no Rio de Janeiro, de 2009 a 2018. Sua área de atuação é a intersecção entre Antropologia da Ciência e Tecnologia, Antropologia Econômica e Antropologia Política. Atualmente, seus interesses de pesquisa são: segurança nacional, privacidade e vigilância, propriedade intelectual e pirataria.

PEDRO HENRIQUE SOARES RAMOS Graduado pela Universidade de São Paulo (USP), Mestre pela Fundação Getulio Vargas (FGV), pós-graduado pela University of Southern California e pelo IICS. Foi pesquisador associado do InternetLab e pesquisador visitante da Stanford Law School, onde atuou junto com a equipe de pesquisa do Center of Internet and Society, desenvolvendo trabalhos sobre neutralidade da rede e o impacto de estratégias de *zero-rating* em países em desenvolvimento, e que foram apresentados em fóruns como a Telecommunications Policy and Research Conference e o Internet Governance Forum. Professor convidado na USP, London School of Economics e Cornell Law School. Sócio do Baptista Luz Advogados e faz parte do conselho de diversas associações de fomento a empreendedorismo e inovação.

PEDRO NICOLETTI MIZUKAMI Diretor de Pesquisa do CNTR. Mestre em Direito Constitucional pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Doutorando no programa de Políticas Públicas, Estratégias e Desenvolvimento do Instituto de Economia da Universidade Federal do Rio de Janeiro (UFRJ).

RENAN MEDEIROS DE OLIVEIRA Mestrando em Direito Público e Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Pós-graduando em Direito Público pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). Pesquisador no Centro de Justiça e Sociedade da Fundação Getúlio Vargas (CJUS/FGV) e na Clínica de Direitos Fundamentais da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ) Clínica UERJ Direitos. Pesquisador Permanente do Laboratório de Regulação Econômica da UERJ – UERJ Reg.

RENATO LEITE MONTEIRO LL.M.em Global Business Law pela New York University – NYU. LL.M em Propriedade Intelectual, Direito e Tecnologia pela National University of Singapore – NUS. Professor e Fundador do Data Privacy Brasil. Sócio do Baptista Luz Advogados.Professor Convidado da Fundação Getúlio Vargas de São Paulo (FGV-SP) e do Insper.

RENATO ROCHA SOUZA Graduado em Engenharia Elétrica, Mestre em Engenharia de Produção, Doutor em Ciência da Informação e Pós-doutor em Ciência da Computação. É professor e pesquisador da Escola de Matemática Aplicada (EMAp) da Fundação Getúlio Vargas e professor colaborador da Escola de Ciência da Informação da Universidade Federal de Minas Gerais.

RICKY RIBEIRO (LUIZ HENRIQUE DA CRUZ RIBEIRO) Graduado em Administração Pública pela Fundação Getulio Vargas (FGV-EAESP), com mestrado em Sustentabilidade pela Universidade Politécnica da Catalunha (UPC) e MBA Executivo pela Universidade de Barcelona (UB). Fundador da OSCIP Associação Abaporu e do portal Mobilize Brasil – Mobilidade Urbana Sustentável. Membro da equipe de Sustentabilidade Corporativa da empresa EY (Ernst & Young). Coautor do livro Movido pela Mente. Diagnosticado em 2008 com uma doença neurológica degenerativa, a esclerose lateral amiotrófica (ELA) lhe tirou todos os movimentos, sem afetar sua mente. Hoje, trabalha e se comunica por meio de um leitor óptico que interpreta os movimentos da pupila.

STANLEY SHANAPINDA Stanley Shanapinda é doutorando no Centro Australiano de Cibersegurança (ACCS), da Universidade de New South Wales (UNSW), em Sydney. É Mestre em Políticas Públicas e Regulação de Tecnologias de Informação e Comunicação pela Universidade de Witwatersrand (Joanesburgo, África do Sul). Stanley é advogado atuante na Suprema Corte da Namíbia; o primeiro CEO da Autoridade Reguladora de Comunicações da Namíbia (CRAN) e Diretor Jurídico da Telecom Namibia Limited. Stanley foi Fellow de pesquisa no Centro de Tecnologia e Sociedade (CTS) da FGV Direito Rio em 2017.

TOMÁS WISSENBACH Mestre em Geografia Humana pela Universidade de São Paulo (USP) e doutorando em Administração Pública e Governo de São Paulo pela (FGV-SP), onde também é Pesquisador do Centro de Política e Economia do Setor Público Especialista em planejamento territorial e indicadores georreferenciados foi Diretor de Informações da Secretaria de Desenvolvimento Urbano em São Paulo, responsável pelo desenvolvimento do GeoSampa, sistema de informações geográficas da Prefeitura de São Paulo. Atuou em empresas de planejamento e urbanismo (Emplasa e SP Urbanismo) e na Fundação Seade.

VINICIUS BORGES FORTES Pós-doutorado em Direito pela Vrije Universiteit Brussel (VUB). Doutor em Direito pela Universidade Estácio de Sá do Rio de Janeiro (UNESA/RJ), com a linha de pesquisa "Direitos Fundamentais e Novos Direitos". Mestre em Direito pela Universidade de Caxias do Sul do Rio Grande do Sul (UCS/RS). Professor Permanente do Programa de Pós-Graduação Stricto Sensu – Mestrado em Direito da IMED – Faculdade Meridional. Pesquisador do Grupo de Pesquisa em Direito e Desenvolvimento. Pesquisador visitante na Universidad de Zaragoza (2014-2015). Professor visitante na VUB – no LSTS – Law, Science, Technology and Society Research Group no âmbito do projeto Brussels Privacy Hub (2016). Advogado com experiência nas áreas Direito e Novas Tecnologias, Direito do Trabalho e Direito Empresarial.

INTRODUÇÃO

Desde sua criação em 2003 o Centro de Tecnologia e Sociedade da Fundação Getulio Vargas (CTS-FGV) tem se destacado como polo de reflexão sobre as implicações jurídicas, sociais e culturais advindas das mudanças nas tecnologias da informação e da comunicação. Essas reflexões, por sua vez, sempre tiveram como objetivo impactar a formação de políticas públicas comprometidas com a democracia, os direitos fundamentais e a preservação do interesse público.

Como é de se esperar, o ritmo da reflexão acadêmica é diferente do ritmo das mudanças tecnológicas – e ainda mais destoante do ritmo das mudanças legislativas e regulatórias. Há uma diversidade muito grande de temas, abordagens e metodologias dentro do campo que viria a ser conhecido como Direito e Tecnologia – que pensamos ser, por sua vez, um recorte de perspectiva dos Estudos Sociais de Ciência e Tecnologia. Portanto, o desafio de acompanhar as mudanças tecnológicas e legislativas, e ao mesmo tempo em manter a qualidade da reflexão acadêmica, sempre impulsionou o CTS a garantir-se como referência no campo. Podemos destacar, por exemplo, os trabalhos que o centro realizou nas discussões sobre propriedade intelectual, governança da internet e democracia digital.

Por se tratar de um campo amplo e controverso, sujeito a mudanças constantes que trazem, muitas vezes, mais questões do que respostas, os pesquisadores do Centro decidiram realizar uma abordagem exploratória dos desafios de atuação e reflexão de determinados temas. Em 2015 inicia-se o projeto Ciclo de Debates, com apoio da Presidência da Fundação Getulio Vargas, que trazia especialistas de diversos setores para debater transformações tecnológicas, políticas públicas, desafios regulatórios, resultados de pesquisas, posicionamentos da sociedade civil, preocupações, soluções e oportunidades.

Foram, ao todo, cinco eventos do Ciclo de Debates que envolveram pessoas e instituições de formas variadas – como organizadores, palestrantes, moderadores e pesquisadores – e que trouxeram inúmeras oportunidades de diálogo, aprendizado e construção de redes. Os temas escolhidos para enquadrar cada um dos eventos se complementam e se relacionam, pois

trataram de mobilidade, conectividade, privacidade e segurança, cidades inteligentes e inovação. Ao olhar para todo material gerado nos encontros, a ideia do livro apareceu como uma oportunidade de expandir o projeto e seus múltiplos recortes, abordagens, controvérsias e proposições. Dessa forma, o presente livro pode levar o debate para todos aqueles que não estiveram presentes nos eventos, mas se interessam pelas discussões apresentadas. O livro também dá um passo adiante e congrega desdobramentos de questões levantadas, assim como oferece um panorama dos debates em tecnologia e sociedade desse momento.

Organizar um livro deste tamanho e com uma abrangência tão variada de temas e de opiniões não é uma tarefa fácil. Costurá-los em seções, criando uma narrativa, mostrou-se como um interessante desafio. O resultado é uma multiplicidade de vozes, experiências e reflexões, que se complementam ou se antagonizam, oferecendo aos leitores a possibilidade de explorar diversos caminhos. *As opiniões não necessariamente refletem a trajetória do CTS e dos organizadores*, mas tentou-se criar um debate plural, multifacetado e complexo – capaz de evidenciar, portanto, a intensidade da variedade de atores e posicionamentos nos estudos de tecnologia.

É evidente que os temas tratados são distintos e trazem questões diversas. No entanto, a unidade desta obra se encontra justamente na construção de um debate interdisciplinar e diversificado sobre o papel da tecnologia na sociedade contemporânea. Metodologias, atuações e vivências se encontram e se esbarram na tentativa de oferecer um enquadramento das discussões que parecem pertencentes ao imaginário de um futuro distante e, ao mesmo tempo, muito próximas de nosso cotidiano. A ideia de se olhar para um horizonte que se aproxima e se faz cada vez mais presente guiou a criação, composição e publicação desta obra, dividida por seções temáticas.

A primeira seção do livro, intitulada "Cidades, dados e direitos", apresenta discussões sobre alguns dos impactos causados pela adoção de tecnologias nas cidades contemporâneas, sob diversas perspectivas. Traz abordagens que olham para o direito à cidade, a reprodução de desigualdades e a análise de políticas públicas, privacidade e padrões de mobilidade, com textos que contribuem para o entendimento de temas que vem ganhando cada vez mais espaço nas agendas de pesquisa, na mídia e nas relações entre setor público e privado. O primeiro capítulo, de autoria de Marina Barros e Jamila Venturini e cujo título é *Os desafios do avanço das iniciativas de cidades inteligentes nos municípios brasileiros*, traz à tona uma reflexão sobre as contradições da ascensão das cidades inteligentes no Brasil a partir de dois estudos, um sobre legislação aplicável ao uso de dados pessoais pelo Estado e outro sobre o nível de transparência das políticas de gestão da

informação alguns municípios. O segundo capítulo , *Política pública de informações e abertura de dados: qual o limite para a privacidade de dados cadastrais nas "Cidades inteligentes"?*, escrito por Tomás Wissenbach, apresenta uma experiência concreta da construção da infraestrutura de dados espaciais na cidade de São Paulo na gestão de Fernando Haddad, ao mesmo tempo em que se propõe a discutir o papel das informações sobre a cidade no âmbito de sua gestão democrática, em um contexto cujos fatores estruturais levariam ao aumento das assimetrias informacionais. Já o terceiro capítulo, *Smart Cities além dos sensores: o uso de dados para aproximar governo e cidadãos*, escrito em coautoria por Pablo Cerdeira e Renan Medeiros de Oliveira, inicia um debate sobre a importância da adoção de tecnologias de cidades inteligentes que promovam o desenvolvimento das cidades, uma gestão estatal mais transparente e a aproximação entre governo e cidadãos – e traz exemplos da cidade do Rio de Janeiro. No quarto capítulo, *Padrões de mobilidade humana na Região Metropolitana do Rio de Janeiro*, os autores Julio C. Chaves, Gabriel S. D. Carvalho, Moacyr A. H. B Silva e Alexandre G. Evsukoff apresentam uma modelagem espaço-temporal da Região Metropolitana do Rio de Janeiro em unidades geográficas que permite a integração com dados de Call Detail Records (CDR) agregados com dados demográficos e de outras fontes, identificando os principais deslocamentos da população do estudo. No quinto capítulo, *Porto Maravilha, demolição da Perimetral e quebra de paradigmas urbanos: os desafios da gestão das mudanças*, Alberto Silva faz um relato sobre as inovações na condução do processo de mudanças de uma gestão urbana inteligente, a partir da análise da implantação do Porto Maravilha no Rio de Janeiro.

Ainda na primeira seção, o sexto capítulo, *Computação em nuvem e cidades inteligentes: das convicções tecnológicas às precauções jurídicas*, de autoria de Cristiano Therrien, analisa as funções que as nuvens computacionais vêm desempenhando para tornar as cidades mais "inteligentes" e observa as semelhanças e distinções de seus modelos de aplicação em governos municipais, ao mesmo tempo em que avalia os reflexos causados no direito. O sétimo capítulo, intitulado *O direito à cidade (inteligente): tecnologias, regulação e a Nova Agenda Urbana*, escrito por Jhessica Reia, discute os conceitos de cidade inteligente a partir da perspectiva do direito à cidade incorporado pela Nova Agenda Urbana, fazendo uma análise crítica das relações entre tecnologias, regulação e espaços urbanos. Os últimos capítulos da seção trazem importantes reflexões sobre o direito à cidade voltadas para a intersecção entre cidade e a caminhabilidade, o racismo e o aquecimento global. O oitavao capítulo, *Caminhabilidade nas cidades brasileiras: muito além das calçadas* de Ricky Ribeiro e Marcos de

Souza, contextualiza o conceito de caminhabilidade – *walkability* – na mobilidade urbana, enfatizando os desafios de caminhar pela cidade, ao mesmo tempo em que apresenta boas práticas. No nono capítulo, *Direito à cidade, capitalismo e racismo em protestos no Rio de Janeiro de 2013-2014*, Mario Campagnani e Natália Damazio apresentam alguns componentes específicos do processo de repressão e criminalização de protestos no Rio de Janeiro, discutindo também o uso e monitoramentos de redes sociais nesse contexto. Por fim, o décimo capítulo, escrito por Natalie Unterstell e intitulado *A cidade instantânea no futuro mais quente e incerto*, explora determinadas situações em que as cidades buscam expandir sua conectividade e sua inteligência, ao mesmo tempo em que ela mostra algumas das limitações e oportunidades desse processo, do ponto de vista da sustentabilidade e da resiliência.

A segunda seção, "Privacidade e proteção de dados", traz quatro reflexões acerca desses temas, dentro de um contexto que envolve as tecnologias de informação e comunicação. Nos últimos anos, privacidade e proteção de dados se transformaram nos principais tópicos de discussão dentro dos debates de Direito e Tecnologia. Assim, é evidente que os capítulos desta seção não pretendem esgotar todas as abordagens possíveis a respeito da privacidade e da proteção de dados. Ao contrário, a seção apresenta contribuições pontuais sobre aspectos distintos do debate mais amplo envolvendo a proteção de dados pessoais, demonstrando como essa discussão atinge questões diversas. No décimo primeiro capítulo, *Revisitando a #Privacidade na @Sociedade Digital*, Andriei Gutierrez propõe um novo olhar para a proteção de dados pessoais, tendo em vista as mudanças sociais e tecnológicas que transformaram a nossa sociedade em uma Sociedade Digital. O autor defende que, conforme os dados se tornam o motor de desenvolvimento econômico e social, é preciso pensar um modelo que garanta, ao mesmo tempo, o uso responsável desses dados e a sua proteção. No décimo segundo capítulo, *Proteção de dados pessoais como elemento de inovação e fomento à economia: o impacto econômico de uma lei geral de dados*, Bruno Bioni e Renato Leite Monteiro contestam a percepção de que a proteção de dados pessoais é incompatível com o desenvolvimento da economia. Os autores apresentam uma narrativa na qual a proteção é o fator que pode dar segurança jurídica e estabilidade para as relações econômicas no meio digital. O décimo terceiro capítulo, *Habilitando a localização de dados para cidades inteligentes: explorando os regimes de proteção e retenção de metadados no Brasil*, Stanley Shanapinda faz uma exploração dos regimes de retenção de metadados e proteção de dados pessoais no Brasil para, a partir daí, verificar como esses dados e metadados podem ser utilizados para se construir iniciativas de cidades

inteligentes. Por fim, a seção termina com o décimo quarto capítulo, *Quem mexeu no meu "porn"? Breves apontamentos acerca da relação entre o Direito, a tecnologia e a indústria do sexo*, de Nathalia Foditsch. Neste capítulo, a autora traz uma interessante discussão a respeito da relevância da proteção de dados pessoais no contexto da produção e consumo de conteúdo adulto na Internet. A ideia é ir além das urgentes discussões sobre pornografia de vingança, trazendo à baila questões importantes sobre privacidade na indústria pornográfica.

A terceira seção, "Tutela das comunicações e segurança na era digital", oferece ao leitor cinco capítulos que tratam de discussões referentes a regimes jurídicos de tutela das comunicações, sejam elas entre indivíduos ou envolvendo indivíduo e instituições – públicas ou privadas – em situações onde questões de segurança nacional e segurança pública estão em jogo. No décimo quinto capítulo, *Vigilância, privacidade e inteligência no Brasil: o marco legal e suas lacunas*, Pedro A. P. Francisco e Jamila Venturini apresentam um panorama do marco legal brasileiro sobre privacidade, confidencialidade das comunicações e atividades de inteligência, mostrando como como o país vem lidando com o desafio de equilibrar segurança pública e nacional com a proteção de direitos individuais. Em seguida, os autores apontam como as lacunas nesse marco legal são responsáveis por gerar problemas que afetam ao mesmo tempo a garantia de direitos e a manutenção da segurança. O décimo sexto capítulo, *Informações de Defesa e Segurança Nacional: entre a legitimidade do segredo e o direito à informação*, Karina Furtado Rodrigues discute o conflito que surge quando cidadãos exercem legitimamente seu direito à informação com vias de obter dados que podem ser sensíveis para a defesa e segurança nacional. A autora traz instrumentos para se pensar como estabelecer um equilíbrio segredo nacional e direito à informação. No décimo sétimo capítulo, *Securitização e governança da Segurança Cibernética no Brasil*, Louise Marie Hurel mostra o processo que levou o Brasil a considerar o setor cibernético como estratégico para a defesa e segurança nacional. Os últimos capítulos dessa seção tratam de aspectos específicos voltados à questões de segurança pública, a partir da perspectiva de duas representantes do Ministério Público. O décimo oitavo capítulo, *Atuação do Ministério Público Federal no combate aos crimes cibernéticos*, de Neide M. C. Cardoso de Oliveira, é um panorama da estrutura e das ações realizadas por este órgão na manutenção da segurança pública no ambiente digital. Por fim, o décimo nono capítulo, *Internet e jurisdição, acesso transfronteiriço a dados e o caso Irlanda Microsoft*, de Melissa Garcia Blagitz de Abreu e Silva, é a apresentação de um caso que ilustra os obstáculos para se investigar e julgar crimes em um mundo conectado pela Internet, mostrando as dificuldades da persecução penal

quando é preciso obter provas digitais em uma jurisdição distinta daquela de onde o crime foi praticado.

A penúltima seção do livro, intitulada "Neutralidade de rede: acesso, autonomia e inovação", apresenta uma discussão completa dos diversos aspectos sustentados pelo princípio da neutralidade de rede. Além do debate conceitual e principiológico ele também é analisado sob o ponto de vista regulatório, institucional, tecnológico e prático. Os dois capítulos iniciais introduzem o tema de forma complementar: enquanto o vigésimo capítulo, *A neutralidade de rede: norma fundamental para a proteção da expressão e do empreendedorismo na internet*, de Luca Belli, traz um panorama nacional e internacional acerca dos debates sobre o princípio da neutralidade – sustentando-o como fundamento para a proteção da expressão e do empreendedorismo na internet – o vigésimo primeiro capítulo, escrito por Diego Vicentin e intitulado *Convergência, conectividade comunitária e questão do espectro*, traça os riscos da convergência entre telecomunicações e computação em rede tratado na Agenda da ANATEL e exemplifica um deles como sendo a ameaça às redes comunitárias no Brasil. Os capítulos seguintes desenvolvem reflexões fundamentais sobre a aplicação do princípio da neutralidade de rede. O vigésimo segundo capítulo, *Da teoria à prática: a fiscalização e aplicação da neutralidade da rede no Brasil*, de Pedro H. S. Ramos e Andressa B. Andrade, desenvolve uma análise sobre a eficácia das ferramentas institucionais e regulatórias existentes no Brasil bem como as competências de cada uma das instituições envolvidas no *enforcement* de tal princípio. Já o vigésimo terceiro capítulo, intitulado *Ferramentas auxiliares para medição da neutralidade de rede pelos usuários*, de Nathalia S. Patrício, discorre sobre as diversas métricas que podem ser usadas para verificar o desempenho de uma rede apresentando também ferramentas que permitem ao usuário detectar violações no princípio da neutralidade da rede. Por fim os dois capítulos finais tratam da neutralidade de rede na criação e desenvolvimento de novos modelos de negócio na internet. O vigésimo quarto capítulo, *A franquia da banda larga fixa pode limitar o acesso à internet?*, de autoria de Gabriela Knupp e André Aprigio, trata da polêmica envolvendo o modelo de franquia de banda larga fixa que ganhou notoriedade a partir do anúncio feito por uma operadora no início de 2016. Já o vigésimo quinto capítulo, escrito por Pedro N. Mizukami e intitulado *Inovação em distribuição de vídeo digital: entre enforcement de direitos autorais e novos modelos de negócio*, sedimenta o debate sobre novos modelos de negócios em vídeo digital trazendo o panorama do direito autoral e lançando apontamentos para um trabalho mais aprofundado a respeito das implicações das regras de neutralidade de rede sobre a distribuição e produção de conteúdo entre outras dimensões.

A última seção, que discute "O futuro das coisas", apresenta um panorama sobre a constante interação entre dispositivos inteligentes, sensores e pessoas que compõem o cenário de Internet das Coisas (IoT). A seção traz, no vigésimo sexto capítulo, de autoria de Caitlin Mulholland e intitulado *A tutela da privacidade na Internet das Coisas (IoT)* uma reflexão sobre a proteção da privacidade e dados pessoais que são disponibilizados e coletados pelas "coisas" conectadas. Os autores do vigésimo sétimo capítulo, *Internet das Coisas Anônimas (AnIoT): considerações preliminares*, Eduardo Magrani e Luiz Abrahão, apontam para o número crescente de dados que estão sendo produzidos, armazenados e processados, tratando da importância do anonimato para a proteção de direitos individuais. O vigésimo oitavo capítulo, intitulado *Os direitos de privacidade na internet e a proteção de dados pessoais: uma compreensão conceitual para os direitos fundamentais*, escrito por Vinícius Borges Fortes, apresenta os fundamentos que constituem a base teórica dos direitos fundamentais, estabelecendo a conexão destes com a proteção da privacidade e a tutela dos dados pessoais na internet, especialmente a partir da abordagem do conceito de direitos de privacidade na internet. Já o vigésimo nono capítulo, *Internet das Coisas e inovação na América Latina*, de Olga Cavalli, traz casos paradigmáticos de desenvolvimento de IoT na América Latina através de diversos estudos e exemplos da região. O trigésimo capítulo, de autoria de Eduardo Peixoto, *De produtos à serviços: a IoT e a transformação da manufatura*, discorre sobre o conceito de IoT com uma breve perspectiva histórica, levantando questões sobre a produção e o consumo de variados produtos e serviços conectados. No trigésimo primeiro capítulo, *O gênero da Internet das coisas*, Bruna Castanheira traz uma visão crítica a respeito dos vieses de gênero contidos na construção de aparatos referentes à IoT, e de que maneira até então o desenvolvimento destas tecnologias se concentram em um universo masculinizado. Nessa mesma linha, o trigésimo segundo capítulo, escrito por Helena Ferreira Matos e intitulado *O viés em machine learning: perspectivas regulatórias*, apresenta uma reflexão sobre o potencial impacto discriminatório de algoritmos de aprendizagem automática e possíveis questões de regulação para inteligência artificial. No último trabalho desta seção, *Sobre a ética humana e a ética dos algoritmos*, de Renato R. Souza, há uma breve análise da crescente conectividade, ponderando os desafios da proteção da privacidade com os impactos na esfera constitucional e democrática.

É importante salientar que esse livro contou com a colaboração de muitas pessoas para que ele de fato acontecesse. Agradecemos à todas elas e, de forma especial, à Luiz Moncau, Marília Maciel, Sérgio França, Thaís Mesquita, Cristiana Gonzalez e Bruna Castanheira, assim como à todos os

pesquisadores, estagiários e professores do CTS e da FGV Direito Rio que ajudaram a conduzir esse projeto. Também agradecemos aos autores que se dedicaram a contribuir com as reflexões aqui apresentadas, por toda paciência e empenho ao longo do processo. E somos gratos à Fundação Getulio Vargas por todo apoio, pelo projeto que deu origem ao livro e pela ajuda para que ele se concretizasse.

Esperamos que os textos e as reflexões apresentadas nas próximas páginas possam se unir às muitas vozes que já analisam as relações entre tecnologia e sociedade há décadas, oferecendo mais algumas pistas dos desafios e oportunidades que se desdobram à nossa frente.

CIDADES, DADOS E DIREITOS

OS DESAFIOS DO AVANÇO DAS INICIATIVAS DE CIDADES INTELIGENTES NOS MUNICÍPIOS BRASILEIROS

MARINA BARROS
JAMILA VENTURINI

As recentes propostas de "cidades inteligentes" buscam oferecer soluções eficazes e inovadoras para os problemas gerados pelo rápido crescimento urbano. Na América Latina, 80% da população vive em áreas urbanas e vivencia problemas tais como poluição e congestionamentos. O uso das tecnologias e do processamento de grandes volumes de dados parece um atrativo para gestores públicos dado seu potencial de auxiliar no planejamento urbano. Ao mesmo tempo é impulsionado pelo setor privado, que busca expandir seus mercados, por exemplo, com a intitulada "Internet das coisas". Segundo relatório do McKinsey Global Institute, os dispositivos conectados entre si cresceram cerca de 300% nos últimos cinco anos e até 2025 a Internet das Coisas pode transformar profundamente a economia global. Num contexto em que a tendência é que cada vez mais os dados sejam utilizados pelo poder público para orientar o funcionamento de seus serviços, algumas perguntas permanecem: sob quais regras esses dados são coletados e analisados? Quais os impactos de seu processamento sobre os indivíduos e a vida social como um todo? Qual o papel que resta aos cidadãos nesse cenário de tomada de decisões de forma automatizada? Partindo dessas questões, o presente artigo traz algumas reflexões iniciais sobre as contradições da ascensão das cidades inteligentes no Brasil tendo como base dois estudos realizados pelo Centro de Tecnologia e Sociedade da FGV Direito Rio (CTS-FGV), um sobre a legislação aplicável ao uso de dados pessoais por parte do Estado – dando ênfase às questões de autogerenciamento da privacidade – e outro sobre o nível de transparência das políticas de gestão da informação dos maiores municípios brasileiros. Ao colocar em destaque os principais resultados desses estudos conclui-se que as cidades brasileiras estão despreparadas para os novos desafios colocados pelas práticas de *big data* e que novas ferramentas regulatórias

são necessárias para ampara o gestor nas suas decisões de coleta, uso e compartilhamento de dados bem como adoção de novas tecnologias.

INTELIGÊNCIA E GESTÃO PÚBLICA NAS CIDADES

O crescimento da população em áreas urbanas traz uma série de desafios para a gestão pública em setores como mobilidade, sustentabilidade, segurança, acesso à educação e saúde, entre outros. Diante deste contexto, o uso das Tecnologias de Informação e Comunicação (TIC) e processamento de grandes volumes de dados tem se mostrado atrativo para gestores públicos dado seu potencial de auxiliar no planejamento urbano. Ao mesmo tempo, a incorporação das tecnologias é fortemente impulsionada pelo setor privado que busca expandir seus mercados com a intitulada "Internet das Coisas", que torna objetos cotidianos capazes não só de coletar informações e interagir com o mundo físico, mas de se conectar uns aos outros para o intercâmbio de dados e informações. Ela se baseia na introdução de tecnologias de autoidentificação em objetos que podem intercambiar informações entre si sem necessidade de intervenção humana (BORGIA, 2014). Segundo relatório do McKinsey Global Institute, os dispositivos conectados entre si cresceram cerca de 300% nos últimos cinco anos e até 2025 a Internet das Coisas pode transformar profundamente a economia global.[1]

No Brasil, a agenda internacional de otimização da gestão pública baseada no uso de novas tecnologias esteve associada a realização de megaeventos que impulsionaram o desenvolvimento de iniciativas das chamadas "cidades inteligentes", por exemplo, nas áreas de segurança pública e defesa civil. Projetos desse tipo se multiplicam ao redor do mundo (SETO, 2015) com a promessa de incrementar a eficiência na gestão pública e trazer soluções inovadoras para os problemas urbanos (PAROUTIS; BENNET; HERACLEUOUS, 2013).

Essas propostas se somam às iniciativas de governo eletrônico já em curso, uma vez que a pauta de digitalização no setor público tem acompanhado o avanço das TIC, mas é implementada no país num ritmo mais lento que o dos avanços tecnológicos. Os benefícios atribuídos ao governo eletrônico vão desde a possibilidade de uma forma de governança pública mais inclusiva até aspectos mais práticos como a oferta *on-line* de serviços públicos, a melhoria da gestão pública, a agilidade nos processos administrativos e o melhor uso dos recursos públicos (MIRANDA; CUNHA, 2013).

1 Relatório disponível em: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Quando se trata de "cidades inteligentes", porém, os projetos vão além da mera digitalização dos serviços públicos para propor decisões automatizadas ou semiautomatizadas. A tendência é, portanto, de coleta cada vez maior de dados dos cidadãos. O termo *big data* aparece como coringa na propaganda e defesa deste tipo de iniciativa, por vezes como sinônimo de inovação e eficácia. Ele se refere ao processamento de grandes volumes de dados que marca a etapa contemporânea do desenvolvimento tecnológico global. Embora se trate de um conceito recente, alguns autores apontam como suas características principais:

a. o grande volume de conjuntos de dados – que está além da capacidade dos sistemas de processamento tradicionalmente utilizados para a coleta, armazenamento, gerenciamento e análise;
b. a velocidade na qual a informação é produzida, acessada e analisada;
c. a variedade de formatos de dados;
d. a veracidade da informação, que está relacionada com sua qualidade e precisão;
e. o valor ou potencial de impacto (TERZO; MOSSUCCA, 2015).

Outros, por outro lado, questionam as vantagens do *big data* ao considerar que dados não possuem valor em si mesmos - seu significado é extraído a partir de uma infraestrutura do conhecimento – e que são poucos os agentes que têm a capacidade para o gerenciamento e processamento de bases de dados tão grandes (BORGMAN, 2015).

De todo modo, pode-se observar uma tendência a coleta cada vez maior de dados pelo Estado com o objetivo de subsidiar a tomada de decisões e o funcionamento dos serviços públicos. No caso dos dados pessoais dos cidadãos, eles podem ser obtidos tanto diretamente – por meio de pesquisas e da interação das pessoas com os serviços públicos digitais ou objetos inteligentes instalados na cidade (como sensores e câmeras, por exemplo) –, quanto indiretamente por meio de suas concessionárias de serviços públicos ou a partir de acordos com empresas privadas.

Ainda que possa trazer benefícios, a migração dos serviços públicos para o meio digital e a coleta cada vez maior de informações dos cidadãos através de aplicativos de celular, páginas na internet ou outros objetos no contexto das cidades inteligentes, trazem uma série de novos desafios no que diz respeito à gestão da informação. Especificamente, é possível se identificar ao menos quatro dimensões do conceito de privacidade que podem ser implicadas no desenvolvimento de cidades inteligentes:

I. a privacidade das informações pessoais;

II. a privacidade das pessoas;

III. a privacidade de comportamento;

IV. a privacidade das comunicações pessoais (BARTOLI *et al.*, 2012).

Buscando avançar na compreensão desse cenário e desafios, a seguir apresentaremos uma breve contextualização sobre o marco legal existente no Brasil sobre privacidade e proteção de dados pessoais e uma discussão sobre como o avanço das tecnologias de *big data* colocam em xeque o princípio do consentimento informado no modelo de autogerenciamento da privacidade e as limitações desse modelo no contexto das interações Estado-setor privado que marcam as soluções de "cidades inteligentes". Finalmente, apresentaremos alguns resultados empíricos sobre o grau de preparação dos municípios brasileiros para esse tipo de projeto e breves apontamentos para se somar a discussões futuras sobre o tema.

O MARCO REGULATORIO DE PROTEÇÃO DA PRIVACIDADE NO BRASIL

O Brasil conta com fortes proteções à privacidade no âmbito constitucional, além de aderir aos principais tratados internacionais de direitos humanos que tratam do tema. No âmbito infraconstitucional, o país possui uma legislação sobre interceptação telefônica e telemática (Lei nº 9.296/1996) que regulamenta as situações excepcionais de quebra de sigilo das comunicações – previstas pelo artigo 5º, inciso XII da Constituição Federal – e delimita alguns procedimentos para sua implementação. Cabe observar que a legislação, apesar de atender a alguns dos princípios internacionais de direitos humanos para atividades de vigilância das comunicações (ANTONIALLI; ABREU, 2015), não impediu abusos como a interceptação ilegal de defensores de direitos humanos. Além da instalação de investigações de nível nacional para analisar o uso indiscriminado de interceptações em detrimento das limitações constitucionais, a condenação do Estado brasileiro por ilegalmente espionar as comunicações de ativistas ligados aos movimentos pelo direito à terra pela Corte Interamericana de Direitos Humanos no caso Escher e outros *vs.* Brasil é simbólica nesse sentido.

Outras leis determinam regras para a obtenção de informações para fins de investigação e as obrigações das empresas privadas de colaborar com esse processo. Elas incluem medidas de retenção de dados, acesso a dados cadastrais e a registros de conexão e acesso à internet, entre outras (VENTURINI *et al.*, 2016). Cabe ressaltar que tais normas não apresentam

as mesmas garantias observadas na lei de interceptação telefônica. Nota-se uma flexibilização nas garantias dadas ao conteúdo das comunicações em relação aos chamados metadados tanto por parte do Judiciário, quanto do Legislativo e Executivo.

Desde 2018, o país conta com uma Lei Geral de Proteção de Dados, fruto de quase uma década de discussões. Ela entrará em vigor em 2020 e regulará tanto o tratamento de dados por parte do setor público, quanto por empresas privadas. Além disso, uma série de normas setoriais abrangem o tema, tanto com relação ao tratamento de dados pessoais por parte de agentes públicos, quanto privados. Algumas leis que regulam a atuação do setor privado são o Código de Defesa do Consumidor (Lei nº 8078/1990), a Lei de Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet (Lei nº 12.965/2014).

No que diz respeito especificamente ao tratamento de dados por parte do Estado, as normas existentes são poucas, dispersas e não dão conta dos desafios trazidos pelas novas tecnologias e as propostas de "cidades inteligentes". Mesmo a Lei Geral de Proteção de Dados foi tímida em tratar das questões específicas relacionadas ao tratamento de dados por parte do Estado. Cabe ressaltar a exceção a aplicação da lei para dados relacionados a segurança pública e a autorização para o compartilhamento de dados públicos com entes privados sem necessidade de consentimento. Ainda assim, cabe destacar o mecanismo de *habeas data* – introduzido pela Constituição Federal de 1988 e regulado pela Lei nº 9.507/1997 –, que garante ao titular o direito de acesso e retificação de dados pessoais detidos pelo Estado. Além disso, a Lei de Acesso à Informação Pública (Lei nº 12.527/2011) estabeleceu regras referentes à divulgação de informações de caráter pessoal detidas pelo poder público – incluindo entes estatais e organizações sem fins lucrativos que recebam algum tipo de financiamento público.

No que diz respeito às informações pessoais, a lei restringe o acesso a:

I. funcionários públicos legalmente autorizados;

II. aos titulares dos dados, por um período de 100 anos desde a sua produção.

A publicação ou acesso também serão permitidos se houver uma lei específica ou consentimento expresso do titular autorizando-o. As exceções às regras de proteção previstas incluem: fins médicos, quando o titular de dados não é capaz de oferecer consentimento; o desenvolvimento de estatísticas e pesquisas científicas de interesse público; o cumprimento com a lei e para a defesa e proteção dos direitos humanos e o interesse público.

A lei, porém, não limita a coleta de dados por parte do Estado, deixando lacunas importantes principalmente no que diz respeito às iniciativas das "cidades inteligentes" na forma como têm sido implementadas no Brasil. Em um contexto em que se encontram disponíveis tecnologias sofisticadas para a vigilância de comunicações digitais no mercado e multiplicam-se acordos entre o setor privado e público para a oferta de soluções "inteligentes" de gestão, a ausência de regras específicas e limites à coleta de informações por parte do Estado pode trazer riscos à privacidade e segurança.

Finalmente, não há nas leis supracitadas um detalhamento sobre as medidas de segurança necessárias para prevenir o acesso indevido às bases de dados que contenham informações pessoais. Uma vez que não são especificadas na legislação sobre acesso à informação de nível federal, caberia a princípio a cada ente federativo regular essa questão.

SOBRE O MODELO DE AUTOGERENCIAMENTO DA PRIVACIDADE E SUAS LIMITAÇÕES

A proteção da privacidade em seu aspecto relativo ao tratamento de dados pessoais esteve por muito tempo baseada num modelo de autogerenciamento. Tal modelo se fundamenta na ideia de consentimento, que advém da compreensão de que somente o titular – dotado das informações necessárias para tomar uma decisão consciente – pode autorizar ou não o tratamento de seus dados pessoais. Ele é considerado uma das condições fundamentais para o tratamento de dados, pois permite que os indivíduos possam desfrutar plenamente o seu direito de autodeterminação. Seu objetivo é oferecer às pessoas o controle sobre seus dados pessoais e a possibilidade de tomar decisões sobre o tratamento considerando os custos e benefícios que pode trazer. O modelo de autogerenciamento da privacidade é incorporado pela legislação brasileira relativa ao uso de dados tanto por parte de agentes privados, quanto públicos.

No caso das relações *on-line*, a solicitação do consentimento tem sido implementada pelo setor privado principalmente através de contratos de adesão que os usuários devem aceitar ao utilizar seus serviços, os chamados Termos de Uso. No entanto, se mesmo no mundo *off-line* os contratos de adesão – o tipo de contrato mais comum para a maioria das transações econômicas – poucas vezes são lidos, no ambiente *on-line* essa situação parece se agravar. No mercado de compra e venda de software online, por exemplo, apenas entre 0,22 e 0,5% dos consumidores leem as *End User License Agreements* (EULAs) (BAKOS; MAROTTA-WURGLER; TROSSEN, 2013). E ainda que quisessem se informar sobre as condições de trata-

mento de seus dados pessoais, talvez poucos tivessem o tempo necessário para tanto: segundo um estudo da Universidade de Carnegie Mellon, nos Estados Unidos, um usuário deveria reservar 8h diárias em 76 dias de um ano para ler somente as Políticas de Privacidade de uma média de 1.462 páginas visitadas (MCDONALD; CRANOR, 2008). Com a Internet das Coisas, o cenário deve ser ainda mais preocupante, uma vez que se ampliam as situações de coleta e processamento de dados pessoais reguladas por este tipo de contrato.

Por conta disso, o modelo de autogerenciamento baseado na informação e consentimento tem sido criticado como capaz de proteger a privacidade. Para além da dificuldade de se tomar uma decisão informada, entre outros motivos, aponta-se a que o titular se vê cada vez mais compelido a autorizar certos tratamentos de seus dados para acessar os serviços ou obter os produtos desejados. A União Europeia, por exemplo, conta com uma legislação de proteção de dados pessoais desde os anos 90 cujos princípios em alguma medida contradizem o modelo de negócios em que muitos dos serviços *online* se baseia (PEREIRA, 2015).[2] Isso não impede, porém, que a cada ano haja mais consumidores para tais serviços no continente (JOERGENSEN, 2014).[3]

BIG DATA E CONSENTIMENTO

O surgimento e avanço de novas tecnologias de processamento e de negócios baseadas no tratamento intensivo de dados pessoais, como é o caso das iniciativas de cidades inteligentes, também têm colocado novos desafios para o modelo do consentimento. Solove (2013) fala de problemas estruturais que incluem:

I. um problema de escala, no qual há uma quantidade imensa de entidades que realizam algum tipo de tratamento de dados pessoais, com ou sem conhecimento do titular fazendo a intermediação de certas operações;

2 A decisão da Corte de Justiça Europeia que derrubou o acordo que permitia a transferência de dados de cidadãos europeus para os Estados Unidos, mostra o quanto as premissas que a autorizavam eram frágeis nesse novo contexto.

3 Cabe ressaltar que a contradição não passa alheia à percepção dos consumidores europeus. Apesar da necessidade de consentimento para certos tratamentos de dados pessoais estar garantida há pelo menos uma década, apenas pouco mais de um quarto dos usuários de redes sociais, por exemplo, acredita ter controle total de seus dados (EUROPEAN COMMISSION, 2011).

II. um problema de agregação, ou seja, de que se pode deduzir informações sobre uma pessoa a partir da combinação de dados a princípio inofensivos;

III. um problema de avaliação dos danos, já que os impactos negativos do compartilhamento de certos dados podem ocorrer após um longo período de tratamento, enquanto os benefícios são geralmente imediatos.

De fato, o modelo de "aviso e consentimento" se baseia na definição preliminar do uso dos dados pessoais pelo controlador associada à anuência do titular, e não consegue enquadrar os desafios decorrentes do uso de técnicas de *big data*, que buscam extrair inferências a partir da análise de grandes conjuntos de dados após a coleta. O responsável pelo tratamento não pode, nesse caso, definir – ou até mesmo ter uma compreensão clara – a finalidade do processamento dos dados no momento ou antes da coleta inicial. Por outro lado, a complexidade do tratamento de grandes volumes de dados muitas vezes não permite que os titulares realmente compreendam e possam avaliar suas consequências e potenciais efeitos negativos. Se torna, assim, praticamente impossível o gerenciamento dos dados pelo titular:

> Os tipos de novas informações que podem ser extraídas a partir da análise de informações existentes e a natureza das previsões que podem ser feitas a partir desses dados são muito vastas e complexas, e sua evolução é rápida demais para que as pessoas consigam avaliar os riscos e benefícios envolvidos.[4] (SOLOVE, 2013, *online*, tradução livre)

O MODELO DE CONSENTIMENTO NOS SERVIÇOS PÚBLICOS DIGITAIS

Quando se trata do setor público, a multiplicação de serviços e plataformas *on-line* para a interação com os cidadãos num contexto de governo eletrônico ou cidades inteligentes nem sempre vem acompanhada de políticas claras de gestão. Há pouca informação sobre quais regras se aplicam aos dados e, principalmente, metadados coletados por essas ferramentas no ambiente *on-line*. A falta de clareza se agrava quando o poder público opta por utilizar soluções privadas como o WordPress ou Google Analytics para o desenvolvimento e avaliação de seus serviços ou para a comunicação com os cidadãos.

4 No original: "The types of new information that can be gleaned from analyzing existing information and the kinds of predictions that can be made from this data are far too vast and complex, and are evolving too quickly, for people to fully assess the risks and benefits involved". (SOLOVE, 2013, *on-line*)

Observa-se assim um cenário em que a regulação privada através de contratos substitui ou se sobrepõe às políticas públicas existentes, preenchendo os vazios regulatórios e se impondo também nas relações entre cidadãos e Estado. Diferente do que ocorre no âmbito privado, portanto, em que usuários – ao menos hipoteticamente – têm a opção de aderir ou não às plataformas, no caso dos serviços públicos a opção de consentir ou não com o tratamento de dados pelos mesmos agentes privados – geralmente invisibilizados nessa relação – pode não estar dada.

Exemplos de como isso pode ocorrer são o uso de serviços de e-mail privados por parte de órgãos públicos e a disponibilização de informações de interesse público exclusivamente através de redes sociais.[5]

CONSENTIMENTO NAS RELAÇÕES PÚBLICO-PRIVADAS

As denúncias de que os governos dos Estados Unidos e seus parceiros, no grupo conhecido como "Five Eyes", realizavam atividades de vigilância em massa que afetaram cidadãos e representantes de governos de todo o mundo despertaram reações em diversos setores. O escândalo parece ter materializado preocupações que atormentavam ativistas há algum tempo sobre o aumento da capacidade de vigilância do Estado, em grande medida, a partir da colaboração do setor privado, principalmente das empresas do setor de TIC.

Apesar de, num primeiro momento, as denúncias publicadas pelo jornal britânico *The Guardian* gerarem revolta, inclusive por parte do governo brasileiro - um dos líderes nas discussões internacionais sobre privacidade na era digital[6] –, isso não impediu ou trouxe suficientes garantias quanto ao estabelecimento de parcerias entre poder público e agentes privados no âmbito das cidades inteligentes.

---

5 De acordo com a pesquisa TIC Governo Eletrônico (CETIC, 2015) 90% das prefeituras brasileiras possuem perfil ou conta própria em rede social online para divulgar serviços ou campanhas e 77% para responder a comentários e dúvidas dos cidadãos. Em contrapartida, apenas 13% das prefeituras afirma possuir algum manual ou guia para a publicação de conteúdo em redes sociais *on-line*.

6 Junto ao governo alemão, o Brasil impulsionou os debates internacionais sobre a necessidade de maiores proteções à privacidade na era digital e foi um dos grandes responsáveis pela aprovação na Assembleia Geral das Nações Unidas da Resolução 68/167 sobre o tema. No âmbito nacional, além da realização de uma Comissão Parlamentar de Inquérito para analisar as denúncias de espionagem por parte dos Estados Unidos, a aprovação do Marco Civil da Internet – que já vinha sendo discutido no Congresso – e a realização do encontro NETMundial, marcaram a resposta brasileira aos escândalos de vigilância massiva. Do mesmo modo, o Decreto 8.135 de novembro de 2013 pretendia garantir a segurança das comunicações da administração pública federal.

O Centro de Operações Rio (COR), da Prefeitura do Rio de Janeiro, por exemplo, estabeleceu uma parceria com o aplicativo Waze visando oferecer informações sobre as condições do trânsito na cidade. De acordo com matéria publicada no jornal *O Globo* (MACHADO, 2013), a Prefeitura usa os dados oferecidos pela empresa para identificar engarrafamentos, retenções e acidentes em tempo real. Por mais que na reportagem um dos responsáveis pela iniciativa garantisse que a Prefeitura não tem acesso a informações dos usuários, as condições exatas do acordo não são em nenhum momento esclarecidas. Do mesmo modo, notícias evidenciam o uso de dados do Twitter para monitorar acontecimentos na cidade (PARQUE TECNOLÓGICO UFRJ, 2014).

Para além das práticas de anonimização de dados serem fortemente questionadas (SWEENEY; ABU; WINN, 2013) e colocarem em xeque a premissa de que a Prefeitura não tem acesso a dados pessoais, quando se trata do consentimento a questão é até que ponto ele autorizaria o compartilhamento de informações com o poder público. Ou ainda, quão informados estariam os usuários sobre essa possibilidade caso lessem os Termos de Uso dessas plataformas. A resposta é pouco: estudo recente que analisou os Termos de Uso de 50 plataformas *on-line* aponta que apesar de longos e aparentemente detalhados, esses documentos costumam ter cláusulas genéricas autorizando o compartilhamento de dados e políticas complacentes em relação a pedidos de acesso a dados por parte de governos (VENTURINI *et al*., 2016).

TRANSPARÊNCIA PARA QUEM?

Parece irônico problematizar a divulgação e compartilhamento de informações em um país marcado por uma cultura do segredo e que demorou mais de vinte anos para regulamentar o direito de acesso a informações públicas. No entanto, não se pode ignorar que práticas até então corriqueiras na administração pública podem implicar em usos indevidos de informações pessoais do cidadão comum. Ao mesmo tempo, dados tidos como de acesso público disponibilizados em meio digital podem ser facilmente processados, combinados e agregados: o Decreto de Dados Abertos (n. 8.777/2016), por exemplo, prioriza a publicação de uma lista de treze bases de dados a serem disponibilizadas em formato aberto e processável por máquina. Cinco das bases listadas referem-se a dados pessoais, tais como nascimentos, casamentos, divórcios e mortes, ocupações de cargos de gerência e direção em empresas estatais, dados sobre servidores inativos e aposentados, quadro societário de empresas, entre outros. A facilidade de processamento e combinação desses dados traz novos desafios para a

busca de equilíbrio entre o direito de acesso à informação e a proteção da privacidade (O ESTADO DE S. PAULO, 2015).[7]

Por conta dessas complexidades, adotar políticas de acesso, assim como de proteção de dados pessoais é tarefa complexa e demanda esforços coordenados pela construção de políticas amplas de gestão da informação. Sem isso, as propostas de governo eletrônico e cidades inteligentes se tornam arriscadas independente dos eventuais benefícios que possam trazer no nível imediato.

Por outro lado, ainda é necessário mais transparência sobre as iniciativas de digitalização, oferta de serviços online, processamento massivo de dados e tomada de decisões automatizadas por parte da gestão pública. Surpreendentemente, as cidades que se autointitulam inteligentes tem sido pouco transparentes nesse sentido. O caso da cidade do Rio de Janeiro é simbólico nesse sentido: apesar de ser considerada um exemplo internacional de "cidade inteligente", o município apresenta um dos piores resultados nacionais em termos de transparência pública (MICHENER; MONCAU; VELASCO, 2014).

Numa tentativa de obter dados da gestão municipal e avaliar o grau de transparência das Prefeituras brasileiras com relação à gestão de dados, a oferta de serviços online e a existência de iniciativas de cidades inteligentes na área de segurança pública, pesquisa da Fundação Getulio Vargas (BARROS; VENTURINI, 2016) enviou pedidos de acesso à informação a 43 prefeituras brasileiras. Os pedidos questionavam sobre:

I. a existência de centros integrados de comando e controle com fins de monitoramento e vigilância, suas características e normativas relacionadas;
II. a existência de acordos ou contratos com empresas privadas para a prestação de serviços no âmbito desses centros;
III. a aquisição de tecnologias de vigilância e monitoramento como câmeras, veículos aéreos não tripulados (*drones*) ou robôs nos últimos quatro anos e os documentos relativos a tal aquisição;
IV. a existência de iniciativas de governo eletrônico e participação online através de aplicativos de celular ou páginas de Internet;
V. o uso de mecanismos de análise (do tipo Google Analytics e outros) para a medição de tráfego em seus páginas online e como os dados obtidos são utilizados.

7 O caso do *site* Tudo sobre Todos, por exemplo, gerou um grande debate nacional sobre a exposição dos cidadãos com a publicação de seus dados pessoais de forma organizada e acessível, mas em sua página afirma apresentar informações obtidas apenas de bases públicas como o diário de justiça, diário oficial e de cartórios públicos.

Por outro lado, a pesquisa buscou obter informações sobre o quão preparados estavam os municípios para lidar com as informações obtidas a partir dessas iniciativas questionando sobre: (a) a existência de um órgão ou departamento responsável pelos sistemas de tecnologia da informação em todo o governo; (b) a existência de posições oficiais permanentes dedicadas à gestão de informação; (c) as políticas existentes sobre privacidade, sigilo governamental, segurança da informação, entre outras relacionadas à gestão da informação.

A pesquisa revelou que boa parte dos municípios avaliados ainda estão despreparados para enfrentar os novos desafios colocados pelas práticas de *big data* no que diz respeito às suas políticas de gestão da Tecnologia da Informação e de tratamento de dados pessoais.

Na prática, isso significa que os interesses comerciais e corporativos encontram um terreno suscetível à discricionariedade do agente, ou seja, as decisões de contratação, da escolha de padrões, tecnologias, proteções entre outros elementos de uma política de informação municipal ficam na mão do gestor e, de acordo com a pesquisa, há pouca ou quase nenhuma transparência sobre isso.

Repetindo a baixa taxa de resposta de outros levantamentos realizados anteriormente pela FGV, esta pesquisa também obteve poucas respostas aos pedidos de acesso à informação enviados. Destacam-se, contudo, os seguintes resultados:

- 23 dos 52 municípios avaliados responderam o pedido de acesso sobre a existência de órgão ou departamento responsável por TI no governo. Contudo, apenas 11 deles (26%) enviaram a documentação solicitada com destaque para os municípios de São Paulo e Curitiba;
- Já com relação à pergunta que solicitava as normas de privacidade, o sigilo governamental, segurança da informação e transações eletrônicas utilizadas pelo município obtivemos 24 respostas, apenas treze delas adequadas com destaque para o município de Londrina e Belo Horizonte, Salvador e São Luís;
- Apenas dezenove municípios responderam à pergunta sobre a existência de um centro de comando e controle na cidade, sendo apenas treze consideradas adequadas com destaque para a Prefeitura de Cuiabá, Porto Velho, Belo Horizonte, São Luís e Palmas;
- Com relação ao pedido que solicitava informação sobre aquisição de equipamentos de monitoramento e vigilância, os municípios de Porto Velho, Curitiba, Londrina, Palmas e Belo Horizonte foram os únicos que responderam à pergunta de forma completa, fornecendo a documentação relativa à aquisição destes serviços tais como os editais de licitação, contratos de compra e notas fiscais.

O *enforcement* da transparência sobre tais temas se faz relevante não só pela vigência da Lei de Acesso à Informação no Brasil como também pela importância do controle social sobre os aspectos que regulam a vida do cidadão nos grandes centros urbanos.

Permitir conhecer as políticas de tecnologia da informação de seu município, as práticas de vigilância ou os decretos que regulam o uso de dados, entre outras práticas da gestão municipal no âmbito da tecnologia da informação, é dar ao cidadão a garantia do exercício do controle social sobre a administração pública.

Os dados e exemplos acima evidenciam um aparente desequilíbrio no qual as atividades do Estado – inclusive na área de segurança pública e vigilância – seguem secretas e pouco sujeitas a escrutínio público, enquanto os cidadãos encontram-se cada vez mais expostos tanto frente ao próprio Estado, quanto a outros agentes privados.

CONSIDERAÇÕES FINAIS

A exposição acima buscou evidenciar por um lado as limitações existentes na legislação brasileira de proteção da privacidade e por outro o quanto certas soluções regulatórias encontram-se ultrapassadas no contexto de avanço tecnológico e das propostas de cidades inteligentes. Para isso, foram trazidos exemplos de como os cidadãos encontram-se fragilizados nesse cenário, enquanto as práticas do Estado seguem ocultas. Buscou-se ainda problematizar a relação entre o setor público e privado nas atividades de monitoramento e vigilância populacional, o que traz mais dificuldades para o controle dessas atividades. Nesse sentido, políticas de transparência parecem ser fundamentais, assim como o desenvolvimento de planos de gestão da informação para lidar com questões como segurança, documentação, armazenamento, etc.

No entanto, para além de eventuais propostas regulatórias, parece relevante refletir sobre as limitações de uma compreensão da privacidade como direito individual e quais as consequências de se "trocar" a privacidade por outros bens nas democracias contemporâneas. Para Cohen (2013), por exemplo, os indivíduos não deveriam poder abrir mão de sua privacidade em certas circunstâncias. Solove (2013) ao refletir sobre o modelo de *privacy self-management*, concorda ao concluir que ele deve ir além de uma abordagem que se pretenda neutra sobre o mérito de tratamentos de dados particulares.

No desenvolvimento de políticas de cidades inteligentes, cabe repensar a privacidade enquanto bem social para além de sua dimensão individual no momento de sopesar interesses conflitantes. Não se pode negar categoricamente que essas propostas podem trazer benefícios sociais, mas é necessário que haja escrutínio público e um debate aberto sobre as garantias e limitações que serão necessárias para que elas sejam implementadas.

REFERÊNCIAS

ANTONIALLI, D.; ABREU, J. Vigilância das comunicações pelo Estado brasileiro e a proteção de direitos fundamentais, 2015. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf>. Acesso em: 4 nov. 2016.

BAKOS, Y.; MAROTTA-WURGLER, F.; TROSSEN, D. R. Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts. *Journal of Legal Studies*, v. 43, n. 1, 2014. Disponível em: <http://ssrn.com/abstract=1443256>. Acesso em: 6 jul. 2018.

BARTOLI, A.; HERNANDEZ-SERRANO, J.; SORIANO, M.; DOHLER, M.; KOUNTOURIS, A.; BARTHEL, D. *On the Ineffectiveness of Today's Privacy Regulations for Secure Smart City Networks*. Washington: Smart Cities Council, 2012.

BORGIA, E. The Internet of Things Vision: Key Features, Applications and Open Issues. *Computer Communications*, n. 54, p. 1-31. [S.l.: s.n.], 2014.

CARDOSO, B. D. V. Megaeventos esportivos e modernização tecnológica: planos e discursos sobre o legado em segurança pública. *Horizontes Antropológicos*, n. 19, v. 40, p. 119-148, 2013.

COHEN, J. E. What Privacy Is For. *Harvard Law Review*, v. 126, 2013. Disponível em: <http://ssrn.com/abstract=2175406>. Acesso em: 1 nov. 2016.

COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro: TIC governo eletrônico 2015. 2016. Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_eGOV_2015_LIVRO_ELETRONICO.pdf>. Acesso em: 4 nov. 2016.

EUROPEAN COMMISSION. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, TNS Opinion and Social at the request of Directorate-General Justice, 2011. Disponível em: <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf>. Acesso em: 5 dez. 2018.

LOUZADA, L.; VENTURINI, J. A regulamentação da proteção de dados pessoais no Brasil e na Europa: uma análise comparativa, 2015. Disponível em: <http://lavitsrio2015.medialabufrj.net/anais/#theme-1>. Acesso em: 1 nov. 2016.

MACHADO, A. Prefeitura começa a usar Waze no Centro de Operações Rio. O Globo, 2013. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/

prefeitura-comeca-usar-waze-no-centro-de-operacoes-rio-9152370>. Acesso em: 4 nov. 2016.

MCDONALD, A. M.; CRANOR, L. F. The Cost of Reading Privacy Policies. *ISJLP*, n. 4, 543, 2008. Disponível em: <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf>. Acesso em: 1 nov. 2016.

MICHENER, G.; MONCAU, L. F. M.; VELASCO, R. Estado Brasileiro e transparência: avaliando a aplicação da Lei de Acesso à Informação, 2014. Disponível em: <http://transparencia.ebape.fgv.br/sites/transparencia.ebape.fgv.br/files/105_-_brasil_-_estado_brasileiro_e_transparencia_0.pdf >. Acesso em: 1 nov. 2016.

O ESTADO DE S. PAULO. Site 'Tudo Sobre Todos' divulga seu CPF, endereço e até quem são seus parentes e vizinhos. Brasil Post, 2015. Disponível em: <http://www.brasilpost.com.br/2015/07/28/site-tudo-sobre-todos_n_7886240.html>. Acesso em: 4 nov. 2016.

PAROUTIS, S.; BENNETT, M.; HERACLEOUS, L. A Strategic View on Smart City Technology: The Case of IBM Smarter Cities during a Recession. *Technological Forecasting and Social Change*, n. 89, p. 262-272, 2014. Disponível em: <http://www.sciencedirect.com/science/journal/00401625>. Acesso em: 17 ago. 2016.

PARQUE TECNOLÓGICO DA UFRJ. Equipe do Parque Tecnológico da UFRJ visita COR, 2014. Disponível em: <http://www.parque.ufrj.br/wp-content/uploads/2014/04/Parque-UFRJ-21.03.2014.htm>. Acesso em: 4 nov. 2016.

PEREIRA, L. Queixa de um único cidadão derruba acordo de coleta de dados entre EUA e Europa. Olhar Digital, 2015. Disponível em: <http://olhardigital.uol.com.br/noticia/queixa-de-um-unico-cidadao-derruba-acordo-de-coleta-de-dados-entre-eua-e-europa/51929>. Acesso em: 4 nov. 2016.

SETO, Y. Application of Privacy Impact Assessment in the Smart City. *Electronics and Communications in Japan*, n. 98, v. 2, p. 52-61, 2015.

SOLOVE, D. Introduction: Privacy Self-Management and the Consent Dilemma, *Harvard Law Review*, v. 126, p. 1884, 2013. Disponível em: <http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf>. Acesso em: 21 jul. 2016.

SWEENEY, L.; ABU, A.; WINN, J. Identifying Participants in the Personal Genome Project by Name, 2013. [S.l.: s.n.] Available at SSRN 2257732.

TERZO, O.; MOSSUCCA, L. (Eds.). Cloud Computing with e-Science Applications. Crc Press. [S.l.: s.n.], 2015.

VENTURINI, J.; LOUZADA, L.; MACIEL, M.; ZINGALES, N.; STYLIANOU, K.; BELLI, L. Termos de uso e direitos humanos: uma análise dos contratos das plataformas online. No prelo. [S.l.: s.n.], 2016.

VENTURINI, J.; MACIEL, M.; DICKOW, M.; DAHLMANN, A. Privacidade e vigilância na era digital: um estudo comparativo do marco legal brasileiro e alemão. [S.l.: s.n.], 2016.

POLÍTICA PÚBLICA DE INFORMAÇÕES E ABERTURA DE DADOS: QUAL O LIMITE PARA A PRIVACIDADE DE DADOS CADASTRAIS NAS "CIDADES INTELIGENTES"?

TOMÁS WISSENBACH

INTRODUÇÃO

A evolução das tecnologias da informação e da comunicação tem colocado em relevo os potenciais e os riscos de uma ampla coleta de dados, inclusive os pessoais, no âmbito da gestão urbana. Não à toa, pois praticamente todas as dimensões das relações sociais na cidade passaram a ser permeadas por mediações tecnológicas, seja no âmbito privado, na oferta de serviços públicos ou na interação do cidadão com o estado. Em suma, passam a permear as interações entre consumidores e empresas, burocracias e prestadores de serviço, entre cidadão e governos.

São muitos os exemplos do imenso volume de informações, os famosos *big data*, gerados por essas interações. Os dispositivos móveis com localizador e GPS permitem armazenar informações sobre trajetos, caminhos e rotinas. As buscas por serviços, geolocalizadas, dão ao setor privado ampla possibilidade de identificar e prever padrões de comportamento deslocamento e as preferências de todos nós. O próprio uso de serviços públicos fornece incontáveis dados que, a princípio, fortalecem a capacidade estatal de planejamento: se antes, para saber o padrão de mobilidade do cidadão era preciso realizar custosas pesquisas de origem-destino, agora os dados dos usuários de transporte público são armazenados e cadastrados eletronicamente, com imensos potenciais para as políticas públicas. Há ainda os mecanismos de consultas públicas e participação digital, que abrem novas possibilidades de incidência do cidadão nas políticas públicas e os sistemas de gestão da zeladoria urbana, que oferecem a possibilidade simultânea de acompanhamento e controle das atividades pelo gestor e a melhor alocação de recursos em relação às demandas da cidade.

Não há dúvida de que existe uma transformação em curso, que está mudando e mudará as dinâmicas das cidades. A intensidade e a novidade desse fenômeno têm levado a muitos pesquisadores a indagar: afinal, qual o sentido dessas transformações? Tornarão as cidades mais justas e democráticas ou aprofundarão as desigualdades e a concentração de poder e riqueza?

Esse campo de possibilidades tem levado a projeções de impactos positivos das novas tecnologias para as cidades e para o planejamento urbano e que, não raro, são abrigadas no rótulo de cidades inteligentes. Tecnologias baratas, como simples sensores instalados em semáforos, parques ou terminais de ônibus permitiriam o aumento exponencial de dados disponíveis que resultariam em conhecimento mais profundo sobre as dinâmicas das cidades e, com isso, ampliariam a capacidade de uma intervenção mais efetiva sobre elas (BYRNES, 2015). De forma geral, são baseados na expectativa da convergência entre:

I. o planejamento e gestão urbana, sob a premissa da eficiência;

II. o aumento exponencial da capacidade de coleta e processamento de dados pessoais georreferenciados;

III. na promoção de novas infraestruturas necessárias para a transmissão dessas informações (LUQUE-AYALA; MARVIN, [s.d.]).

Os potenciais positivos dessa convergência operariam em variados campos. Ao organizar seus fluxos a partir das novas tecnologias, a mobilidade urbana poderá se tornar mais eficientes e, com isso, diminuir suas emissões de gases de efeito estufa. A simplificação e automatização de processos otimizará a entrega de serviços públicos permitindo, com isso, gastar menos e produzir mais. Algumas dessas aplicações já têm sido testadas e reportadas em experiências para cidades específicas (MAJCHER, K., 2015). No atendimento de emergências, para o gerenciamento de riscos e mitigação de impactos de desastres naturais, para a prevenção ao crime e promoção da segurança urbana, as novas tecnologias de sensoriamento e monitoramento permitiriam maior efetividade na ação estatal por meio de mobilização dos recursos necessários e no momento certo. Mais informação sobre as dinâmicas urbanas poderá aprimorar a capacidade de tomada de decisão cotidiana, e também de construir modelos e ferramentas para a construção de cenários de longo prazo. Haveria, ainda, uma ampliação da participação do cidadão nas decisões políticas, por meio de canais de participação não presenciais. Bons exemplos nesse sentido são as consultas públicas, minutas participativas de projetos de lei e canais fáceis de atendimento ao público.

Apoiada por organizações internacionais e por grandes empresas de tecnologia da informação, a agenda das cidades inteligentes tem se tornado prioritária para muitos governos municipais, seja em termos de recursos, de visibilidade e em termos orçamentários.[1] Faz surgir também, para administradores públicos municipais e planejadores urbanos, "[...] um novo léxico através dos quais as cidades (inteligentes) estão sendo forjadas – apps urbanos, *big data*, infraestrutura inteligente, sensores urbanos, painéis urbanos, smart meters, edifícios inteligentes e *smart grid*". (LUQUE-AYALA; MARVIN, 2015).

Por outro lado, são crescentes as preocupações relacionadas ao uso dessas informações, seja do ponto de vista de sua apropriação privada, seja do ponto de vista dos riscos do monitoramento para fins escusos. Com efeito, há enorme desconfiança em relação à participação das grandes empresas na gestão urbana, dada a pouca transparência em diversos casos e a finalidade privada da sua participação. Sem dúvida, criar – e vender – sistemas é um negócio altamente lucrativo, e o setor público um importante cliente para as empresas de tecnologia. O rótulo "cidades inteligentes" torna-se, dessa forma, um campo aberto – e muitas vezes com pouco controle – para corporações promoverem suas soluções combinando desenvolvimento de sistemas inovadores e a difusão de utopias urbanas (SÖDERSTRÖM; PAASCHE; KLAUSER, 2014).

Uma abordagem acrítica do uso dessas tecnologias pode significar, ainda, uma roupagem moderna para um planejamento e gestão urbana de cunho tecnocrático, ao sugerir que o desafio da questão urbana brasileira seria simplesmente desenvolver as ferramentas corretas para identificar os problemas e operar as soluções, em algo próximo do que foi identificado por Scott como solucionismo (SCOTT, 2016). À gestão autoritária e à apropriação privada, soma-se ainda a falta de transparência na política de privacidade dos dados e, dado o volume de informações sobre o cidadão, os riscos que representam o *big data* e o sensoriamento das cidades no âmbito dos direitos civis (THRIFT, 2014).

Entre potenciais e aspectos críticos, fica claro que o debate a respeito do impacto das novas tecnologias da informação no planejamento e gestão de cidades merece aprofundamento. Evidentemente, o sentido das transformações advindas da ampla utilização das novas tecnologias pelo setor público leva necessariamente a um debate conceitual e universal sobre o tema, dado que esse é um fenômeno abrangente nas dinâmicas de

1 Ver, por exemplo: European Commission. EU SET-Plan: Strategic energy technology plan. [s.d.] Disponível em: <https://setis.ec.europa.eu/set-plan-implementation/technology-roadmaps/european-initiative-smart-cities e>. Acesso em: 05 set. 2017.

cidades por toda parte no globo. Entretanto, sob pena de estabelecer uma abordagem descontextualizada, convém travar esse debate a partir de um conjunto de mediações a partir da realidade nacional.

Necessário considerar, de início, que o processo de urbanização no Brasil se deu no âmbito de um processo autoritário no qual o território – ou parte dele, de forma seletiva – e não o povo, foi objeto da modernização conservadora (MORAES, 2005). O Estado, nesse contexto, foi marcado pela tradição patrimonialista das elites brasileiras, configurando-se como uma estrutura para operar a apropriação privada dos bens comuns. No plano das informações, tais características marcaram um processo no qual pesou a tradição cartorial, e se constituiu uma dinâmica de desorganização intencional dos registros territoriais que permitiu a captura da regulação da produção do espaço pelo setor privado.

A partir das questões apontadas brevemente nessa apresentação, esse capítulo tem como objetivo apresentar uma experiência concreta da construção da infraestrutura de dados espaciais na cidade de São Paulo na gestão de Fernando Haddad (2013-2016). Pretendemos também discutir o papel das informações sobre a cidade no âmbito de sua gestão democrática, em um contexto cujos fatores estruturais levariam ao aumento das assimetrias informacionais. Particularmente trataremos da disponibilização do cadastro imobiliário da cidade: o Cadastro Territorial, Predial, de Conservação e Limpeza (TPCL), base para o cálculo do Imposto Territorial e Predial Urbano (IPTU). Tal divulgação, pioneira no contexto nacional, abre um debate em torno da divulgação de bases de dados públicas que contém informações pessoais. Em função disso, pretendemos apresentar alguns resultados da utilização dessa base por pesquisadores e organizações da sociedade civil, que só puderam ser realizados a partir da sua disponibilização integral, e que tocam em pontos centrais da reprodução da desigualdade urbana.

INFORMAÇÃO SOBRE O TERRITÓRIO, ASSIMETRIAS E GESTÃO DEMOCRÁTICA DAS CIDADES

Do ponto de vista mais abstrato, avançar no debate a respeito da interface entre a política urbana e as novas tecnologias pede a retomada, ainda que breve, da relação entre informação e território. Nesse, é importante pontuar inicialmente que o território, ou mais genericamente, o espaço, não se confunde com o ambiente construído. Pelo contrário, ele tem sido interpretado e abordado como uma dimensão específica da vida social, o que tem levado às noções de apropriação e produção do espaço (SANTOS, 2002; MORAES;

COSTA, 1999). Será sempre, portanto, mediada por relações sociais: o ordenamento jurídico, as relações de poder, a propriedade privada, a condição espacial – por exemplo, a condição periférica –, caracterizam o território tanto quanto os prédios, as avenidas, as infraestruturas físicas. Nesse sentido, a informação sobre o território é uma das mediações fundamentais que constituem as relações econômicas e de poder nas sociedades. Tomando como exemplo um determinado lote urbano. Saber se ele está em área contaminada, saber se ele é público ou privado, saber se é uma ZEIS – interesse social – ou Eixo – alto aproveitamento do solo. Todas essas características são constitutivas daquele lote e, portanto, fazem parte do que podemos ou não fazer como ele. Em função disso, a assimetria informacional sempre foi, e é continuamente, elemento central para que a ação pública e privada no território se dê em direção à reprodução da desigualdade.

Embora ao longo da história das sociedades a informação sempre teve um papel importante em relação à afirmação das estruturas de poder, sua importância tem sido crescente. Uma contribuição teórica nesse sentido, elaborada por Milton Santos, propõe uma macroperiodização da relação do homem com seu meio em três grandes etapas: o meio natural, o meio técnico e o meio técnico científico informacional (SANTOS, 2002). Na primeira delas, a condição de coletor e extrativista impunha ao homem e às sociedades o tempo natural e o "homem escolhia da natureza o que era fundamental ao exercício da vida" (SANTOS, 2002). Com o tempo, os instrumentos de transformação do meio natural ganharam maior densidade técnica, as estruturas sociais se complexificaram e a capacidade de transformação da natureza se ampliou. As técnicas de produção agrícola mecanizada, o desenvolvimento dos meios de transporte como as ferrovias e os navios a vapor e a revolução industrial fizeram emergir um espaço mecanizado. Isso permitiu progressivamente às sociedades tanto a "transgressão das distâncias" como a sobreposição do tempo social em relação ao tempo natural. Esse processo, no entanto, era geograficamente circunscrito.

Contudo, o desenvolvimento das forças produtivas levou a um novo tipo de relação entre sociedade e espaço, marcado pela fusão progressiva da técnica com a ciência, impulsionadas principalmente a partir do final da segunda guerra mundial. Em seguida, a evolução das tecnologias relacionadas à microinformática, marcada pela formidável capacidade de processamento de dados e dos meios de comunicação, especialmente com as tecnologias de sensoriamento remoto e transmissões por satélite, elevou a capacidade de produção e difusão da informação em escala planetária. Marcadamente, os sistemas de informação fundidos com as tecnologias de comunicação passaram a caracterizar um meio técnico científico informacional. Nesse

âmbito, ciência, tecnologia e informação estão na base da produção e da utilização do território e requalificam os espaços para atender aos interesses hegemônicos da economia e da política (SANTOS, 2002).

Essa difusão, juntamente com processos de desregulamentação do capital financeiro, levou a um rápido processo de descentralização da produção sob estruturas de comando centralizadas (SASSEN, 1991). Para atender a essas funções, os territórios são equipados de forma que a informação circule. Porém, dentro de uma estrutura socioeconômica concentradora, o controle sobre amplas porções do globo requer um acesso seletivo às informações. Nesse sentido, Santos afirma que "controle centralizado e organização hierárquica conduzem à instalação de estruturas inegalitárias, já que a informação essencial é exclusiva e apenas transita em circuitos restritos". (SANTOS, 2002).

O crescente papel da informação nas estruturas concentradas de poder se estrutura, dessa forma, a partir de um processo econômico global há pelo menos três décadas. Há, no entanto, um elemento novo, mais recente, que provoca novas consequências e que se estrutura em duas vertentes. Por um lado, um sistema de objetos técnicos, constituídos por redes de fibra ótica, transmissores via satélite, antenas e distribuidores de sinais e, sobretudo dispositivos móveis, que difundidos em escala planetária, por todas as classes sociais, o que potencializa a capacidade de transmitir e, sobretudo, de coletar informações detalhadas de bilhões de pessoas. Por outro lado, uma estrutura monopolista de grandes corporações de tecnologias que dominam esse mercado. Segundo Taplin,

> O Google tem 88% de participação no mercado de publicidade vinculada a buscas, o Facebook (e suas subsidiárias Instagram, WhatsApp e Messenger) detém 77% do tráfego nas redes sociais, e a Amazon controla 74% do mercado de livros eletrônicos. (TAPLIN, 2017).

Quais as consequências disso? Qual o sentido dessa transformação para as relações políticas e econômicas que envolvem o território: ampliação da assimetria informacional na sociedade ou maior democratização da informação?

A resposta para essas indagações está nas possibilidades de construção de um robusto sistema público de informações. E aqui temos um cenário bastante desanimador. É cada vez mais difícil, dentro do cenário atual, investir em informação pública, isto é, aquelas produzidas por órgãos públicos e oficiais. Seja na qualidade delas, seja na sua captação, os investimentos têm se reduzido constantemente. Por um lado, à exceção do IBGE – que trabalha de forma pioneira e ousada na reformulação de suas pesquisas domiciliares – com a PNAD contínua, os institutos públicos

quase não promovem mais pesquisas amostrais. O último Censo registrou recorde de recusas a entrevistas, especialmente nas áreas mais ricas da cidade, em condomínios e prédios de luxo, justificadas por supostas questões de segurança.

A CONSTRUÇÃO DO GEOSAMPA: UM SISTEMA PÚBLICO DE INFORMAÇÕES

Os sistemas públicos de informação representam um importante vetor, se não o único, para buscar melhor simetria entre os agentes e atores que fazem a disputa das pautas urbanas. Evidentemente que se poderia pensar na regulação das grandes empresas de TICs, porém esse procedimento extrapolaria a escala nacional. O ambiente público municipal, pelo contrário, permite o acompanhamento e controle em relação aos objetivos, à difusão e à proteção da privacidade do cidadão contra usos políticos ou econômicos. Nesse ambiente, a decisão a respeito do uso das informações é sujeita ao controle social e, uma vez dado o acesso às informações disponíveis, elas se tornam públicas para todos os agentes, sem privilégios. Essa é uma questão central para o processo de planejamento e gestão urbana, uma vez que é exatamente o maior equilíbrio nas informações sobre o território que permite avançar no partilhamento dos processos decisórios sobre a cidade.

Porém as dificuldades são muitas. As limitações de mobilização de recursos públicos para realização de pesquisas ou mesmo para fortalecimento das instituições públicas que lidam com a informação são crescentes. A baixa capacidade de investimento dificulta, por exemplo, tornar as plataformas públicas mais amigáveis e atrativas para o público. Da mesma forma, que as carreiras públicas existentes ainda não se adaptaram às novas tecnologias, e, por conta disso, os entes públicos tem dificuldade da contratação de profissionais com o perfil adequado.

Assim, diante da impossibilidade de repetir o mesmo modelo e competir com o monopólio das gigantes multinacionais da informação, pelas limitações apontadas e tantas outras, qual o potencial de estruturar uma política de informações públicas? Se não há capacidade de investimento para novas e mais pesquisas, quais são os ativos nos quais uma política de informações públicas pode se apoiar? Entendemos necessárias três estratégias:

I. articular as diversas bases de dados existentes, oriundas dos registros administrativos;

II. mobilizar a colaboração da sociedade civil;

III. trabalhar com a adesão do setor privado.

A primeira estratégia é articular um grande ativo de informações para o setor público, resultado da ampla atribuição do Estado de exercer o controle ou gerenciar as atividades urbanas. Para cobrar impostos territoriais, para organizar a demandas habitacionais, para permitir a construção de novas edificações, para prestar benefícios sociais, o poder público tem que necessariamente realizar cadastros ou exigir que pessoas, empresas e organizações prestem informações compulsoriamente. Dado que o Estado está presente em quase todas as dimensões da vida social, o potencial de geração de informação é realmente gigantesco. A utilização dessas bases de forma integrada e consistente, porém, não é trivial. Tomando a Prefeitura do Município de São Paulo como exemplo, vemos que há uma grande pluralidade de órgãos que produzem sistemas distintos realizados em períodos distintos, com tecnologias e estruturas incompatíveis entre si e, muitas vezes, com sobreposição e duplicação de informações.

Para as informações imobiliárias urbanas, por exemplo, esse emaranhado se faz muito forte. O controle para tributação é um, a base para aprovação de projetos imobiliários é outra. Já o cadastro de assentamentos informais é estruturado também de forma apartada. Tudo isso combinado, muitas vezes, com a falta de uma cartografia precisa para referenciar todas essas informações. Mas, mais importante, é reconhecer que não se trata de uma situação criada espontaneamente. A desarticulação dos registros e das informações a respeito da informação urbana não é fruto do acaso, mas um contexto construindo institucionalmente como forma de solapar a capacidade do Estado, da esfera pública, em planejar e controlar as dinâmicas de perpetuação da desigualdade no contexto urbano.

> A sobreposição de sistemas e registros fundiários e a precariedade das bases cartográficas correspondentes não são apenas detalhes acidentais e muito menos falhas, mas sim parte importante da estrutura jurídico institucional de manutenção do *status quo* em termos de específica organização social, da qual um dos aspectos importantes é a inviabilidade do planejamento territorial por parte do Estado (BATTAGLIA, 1995).

A segunda estratégia é mobilizar a colaboração da sociedade para produzir informações de forma colaborativa. Evidentemente que o potencial é menor do que a entrega voluntária de dados pessoais que passamos para o monopólio das gigantes multinacionais da informação – que tem a seu favor o aspecto de "modernidade", o desenvolvimento tecnológico que é capaz de mobilizar e o pesado investimento em *marketing*. Porém, à medida que os governos forem capazes de fomentar a gestão compartilhada e participativa das cidades, o potencial de produção conjunta de dados com a sociedade civil pode se tornar uma realidade poderosa. Nesse

sentido, existem iniciativas contundentes que demonstram a capacidade de executar essa estratégia. No município de São Paulo, por exemplo, o MobiLab[2] estabeleceu uma política de abertura de dados relacionados ao transporte público e com isso conseguiu tanto fomentar o desenvolvimento de aplicativos que auxiliam o usuário desse serviço público, quanto, por meio desses aplicativos, obter informações relevantes que auxiliam o planejamento dos transportes. Outro bom exemplo é o Open Street Maps,[3] que permite a alimentação colaborativa em um tema de enorme complexidade que é a elaboração e manutenção de uma base pública de logradouros, sobretudo em metrópoles com grande incidência de informalidade urbana. Além disso, há instituições da sociedade civil que tem na informação o seu objeto de trabalho, como entidades de classe, sindicatos, organizações da sociedade civil, universidades, centros de pesquisa.

A terceira estratégia importante para fortalecer um sistema público de informações é trabalhar com a adesão do setor privado, voluntária em alguns casos ou compulsória em outros. Pode ser compulsória no caso das concessionárias de serviços públicos, prestadoras de serviço no espaço público ou mesmo no caso de aplicativos que tem na sua essência a utilização da cidade como plataforma. Nesse caso, além de trabalhar com normas e contratos que obriguem o compartilhamento dos dados, é preciso também ter na estrutura pública a capacidade de especificar formatos, monitorar o compartilhamento, condicioná-los às medições de serviços. A adesão voluntária, por sua vez, pode ocorrer no caso de empresas que possam ter algum interesse em ter a sua informação disseminada, o que pode ser relevante para alguns serviços. Para isso, pode ser importante estabelecer incentivos para que empresas possam alimentar os sistemas públicos de informação.

São precisamente como articuladoras dessas três estratégias que surgem iniciativas públicas de estruturação de infraestruturas de dados – Dados Abertos e Dados Espaciais. Essa foi a aposta da política de informações realizada na Prefeitura de São Paulo no quadriênio 2013-2016. Essas infraestruturas de dados se baseiam em três pilares. O primeiro é a padronização da informação e de sua gestão. O compartilhamento e a troca

2 O Mobi Lab é uma iniciativa da Prefeitura de São Paulo para "introduzir inovação e mudar o relacionamento da administração pública com tecnologia. Sua criação veio principalmente para melhorar a transparência e a qualidade e utilização dos dados brutos produzidos pela Secretaria de Transportes, CET e SPTrans". Ver: MOBILAD. Disponível em: <http://mobilab.prefeitura.sp.gov.br/>. Acesso em: 05 dez. 2018.

3 Ver: OPENSTREETMAP! Disponível em: <https://www.openstreetmap.org/#map=4/-15.13/-53.19>. Acesso em: 05 dez. 2018.

de informações requerem a convergência para normas e procedimentos relacionados à organização dos dados, elaboração de inventários de informações, realização de metadados e dicionários de dados. O segundo é a construção de fluxos de sincronização e conexão dos dados, a partir da construção de ferramentas que permitam o acesso simultâneo às diferentes fontes de informação. O terceiro é a constituição de uma base geoespacial relacional, que permita a convergência das informações a partir de uma referência comum.

Apostar em infraestruturas de dados, criando condições para uma gestão compartilhada e descentralizada dos dados, significa incorporar a experiência acumulada e percorrer um caminho distinto de iniciativas malsucedidas de construção de sistemas públicos de informação. Isto é, evitar a estruturação de um repositório único, a centralização das informações e a imposição de processos de gestão para diversos órgãos públicos e a sociedade civil. Na prática, no entanto, a opção descentralizada exige, mais do que grandes aportes tecnológicos, sinalização política. Essa sinalização aponta para três dimensões importantes:

I. a autonomia tecnológica;

II. a gestão descentralizada;

III. a política de dados abertos.

A autonomia tecnológica implica para o setor público a adoção do caminho do desenvolvimento interno, que pode ser combinado pela capacidade de assimilação – quando esse desenvolvimento for compartilhado – e pelo uso de tecnologias não proprietárias. Isso significa dizer que desenvolver uma infraestrutura deve vir junto com a capacitação de servidores público para a operarem. O uso de plataformas de código aberto, por sua vez, embora não seja condição essencial, pode ser estratégica uma vez que facilita a apropriação tecnológica – exatamente pelo fato de envolver coletivos que trabalham de forma colaborativa – e representam significativa redução de custos de licenças e de desenvolvimento.

Já a gestão descentralizada considera como benéfica a pluralidade na produção de dados sobre a cidade. A realidade da Prefeitura de São Paulo, que provavelmente é o contexto de muitas outras metrópoles brasileiras, é a de muitos órgãos, muitas secretarias produzindo suas informações e estabelecendo as suas prioridades. Se é fato que se trata de uma realidade que tende a aumentar os esforços de coordenação, a aproximação da geração de dados com as áreas fins enriquecem o acervo e facilitam o uso de informações no cotidiano da gestão pública. Por isso integrar sistemas, ao invés de eliminá-los, representa um fato mobilizador, além de ter a van-

tagem adicional de não centralizar o poder de informação, integrando e engajando os diversos órgãos públicos. Finalmente, é essencial uma política transparente de dados abertos. Além de ser um direito do cidadão, uma vez que os sistemas pertencem à esfera pública e não à privada, a ampla abertura de dados estimula o uso, a análise e o debate das escolhas sociais baseadas em evidências. Representa, ainda, uma estratégica de baixo custo para crítica e qualificação dos dados, uma vez que quanto maior for sua utilização, maior o retorno que os produtores terão a respeito de eventuais falhas, erros e lacunas.

Ao longo do quadriênio 2013-2016 a Prefeitura de São Paulo apostou na estratégia descrita e, a partir das premissas apontadas, construiu o GeoSampa. Trata-se de uma infraestrutura de dados municipais, baseada na integração de sistemas públicos de registros administrativos, desenvolvido em tecnologias de código livre e que disponibiliza em formato aberto todo o seu conteúdo. O GeoSampa possui hoje mais de 184 camadas de informações, de escopo temático bastante diversificado e sincronizado com diferentes plataformas de dados. O resultado é um amplo acesso público, com cerca de 70 mil visitantes por mês e uma série de trabalhos de pesquisa desenvolvido a partir dele. Foi a base também de uma política de dados abertos que teve como ponto representativo a abertura dos dados cadastrais imobiliários, tema da próxima seção. Sua ampla utilização pelo próprio setor público, setor privado – principalmente aqueles relacionados à incorporação imobiliária – e universidades garantiu a sua continuidade na mudança de gestão.

DADOS CADASTRAIS DE PROPRIEDADE URBANA: INFORMAÇÃO PÚBLICA OU PRIVADA?

Na sequência de um amplo processo de estruturação da infraestrutura municipal de dados espaciais e da infraestrutura municipal de dados abertos, uma decisão de abertura de informações cadastrais representou um marco importante entre os avanços da publicização de cadastros urbanos. Em dezembro de 2015, o decreto municipal 56.071 autorizou a divulgação para consulta das informações sobre a propriedade imobiliária na cidade de São Paulo. Os dados individualizados lote a lote passaram a ser consultados em diversos dos campos do cadastro, contendo tanto as informações relativas às suas dimensões físicas, como aquelas relacionadas aos seus proprietários. Essa iniciativa foi ainda fortalecida com o decreto 56.932 publicado em abril de 2016, que ampliou os campos a serem disponibilizados e, ainda, autorizou sua disponibilização integral em formato aberto. A inclusão desses dados em uma única base, no entanto, suscita o debate em torno da questão da privacidade dos dados pessoais.

Para avançar nessa discussão e desde um ponto de vista que defende a sua divulgação, é preciso compreender a natureza dos registros e dos cadastros que tratam da propriedade imobiliária. É preciso pontuar, de início, que, no Brasil, o registro é condição da existência de uma propriedade privada imobiliária. Diferentemente do registro de uma pessoa, por exemplo, a propriedade só existe quando reconhecida por um documento público. A organização dessas informações, no entanto, é problemática por vários motivos, notadamente por dois aspectos. Em primeiro lugar, os dados são imprecisos, porque não amparados em uma cartografia digital de boa acurácia. Em segundo lugar, são sobrepostos, porque oriundos de três fontes distintas e não integradas:

I. dos cadastros das prefeituras para fins tributários;

II. das matrículas dos cartórios de registro de imóveis;

III. nas escrituras de compra e venda, caso que é comum na realidade brasileira (BATTAGLIA, 1995).

As condições expostas a respeito da natureza das informações sobre a propriedade afetam também o acesso a elas, tornando-as opacas. A princípio, os registros cartoriais são públicos, porém onerosos a quem os solicita. Dessa forma, é a capacidade financeira dos agentes que determina a sua capacidade de extração dos dados cadastrais. Ou seja, há aqui uma grande assimetria de informação entre o Estado e a sociedade, entre os agentes privados e os movimentos sociais. Essa situação contribui para mascarar o papel da concentração da propriedade imobiliária como mecanismo de reprodução das desigualdades. Um bom exemplo trata da retenção especulativa dos imóveis urbanos: enquanto o Censo demográfico calcula mais de 290 mil imóveis vagos na cidade de São Paulo,[4] e o TPCL aponta para 13% da área cadastrada como não edificada, o Plano Municipal de Habitação[5] aponta para quase 400 mil domicílios o déficit habitacional da Cidade de São Paulo.

À medida que estudos e pesquisas elaboradas a partir da abertura dos dados cadastrais do IPTU vão surgindo, fica claro que a propriedade imobiliária é chave para entender e gerir a cidade, para construir justiça social. Essa leitura é reforçada pelo fato de que a utilização das bases não está sendo feita apenas pela academia, mas também por organizações da so-

4 [S.a]. Secretaria Municipal de Desenvolvimento Urbano. Vacância domiciliar cai 30% entre 2000 e 2010. *Informes Urbanos*, n. 23. São Paulo, 2014. Disponível em: <http://smdu.prefeitura.sp.gov.br/informes_urbanos/pdf/35.pdf>. Acesso em: 05 set. 2017.

5 [S.a]. Secretaria Municipal de Habitação. Plano Municipal de Habitação: caderno para discussão pública. São Paulo, 2016.

ciedade civil e pela imprensa. A primeira evidencia nesse sentido aparece em reportagem que aponta o nível de concentração dessas propriedades: 1% dos proprietários (22, 4 mil) detinham, em 2016, R$ 479 bilhões em propriedade, ou seja, 45% dos 1,7 trilhão do valor total de bens imobiliários no município de São Paulo (BURGARELLI; RIBEIRO; DUARTE; TOLEDO, 2016). Ao compararmos as informações de rendimentos extraídas do Censo/IBGE, na qual o mesmo estrato de 1% possui 20% da renda declarada,[6] percebemos o papel dos bens imobiliários na desigualdade urbana. Essa perpetuação da desigualdade fica clara também no plano da arrecadação tributária. Será que tamanha concentração de propriedade se reflete na cobrança progressiva dos impostos territoriais e urbanos? Um indício dessa questão apareceu em outra reportagem que, a partir das bases de dados publicadas, calculou o valor da isenção de IPTU para um segmento específico, as igrejas. Uma reportagem da *Folha de S.Paulo* mostrou que a renúncia de receita com os imóveis de propriedade das igrejas chegou a 110 milhões de reais por ano (MONTEIRO; RODRIGUES, 2016).

Ao mesmo tempo em que a propriedade de bens imóveis aprofunda e perpetua a desigualdade social e a regressividade na cobrança de impostos, também impõe um obstáculo para a promoção da igualdade de gênero. Esse aspecto ficou claro em estudo divulgado pelo portal NEXO que trouxe uma pesquisa ainda inédita sobre o tema, realizada por Priscila Spécie e Miguel Stevanato Jacob (LIMA, 2017). A pesquisa revelou que as mulheres, que são 52% da população, são proprietárias de apenas 33% dos imóveis na cidade. Mais do que isso, na medida em que caminhamos para as periferias de São Paulo, esse percentual diminui, ou seja, a desigualdade de gênero também é territorial. Finalmente, estudo desenvolvido por uma organização da sociedade civil apontou para o papel dos imóveis na possível ocultação de patrimônio.[7] Isso porque, no ano de 2016 na cidade de São Paulo, nada menos do que 3,4 mil imóveis estavam registrados em nome de empresas *off-shore*, isto é, abertas em paraísos fiscais e jurisdições secretas.

Dessa forma, apresentamos quatro estudos que avançaram em temáticas significativas da cidade:

I. concentração de propriedade;

II. renúncia fiscal;

III. desigualdade de gênero;

6 [S.a]. Secretaria Municipal de Desenvolvimento Urbano. Persiste a alta desigualdade de renda no Município de São Paulo. *Informes Urbanos*, n. 19, 2014. Disponível em: <http://smdu.prefeitura.sp.gov.br/informes_urbanos/pdf/32.pdf>. Acesso em: 05 set. 2017.

IV. corrupção e ocultação de patrimônio.

É também relevante destacar que a divulgação de informação identificada foi fundamental para alcançar esses resultados apresentados, ou seja, há um ganho social relevante em troca da perda de privacidade que a abertura provocou. Todos eles foram realizados após a abertura dos dados cadastrais do IPTU, ou seja, a política de abertura de dados contribuiu para debates relevantes para formulação de políticas urbanas que caminhem para uma cidade mais justa.

CONSIDERAÇÕES FINAIS

O presente capítulo pretendeu trazer a contribuição de uma experiência concreta para o debate acerca do papel das novas tecnologias da informação e da comunicação no âmbito da gestão das cidades. De maneira geral, procurou-se identificar que são necessárias mediações para trabalhar o debate a respeito das práticas englobadas sob o rótulo de cidades inteligentes no Brasil. Parece particularmente importante compreender o papel que as informações desempenham hoje como mecanismo de reprodução da desigualdade. Sendo assim, se há, por um lado, um grande potencial em reunir uma quantidade formidável de dados sobre as dinâmicas urbanas e assim fortalecer a capacidade de gestão e intervenção sobre as suas dinâmicas, por outro lado, é preciso ter como prioridade o caráter público e democratizante dessas informações.

Para que os benefícios de ampla coleta, armazenamento, processamento e análise de dados sobre as dinâmicas urbanas se dê no sentido do interesse público, é preciso que exista clareza e transparência sobre uma política de informações no plano municipal. E, para que isso se dê de forma a permitir o amplo controle social e a gestão pelo público, é necessário envolver o fortalecimento das capacidades estatais garante a autonomia da sociedade civil para, politicamente, definir os rumos e o sentido do uso da informação no âmbito da esfera pública. Caso contrário, serão crescentes os riscos de os sistemas serem pautados pela oferta do setor privado e, com isso, se tornarem descolados das realidades da administração municipal e da cidade como um todo.

Outro aspecto relevante do debate, para o qual intentamos trazer alguns elementos concretos, dizem respeito ao debate em torno da privacidade dos dados. Existem muitas dimensões sob as quais é possível abordar o tema, inclusive apontando para os riscos de o setor público e o privado comercializarem ou utilizarem os dados para monitoramento político

do cidadão. No entanto, no caso aqui citado a respeito das informações pessoais sobre a propriedade de bens imobiliários, a abertura de dados pessoais significa a possibilidade de decifrar uma dimensão estrutural de reprodução da desigualdade urbana, que não seria revelada de outra forma. Portanto, o princípio da privacidade deve ser ponderado por outros princípios tão relevantes quanto, como o da função social da propriedade. Deve proteger, em suma, o cidadão e não as formas desiguais de utilização da cidade.

Como apresentamos, a disponibilização de dados individualizados dos cadastros imobiliários já fomenta uma gama importante de estudos e reportagens que ajudam a desvendar o papel da propriedade imobiliária na reprodução das desigualdades urbanas. Há ainda, uma imensa gama de pesquisas que podem ser realizadas nesse sentido, por exemplo:

I. a respeito dos imóveis de propriedade do Estado, sua utilização e destinação;

II. sobre as isenções tributárias e a taxação do patrimônio imobiliário;

III. sobre a regulação da produção privada do espaço urbano em termos de distribuição dos beneficiários.

Dialogando com o conceito de cidades inteligentes, mais do que estruturar grandes investimentos em infraestruturas para *big data*, ou o desenvolvimento de aplicativos urbanos, a prioridade poderá ser a de estimular a formação de analistas, capazes de estruturar leituras desses dados que sirvam ao debate público na direção de uma cidade mais justa. A experiência do GeoSampa mostra que é possível mudar a forma pela qual a administração pública gerencia seus dados enfrentando inclusive, resistências ligadas à dinâmica da administração pública que pareciam intransponíveis. Afinal, para tomar como exemplo a cidade de São Paulo a tentativa que implementar uma solução de informação geográfica integrada remetia à gestão da Prefeita Luiza Erundina (1989-1992). Mais de duas décadas depois, foi possível avançar na estruturação da informação pública. É necessário agora aprofundar a abertura de dados – garantindo que o Estado tenha os recursos necessários para isso – e estimular que a sociedade se encarregue das análises e do debate público sobre as cidades.

REFERÊNCIAS

[S.a]. Secretaria Municipal de Desenvolvimento Urbano. Vacância domiciliar cai 30% entre 2000 e 2010. Informes Urbanos, n. 23. São Paulo, 2014. Disponível

em: <http://smdu.prefeitura.sp.gov.br/informes_urbanos/pdf/35.pdf>. Acesso em: 05 set. 2017.

[S.a]. Secretaria Municipal de Habitação. Plano Municipal de Habitação: caderno para discussão pública. São Paulo, 2016.

[S.a]. Transparência Internacional. São Paulo: A Corrupção Mora Ao Lado? Empresas Offshore E O Setor Imobiliário Na Maior Cidade Do Hemisfério Sul. Disponível em: <http://www.transparency.org/whatwedo/publication/sao_paulo_a_corrupcao_mora_ao_lado>. Acesso em: 05 set. 2017.

BATTAGLIA, L. *Cadastros e registros fundiários:* a institucionalização do descontrole sobre o espaço no Brasil. 1995. Tese – Fundação de Apoio Universitário, Universidade de São Paulo, São Paulo, 1995, p. 16.

BURGARELLI, R.; RIBEIRO, B.; DUARTE, G.; TOLEDO, J. R. "Um por cento dos donos de imóveis concentra 45% do valor imobiliário de São Paulo". O Estado de S. Paulo, 13 ago. 2016. Disponível em: <http://www.estadao.com.br/noticias/geral,1-dos-donos-de-imoveis-concentra-45-do-valor-imobiliario-de-sao-paulo,10000069287>. Acesso em: 5 set. 2017.

BYRNES, N. Cities Find Rewards in Cheap Technologies. In: MIT Technology Review Business Reports, jan./fev. 2015. Disponível em: <https://www.technologyreview.com/s/532466/cities-find-rewards-in-cheap-technologies/?set=532461>. Acesso em: 05 set. 2017.

EUROPEAN COMMISSION. EU SET-Plan: Strategic energy technology plan. Disponível em: <https://setis.ec.europa.eu/set-plan-implementation/technology-roadmaps/european-initiative-smart-cities e>. Acesso em: 05 set. 2017.

LIMA, J. D. Mulheres são minoria entre donos de imóveis em São Paulo. Por que isso é um problema. Disponível em: <https://www.nexojornal.com.br/expresso/2017/03/26/Mulheres-s%C3%A3o-minoria-entre-donos-de-im%C3%B3veis-em-S%C3%A3o-Paulo.-Por-que-isso-%C3%A9-um-problema>. Acesso em: 26 mar. 2017.

LUQUE-AYALA, A.; MARVIN, S. Developing a Critical Understanding of Smart Urbanism? *Urban Studies 2015*, v. 52, n. 12, p. 2105-2116, mar. 2015.

MAJCHER, K. Mapping Disaster in Jakarta. *MIT Technology Review Business Reports*, jan./fev. 2015. Disponível em: <https://www.technologyreview.com/s/532516/mapping-disaster-in-jakarta/?set=532461>. Acesso em: 05 set. 2017.

MAJCHER, K. Sensing Santander. *MIT Technology Review Business Reports*, jan./fev. 2015. Disponível em: <https://www.technologyreview.com/s/532536/sensing-santander/?set=532461>. Acesso em: 05 set. 2017.

MONTEIRO, A.; RODRIGUES, A. Isenção de IPTU a templos custa 22 creches por ano em São Paulo. Disponível em: <http://www1.folha.uol.com.br/cotidiano/2016/08/1800103-isencao-de-iptu-a-templos-custa-22-creches-por-ano-em-sao-paulo.shtml>. Acesso em: 8 ago. 2016.

MORAES, A. C. R. *Ideologias geográficas*: espaço, política e cultura no Brasil. 5. ed. São Paulo: Annablume, 2005.

MORAES, A. C. R.; COSTA, W. M. *A valorização do espaço*. 4. ed. Hucitec: São Paulo, 1999.

SANTOS, M. *Por uma geografia nova:* da crítica da geografia a uma geografia crítica. Edusp: São Paulo, 2002.

SASSEN, S. *The global city:* New York, London, Tokyo. Princeton: Princeton University Press, 1991.

SCOTT, B. How can cryptocurrency and blockchain technology play a role in building social and solidarity finance. *UNRISD Working Paper*, n. 2016, 2016. Disponível em: <http://www.unrisd.org/unrisd/website/document.nsf/(httpPublications)/196AEF663B617144C1257F550057887C?OpenDocument>. Acesso em: 05 set. 2017.

SÖDERSTRÖM, O.; PAASCHE, T.; KLAUSER, F. Smart cities as corporate storytelling. *City*, v. 18, n. 3, 2014.

TAPLIN, J. Não dá mais para ignorar danos causados pelo Google e Facebook. Folha de São Paulo, 25 abr. 2017. Disponível em: <https://jornalggn.com.br/noticia/nao-e-possivel-ignorar-os-danos-causados-por-google-e-facebook-por-jonathan-taplin>. Acesso em: 05 set. 2017.

THRIFT, N. The promise of urban informatics: some speculations. *Environment and Planning A 2014*, v. 46, p. 1263-1266, 2014.

SMART CITIES ALÉM DOS SENSORES: O USO DE DADOS PARA APROXIMAR GOVERNO E CIDADÃOS

PABLO CERDEIRA
RENAN MEDEIROS DE OLIVEIRA

INTRODUÇÃO

Com a reconfiguração da estrutura adotada pelos Estados ao longo do tempo, a relação entre governantes e governados também foi alterada. Atualmente, ela tem como um ponto de grande importância a utilização de dados produzidos pelos cidadãos e sobre eles. Em outras palavras, o governo deve estar apto a manejar dados relativos aos seus governados e sobre pontos que os afetam cotidianamente para manter uma interação salutar. Mais do que uma relação saudável, trata-se de um aspecto inerente à noção de democracia representativa: é preciso que os governantes tenham consciência das demandas dos cidadãos e pautem suas atuações para atendê-las, na medida do possível.

Diante disso, o presente estudo apresenta algumas experiências que ocorreram na cidade do Rio de Janeiro em que o governo se valeu de dados dos cidadãos para implementar políticas públicas, o que ocorreu por meio do Big Data – PENSA: Sala de Ideias, escritório de captura e processamento de dados da Prefeitura do Rio de Janeiro. No primeiro item, abordamos brevemente o fenômeno da crise democrática, seus aspectos interno – ligado à relação entre governantes e governados – e externo – ligado à relação entre as instituições de poder – e qual sua conexão com o uso de dados. No segundo, fazemos o estudo do caso do Rio de Janeiro, apresentando ações que foram tomadas com o uso de dados para implementar políticas públicas, como ocorreu nas medidas adotadas para diminuição dos casos de dengue na cidade. Por fim, tecemos algumas considerações sobre como as experiências de utilização de dados para a formulação de políticas públicas e para a melhoria da gestão estatal têm se mostrado de grande valia. Isso porque um dos fatores da insatisfação geral com o estado de coisas no cenário político é a falta de proximidade entre representantes e representados, e o uso de dados pode ser utilizado como forma de promover uma gestão da coisa pública eficiente e próxima do cidadão.

A CRISE DEMOCRÁTICA E O USO DE DADOS

Atualmente, vivemos em um cenário em que a atuação da administração pública é, em grande parte, baseada no modelo weberiano, pelo qual o Estado tem o monopólio do uso da força (WEBER, 1982, p. 98).[1] Esse conceito aparece em vários momentos na teoria de Weber, tanto no domínio exercido pelo líder sobre os membros da sociedade com base no poder carismático, quanto nas imposições do poder legal (WEBER, 1982, p. 97 *et seq.*).

No entanto, a estrutura de relação vertical entre Estado e sociedade em que a teoria weberiana se apoia, aparentemente, encontra dificuldades de se manter na atual organização social. Somente a título de exemplo, pode-se apontar as surpresas com a eleição americana de Donald Trump, com o Brexit (REDAÇÃO BBC BRASIL, 2016 e 2017) e com a eleição de Macron.

Esses acontecimentos parecem indicar que estamos vivendo em um momento de grande polarização, o qual tem, dentre as suas causas, a separação do modelo de Estado weberiano – focado na burocracia, na hierarquia, na gestão centralizada e na padronização com vistas a impedir a concessão de benefícios a amigos do rei – da prática das relações sociais – focada no compartilhamento de informações, no imediatismo e no individualismo. É preciso dar atenção ao fato de que um afastamento intenso do governo em relação às demandas específicas de grupos da sociedade pode levar a um cenário de tirania. Esse descompasso é um dos aspectos da crise global do modelo de representatividade democrática (ACKERMAN, 2000).

A falta de identidade dos cidadãos com os representantes eleitos foi crescendo ao longo do tempo, podendo-se citar alguns fatores que contribuíram para expandir a lacuna que há entre as vontades dos eleitores e dos candidatos eleitos, como a prosperidade econômica de parcela da população, que levou ao aumento de suas expectativas em relação ao governo; a democratização, que fez declinar o respeito às hierarquias e os padrões de deferência a superiores sociais; as crescentes pressões sociais por melhorias localizadas; a complexibilidade da gestão estatal; e o aumento das demandas sem o correspondente aumento da capacidade governamental de respondê-las (MIGUEL, 2005). A democracia contemporânea, porém, tem a ideia de funcionários eleitos investidos constitucionalmente para tomar decisões governamentais sobre a política como um de seus pontos fulcrais

1 "Hoje, porém, temos de dizer que o Estado é uma comunidade humana que pretende, com êxito, o monopólio do uso legítimo da força física dentro de um determinado território".

(DAHL, 2001; MANIN, 1997).[2] Sendo assim, a manutenção de um regime democrático deve passar, imprescindivelmente, por uma representação salutar, real e efetiva. Vale dizer, mecanismos procedimentais supostamente democráticos não são suficientes para legitimar a atuação estatal. Para além disso, são necessárias atuações concretas que vão ao encontro das vontades e das necessidades da população – que nem sempre são homogêneas – e que lhe dê voz no momento de elaboração das medidas a serem adotadas.

Uma das formas que pode ser utilizada para promover uma maior aproximação entre o governo e os cidadãos é o uso de instrumentos ligados a cidades inteligentes. Com isso, é possível criar planos de ação de longo prazo que transcendem o mandato eletivo, evitando que o eleitor seja ouvido apenas a cada quatro anos. É importante notar, porém, que a noção de *smart cities* vai muito além da utilização de sensores (CHOURABI, 2012).[3] Vale dizer, não basta o emprego de instrumentos que captem dados de trânsito, de educação e da rede de energia elétrica, por exemplo. Deve haver estudos posteriores de análise de dados e a aplicação prática de seus resultados através de políticas públicas que visem a melhoria da qualidade de vida da população.

Quando se pensa em cidades, essa crise parece ser ampliada. O professor Edward Glaeser (GLAESER, 2012), de Harvard, classifica as cidades como a maior das invenções humanas, porque foi nelas que houve um desenvolvimento satisfatório e em escalas adequadas para gerar todo o progresso que há atualmente, inclusive o tecnológico. A água encanada passou a ser possível, por exemplo, e o modelo de saúde pública e universal prosperou. Em resumo, toda a estrutura econômica e de governo que temos hoje nasce das cidades, e não dos países, os quais são construções artificiais bastante posteriores à invenção daquelas.

É preciso observar que é também nas cidades que as pessoas, de fato, habitam. Em geral, os cidadãos não procuram o presidente ou um governador para resolver seus problemas diários. Eles recorrem aos prefeitos, que é a quem se cobra quando, por exemplo, há um buraco na rua ou um poste apagado. Mesmo no caso de questões que não são de responsabilidade do município, questiona-se o prefeito, que está a frente de quase todos os problemas cotidianos.

---

2 Manin afirma que a ideia de governo representativo abrange tanto mecanismos democráticos como não democráticos.

3 Ainda não há uma conceituação uníssona de *smart cities*, mas, em geral, os autores destacam a utilização de dispositivos inteligentes para otimizar os recursos e fazer com que a gestão governamental seja dotada de mais eficiência.

A sociedade, no entanto, não costuma se comportar tão harmoniosamente, tal como um grupo coeso que busca o desenvolvimento em conjunto, não sendo raro que a interação entre o indivíduo e a sociedade seja norteada por uma lógica egoísta. Tendo em vista essa polarização, ao se tratar de *smart cities*, é necessário pensar não apenas no uso de novas tecnologias e dados, mas também em como podemos empregar tais recursos para transformar essa interação, que coloca a administração pública de um lado e o cidadão do outro. A adoção de tecnologias de cidades inteligentes deve envolver uma contribuição para o desenvolvimento das cidades, para uma gestão estatal mais transparente e a promoção e aproximação entre governo e cidadãos.

O ASPECTO EXTERNO DA CRISE DEMOCRÁTICA: AS RELAÇÕES ENTRE GOVERNANTES E GOVERNADOS

A crise democrática enfrentada por todo o Ocidente é tema de amplo debate global. Estudos apontam que o percentual de pessoas que acreditam ser essencial viver em uma democracia cai de 72% para 30% quando comparados os nascidos antes da II Guerra Mundial e os *millennials* – nascidos após 1980 – nos EUA (MOUNK; FOA, 2017). O mesmo fenômeno foi registrado também, em menor escala, em diversos outros países – Austrália, Grã-Bretanha, Holanda, Nova Zelândia e Suécia –, de acordo com o mesmo estudo.

Surpresas – ou não tão surpresas assim – como as vitórias do Brexit e de Trump, com sua posterior vertiginosa queda em popularidade (AGÊNCIA EFE, 2017), demonstram a existência de um grande abismo entre os anseios da sociedade e o reconhecimento de sua representatividade na classe política. Curiosamente, boa parte dos casos de sucesso eleitoral citados anteriormente creditam seu desempenho ao uso de grandes volumes de dados antes das eleições. O *big data* entrou definitivamente nas campanhas eleitorais, mas não vai além, não fazendo parte dos governos que se formam posteriormente. O resultado não poderia ser outro: logo após as eleições, os candidatos que se valeram do *big data* tendem a sofrer vertiginosas quedas em suas popularidades. Isso pode ser registrado nos casos de Macron, Trump, Doria, entre outros.

O *big data* parece ter ajudado na construção de discursos específicos, para grupos bastante bem delimitados. Ele aproxima o candidato dos anseios particulares de cada pequeno grupo social. Contudo, ao permanecer apenas no discurso e não adentrar na gestão instaurada logo após as eleições, parece criar o efeito contrário, afastando ainda mais rapidamente o eleitor

do político eleito. As promessas genéricas de antes tornam-se promessas personalizadas, direcionadas para cada indivíduo. Mais específicas, portanto. O sentimento de traição ou abandono por parte do eleitor parece ganhar ainda mais destaque nesse cenário.

Há inúmeras razões para sustentar o afastamento dos governos do uso de grandes volumes de dados, a começar pelas denúncias de usos indevidos e abusivos por Edward Snowden. Entretanto, mesmo diante de casos de abusos como os diversos que já alcançaram o conhecimento público, é preciso reconhecer que dados gerados por nossa sociedade não podem ser desconsiderados como valiosas referências não apenas para a comunicação com os eleitores – como realizado durante as campanhas eleitorais –, mas também para o desenho de políticas públicas que melhor respondam aos interesses da sociedade. E, como já está claro pelo que se observa das campanhas que se valem dessas técnicas para personalização, não se pode mais falar de interesses da sociedade, de forma genérica. É preciso falar de interesses de pequenos grupos, bastante bem identificados e que, formados de baixo para cima, compõem o vago "interesse da sociedade".

Dados massivos já são largamente utilizados por grupos privados para melhor atender seus clientes (DONEDA, 2006). Ao buscar uma passagem aérea, ou um hotel, por exemplo, sistemas atuais são capazes de entender o perfil do usuário e personalizar a apresentação de ofertas. As notícias que nos dias de hoje nos chegam através de redes sociais são filtradas e adaptadas às nossas demandas, mapeadas com o uso intensivo de dados. Não há mais a melhor agência de viagem, assim como não há mais o melhor jornal. Há o melhor sistema de sugestão de hotéis ou o melhor sistema de seleção de notícias para o usuário.

Talvez tenha chegado o momento de os governos se repensarem a partir dessa mudança de paradigma. Não se trata mais de escolher o melhor governante ou plano de governo para toda a sociedade, mas aquele que melhor saiba se utilizar dos recursos disponíveis para entregar o melhor gerenciamento para cada cidadão e, assim, construir de baixo para cima a melhor gestão.

Não se discute mais o quão úteis e poderosos podem ser os dados que produzimos e dispomos atualmente. Tais dados, se bem utilizados, permitem um conhecimento muito mais profundo e dinâmico de nossa sociedade – ou dos consumidores – e, consequentemente, contribuem para o desenho de políticas públicas – ou campanhas de *marketing* – que melhor atendam a cada pequeno e específico grupo. Essas técnicas são de grande valia não apenas para governantes, mas também – e principalmente – para a sociedade, em especial em momentos de grande insatisfação desta para com aqueles.

É preciso, portanto, encontrar um equilíbrio, vale dizer, um caminho que permita ao Estado utilizar-se desse grande ativo gerado pela sociedade consolidado nos dados ao mesmo tempo em que garantias e direitos individuais são respeitados. Essa não é uma tarefa fácil, a começar pelo fato de que grande parte dos dados gerados pela sociedade está nas mãos de empresas privadas. Assim, os temas desse debate passam, obrigatoriamente, pelos direitos das empresas e dos consumidores. Passam também por aspectos técnicos, como uma correta definição de propriedade dos dados, que podem, eventualmente, receber a classificação de dados de interesse público; ou novos modelos de contratos entre Estado e setor privado para compartilhamento dos dados.

Diante disso, o aspecto externo, que relaciona governo e governados, é a faceta mais visível da chamada crise democrática, mas não é a única.

O ASPECTO INTERNO DA CRISE DEMOCRÁTICA: AS RELAÇÕES ENTRE AS INSTITUIÇÕES DE PODER

Outro aspecto da crise democrática é o que podemos denominar de interno, que diz respeito à relação entre as instituições de poder. Apesar de complexa, pelo menos uma de suas facetas – a relação entre Poder Executivo e Poder Legislativo –, tornou-se bastante conhecida do público em geral, especialmente nos últimos anos. Por vezes, assume caráter de dependência ou submissão, o que é verdade em todas as esferas: municipal, estadual e federal. Em situações extremas, como nos casos dos impeachments de Fernando Collor de Mello e Dilma Rousseff, o enfraquecimento do Chefe do Executivo permitiu até mesmo a sua remoção do cargo pelo Legislativo.

Nos casos de Poder Executivo extremamente fraco, com o objetivo de manter um mínimo de governabilidade ou garantir a própria continuidade no cargo, a realização de concessões, para além do desejável, ao Legislativo, pode ser a opção mais convidativa, se não a única. A depender do grau de influência do Legislativo sobre o Executivo, o resultado pode ser a captura deste por aquele, tal como ocorre com agências reguladoras em relação às empresas reguladas. Vem desse modelo a concessão de ministérios – ou secretarias, nos âmbitos estadual e municipal – e outros cargos estratégicos para indicados pelo Legislativo. Esse padrão é conhecido como presidencialismo de coalizão (ABRANCHES, 1988; FREITAS, 2016)[4] e poderia ser melhor identificado como governismo de coalização, para abarcar as demais esferas.

4 A expressão "presidencialismo de coalizão" foi utilizada por Sérgio Abranches em artigo de 1988 e desde então tem se difundido na doutrina.

É preciso destacar que tal composição entre os Poderes Executivo e Legislativo é frequente nas democracias da América Latina, da África e do Leste Europeu que adotam o presidencialismo (FREITAS, 2016), modelo representativo em que o poder deve ser compartilhado. É o modelo escolhido pelo nosso legislador para evitar que os Chefes do Executivo tornem-se déspotas ou que vivamos a tirania da maioria, conforme alertou Tocqueville (TOCQUEVILLE, 2005). O problema não está, portanto, na composição entre Legislativo e Executivo, mas, sim, na perda de controle, por parte do Chefe deste Poder, dos rumos de seu governo.

Para se prevenir contra esse desequilíbrio de forças, é importante que o Chefe do Executivo: I. mantenha apoio popular durante todo o mandato; II. detenha profundo conhecimento sobre problemas que afetam os cidadãos sob sua gestão; III. consiga medir, com eficiência, os impactos das medidas tomadas pelos seus ministros ou secretários. De fato, os três aspectos listados são intimamente relacionados e interdependentes. Há exceções, mas a manutenção hígida de um plano de governo não se sustenta sem esse tripé. A ausência de qualquer um deles pode resultar em um governante refém do Legislativo e de seus secretários ou ministros.

Para além do caso clássico em que o governante perde apoio popular e fica dependente do Legislativo, o fenômeno da captura pode ocorrer também de duas outras formas, conforme os três aspectos citados acima. A primeira delas se verifica quando o Chefe do Executivo não tem pleno conhecimento das demandas da sociedade. É com base em tal conhecimento que o governante dita sua agenda pública e segue seu plano de governo. Quando secretários ou ministros tornam-se os responsáveis pela interlocução, em suas áreas, com a população ou com grupos de interesses, passam a definir a pauta do Executivo. O poder do Chefe do Executivo, consequentemente, esvazia-se. Secretários ou ministros tornam-se os filtros através dos quais o governante enxerga os cidadãos, podendo colorir as lentes conforme seus próprios interesses. Da mesma forma, a disputa entre secretários ou ministros pelos recursos disponíveis transmuda-se e reduz-se, facilmente, para uma simples disputa interna de poder. Secretários ou ministros com maior influência conseguem maior participação na batalha por recursos.

A segunda maneira apresenta-se nas situações em que o Chefe do Executivo se enfraquece quando, mesmo tendo apoio popular e conhecimento das demandas da sociedade, não é capaz de verificar os impactos das medidas implementadas pelos seus secretários ou ministros. Neste cenário, mesmo sabendo o que precisa ser feito e como melhor alocar os recursos, o governante não tem condições de avaliar, de forma independente, a execução de seu projeto por parte de seus representantes. Corre,

também neste caso, o risco de captura por parte de outros Poderes, em especial pelo Legislativo.

Assim, conhecer as reais demandas da sociedade no maior nível de detalhamento e segmentação possível e conseguir acompanhar a implementação de seu plano de governo são elementos fundamentais para a manutenção de relação independente entre o Executivo e o Legislativo.

Neste cenário, os dados também desenvolvem papel fundamental. Em especial, dados gerados pela própria sociedade, sujeita ao administrador público, são fundamentais para que o gestor consiga entender a dinâmica social e como a população tem percebido os problemas e recebido as medidas tomadas pelos secretários e ministros.

O EXEMPLO DO RIO DE JANEIRO: POLÍTICAS PÚBLICAS BASEADAS EM DADOS

Em 2013, a cidade do Rio de Janeiro preparava-se para a Copa do Mundo de 2014 e para as Olimpíadas de 2016. Tais eventos não se realizaram isoladamente. Foram acompanhados de eventos preliminares, como a Copa das Confederações, eventos testes das Olimpíadas, grandes shows, visita do Papa e a Jornada Mundial da Juventude, eventos que, aproveitando-se da repercussão que os eventos principais traziam, buscaram o Rio de Janeiro como seu local de realização. Somado a tudo isso, os já tradicionais eventos da cidade também receberam grandes incrementos de público, como o Réveillon e os blocos de Carnaval.

O contexto histórico também exigia diversas ações paralelas, como grandes mudanças viárias, tendo em vista o lançamento das bases para um novo plano de desenvolvimento para a cidade no longo prazo. Exemplos podem ser percebidos com a realização de obras que, pela primeira vez na história do Rio de Janeiro, estimularam o desenvolvimento das áreas mais centrais, em termos geográficos, e a criação de conexões norte-sul, em contraposição ao movimento leste-oeste que sempre pautou a cidade. Listando apenas algumas das ações estratégicas realizadas, temos a substituição da Perimetral pelo Túnel Marcello Alencar, com revitalização da Zona Portuária e redução do tempo da ligação norte-sul – pelo lado leste –; a criação do Parque Madureira – no centro geográfico, para estimular o desenvolvimento local –, acompanhado da escolha de Deodoro como parque olímpico, e a construção da Transcarioca e da Transolímpica – visando à criação do movimento norte-sul pelo centro geográfico da cidade –; e também ações no extremo oeste, com o Túnel da Grota Funda e o

BRT Transoeste, que reduziram o tempo de ligação entre o norte e o sul em mais de 30 minutos para 10% do tempo original.

Importante observar que para além de seu crescimento desordenado ao longo de décadas, o Rio de Janeiro ainda enfrenta o desafio de sua geografia, já que o desenvolvimento econômico da cidade deu-se ao longo da costa, iniciado pelo Centro, em sentido à Zona Sul, e a área com maior desenvolvimento econômico foi sempre isolada: ao sul pela costa marítima e ao norte pelos maciços da Tijuca, da Pedra Branca e de Gericinó, este último separando o município do Rio de Janeiro dos municípios da Baixada Fluminense. Inclua-se nos desafios a presença de lagoas como a Rodrigo de Freitas e todo o complexo lagunar da Barra da Tijuca.

O grande desafio posto era, portanto, realizar todas as grandes mudanças pelas quais passaria a cidade, atendendo às demandas sempre crescentes dos cidadãos e gerando o mínimo possível de impactos e os maiores benefícios. Some-se a isso a necessidade de o Chefe do Executivo enfrentar as duas crises democráticas citadas acima: a externa, perante a população, e a interna, diante do Legislativo. Esse aspecto, muitas vezes relegado, será de importância crucial no posterior modelo de gestão que se valerá de dados.

No campo prático, como forma de manter sua independência do Legislativo e atender às reais demandas da sociedade, o prefeito desenvolveu iniciativas que, apesar de parecerem muito distintas entre si, traziam em sua essência o mesmo objetivo. As medidas adotadas foram: I. a criação da Central 1746, canal único e exclusivo para solicitações dos cidadãos; II. a criação do Centro de Operações Rio – COR; III. a criação do primeiro escritório de dados para políticas públicas do Brasil, o Big Data: PENSA - Sala de Ideias.

A Central 1746 foi criada com o objetivo de facilitar o envio de demandas por parte dos cidadãos. Mas, para além disso, desempenhou outros papéis importantes para o Chefe do Executivo. Permitiu que o prefeito entendesse e pudesse comparar, com números e outros dados objetivos, quais eram as maiores demandas dos cidadãos. Ao invés de se fiar exclusivamente em informações fornecidas pelos secretários responsáveis por cada pasta, o prefeito detinha condições de, ele mesmo, identificar quais questões estavam gerando mais insatisfação entre a população do Rio de Janeiro. Para além disso, a existência de uma central única para onde todas as demandas relacionadas à gestão municipal deveriam ser direcionadas tornou menos efetiva as atuações de grupos de influência. De posse de dados reais gerados pela população o prefeito tinha condições de, de fato, identificar se as demandas por podas de árvores, por exemplo, eram superiores às demandas relacionadas a estacionamentos irregulares. E mais, conseguia

saber qual a população mais afetada por um ou por outro problema, melhor direcionando, assim, os recursos públicos.

O Centro de Operações Rio, um dos maiores do Hemisfério Sul, também cumpriu papel semelhante. Centralizando mais de vinte órgãos municipais, estaduais e empresas prestadoras de serviços públicos, permitia acesso transversal do Chefe do Executivo às equipes operacionais. Diversos casos complexos, que ocorrem no dia a dia de qualquer grande cidade, demandam a integração de múltiplos órgãos para sua solução. Um exemplo real: um caminhão desgovernado atropelou pessoas, derrubou postes e invadiu um prédio, deixando-o sob risco de desmoronamento. A solução a tempo desse problema envolvia órgãos de saúde, de trânsito, da defesa civil, de transporte público e até mesmo concessionárias de água, gás e energia elétrica, uma vez que a fiação rompida ameaçava gerar explosões com o vazamento de gás. Assim, a existência de um Centro de Operações, para além de trazer maior agilidade, permitia ao prefeito a tomada de decisões e a emissão de ordens diretamente com as equipes técnicas e de campo, algo que seria quase impossível em um modelo em que o Chefe do Executivo precisa dialogar através de secretários.

Por fim, como forma de integrar dados de diversas origens distintas – gerados pela própria prefeitura, pela sociedade e por empresas privadas – foi criado o Big Data – PENSA: Sala de Ideias, que será melhor tratado a seguir.

O PRIMEIRO ESCRITÓRIO DE BIG DATA PARA POLÍTICAS PÚBLICAS DO BRASIL

O Big Data – PENSA: Sala de Ideias, escritório de captura e processamento de dados da Prefeitura do Rio de Janeiro, foi criado pelo Decreto nº 37.215, de 2013. Buscou-se desenvolver novos métodos para o desenho de políticas públicas, projetos e tomada de decisão que tivessem como principal fonte a real demanda da sociedade carioca, muitas vezes escondida, velada, e que só se manifestava quando da análise de grandes volumes de dados. Foi o primeiro escritório de *big data* do Brasil, inspirado pelo Mayor's Office of Data Analytics (MODA), de Nova York, criado logo antes pelo prefeito Michael Bloomberg.

O escritório tinha como premissa o entendimento de que, diante das crises externas e internas da democracia, o poder público precisava experimentar novos modelos – e o uso de dados, como já exposto acima, é elemento indispensável para a construção de um novo paradigma de democracia, que ainda estamos começando a esboçar.

Assim, na cidade do Rio de Janeiro, alguns estudos já foram desenvolvidos com base em mecanismos de *smart cities*. Projetos ligados a dados de trânsito e espalhamento de doenças, por exemplo, foram realizados para que o governo pudesse pautar sua atuação com base nas necessidades reais dos cidadãos e nas áreas que precisam de intervenção mais urgente. Com isso, aumenta-se a eficiência na gestão da coisa pública, diminui-se o espaço entre governo e cidadãos e melhora-se a qualidade de vida destes. Outro exemplo do uso de dados no Rio de Janeiro foi o uso de informações coletadas pelo aplicativo Waze, as quais foram utilizadas para modificar a maneira pela qual a prefeitura se relacionava com o cidadão e como esse se relacionava com a prefeitura (ÇOLAK; LIMA; GONZÁLEZ, 2016; GONZÁLEZ; XU, 2017; DIAS, 2016). A administração municipal carioca estabeleceu um convênio com o Waze – aplicativo que já tem, inclusive, mudado a forma como as pessoas dirigem em algumas cidades –, que utiliza os dados de motoristas para realizar alterações nas vias públicas.

A seguir, são expostos alguns casos – como os relativos a água, espalhamento de doenças, arrecadação e alocação de alunos – em que o Big Data: Pensa – Sala de Ideias utilizou dados produzidos pela população da cidade para a elaboração de políticas públicas.

O CASO PERIMETRAL

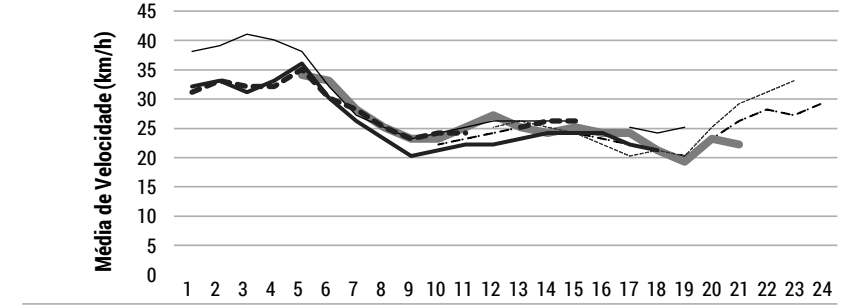
Um dos estudos desenvolvidos pelo projeto Pensa foi o relativo aos impactos causados na mobilidade urbana da cidade em decorrência da substituição da Perimetral. Foram utilizados dados GPSs de ônibus da frota municipal –horário de informe, número do carro, número da linha, velocidade instantânea, latitude e longitude – e do aplicativo Waze durante o período de 26 de setembro a 05 de novembro de 2013.[5]

No que diz respeito aos dados dos mais de 8 mil ônibus que compuseram o estudo, foram utilizados dois tipos distintos de médias: I. médias de velocidades de deslocamento, por meio das quais se analisa a velocidade de movimentação, e não a velocidade de cada ônibus; II. médias mínimas de velocidade. A média de deslocamento dos ônibus em toda cidade não sofreu grandes impactos por conta do fechamento da Perimetral. A média de velocidade de deslocamento dos ônibus na área de 6 km de lado no entorno do elevado, que foi a mais afetada de forma direta pelas mudanças realizadas, não foi impactada de forma significativa: houve uma redução

5 Houve interrupções parciais nas coletas de dados devido às adaptações iniciais dos sistemas.

em apenas 1,6 km/h. O gráfico a seguir indica esta média, cujo cálculo não envolveu velocidades iguais a zero:

Figura 1 – Média de velocidade dos ônibus às segundas – Valores de velocidade instantânea maiores do que zero no entorno da Perimetral

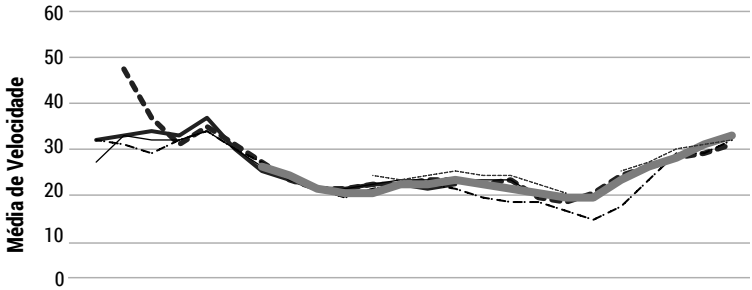


	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
30/10/2013										22	23	24	25	24	24	23	22	21	20	23	26	28	27	29
07/10/2013					34	33	28	25	23	23	25	27	25	24	25	24	24	21	19	23	22			
14/10/2013					24				24			25	26	25	24	22	20	21	20	25	29	31	33	
21/10/2013	38	39	41	40	38	32	27	25	23	24	25	26	26	26	26		25	24	25					
28/10/2013	31	33	32	32	35	30	28	25	23	24	24		25	26	26									
04/11/2013	32	33	31	33	36	30	26	23	20	21	22	22	23	24	24	24	22	21						

Fonte: Pensa - Sala de Ideias. Elaboração própria.

O cálculo das médias de velocidade considerando registros de velocidade igual a zero até às 19h20 do dia 4 de novembro de 2013 mantém o mesmo quadro. A média de velocidade de deslocamento foi reduzida em apenas 1,4 km/h. Confira-se:

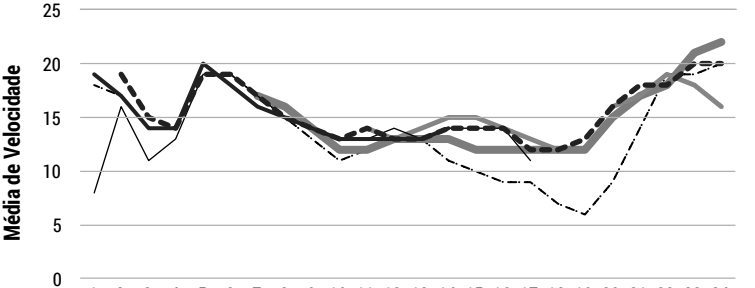
Figura 2 – Média de velocidade dos ônibus na Região da Perimetral às terças-feiras (excluindo registros com velocidades iguais a 0)



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
01/10/2013	33	32	30	33	35	31	28	24	22	20	22	23	23	22	20	19	19	17	15	18	24	30	30	33
08/10/2013							27	25	22	21	21	23	23	24	23	22	21	20	20	24	27	29	32	34
15/10/2013	31										25	24	25	26	25	25	23	21		26	28	31	32	33
22/10/2013	28	34	33	33	35	31	27	24	22	22	23	24	24	24	24	24	20							
29/10/2013		49	38	32	36	32	28	24	22	22	23	23	24	24	23	24	20	19	21	25	27	29	30	32
05/11/2013	33	34	35	34	38	31	26	24	22	22	23	23	22	23										

Fonte: Pensa - Sala de Ideias. Elaboração própria.

Figura 3 – Média de velocidade dos ônibus na Região da Perimetral às terças-feiras (incluindo registros com velocidades iguais a 0)



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
01/10/2013	18	17	14	14	19	19	17	15	13	11	12	13	13	11	10	9	9	7	6	9	14	19	19	20
08/10/2013							17	16	14	12	12	13	13	13	12	12	12	12	12	15	17	18	21	22
15/10/2013	9										14	13	14	15	15	14	13	12		16	17	19	18	16
22/10/2013	8	16	11	13	19	19	17	15	14	13	13	14	13	14	14	14	11							
29/10/2013		19	15	14	19	19	17	15	14	13	14	13	13	14	14	14	12	12	13	16	18	18	20	20
05/11/2013	19	17	14	14	20	18	16	15	14	13	13	13	13	14										

Fonte: Pensa - Sala de Ideias. Elaboração própria.

Dessa forma, de acordo com a metodologia adotada, a média de velocidade reduzida no dia 4 de novembro de 2013 foi entre 1,4 e 1,6 km/h, ou seja, entre 7 e 10%. Neste mesmo dia, o horário de maior impacto foi entre 8h e 11h, quando houve redução da média de velocidade dos ônibus em 3,6 km/h, ou seja, inferior a 15%. No final do dia, entre 21h e 23h, a velocidade dos ônibus estava superior à média em até 10%.

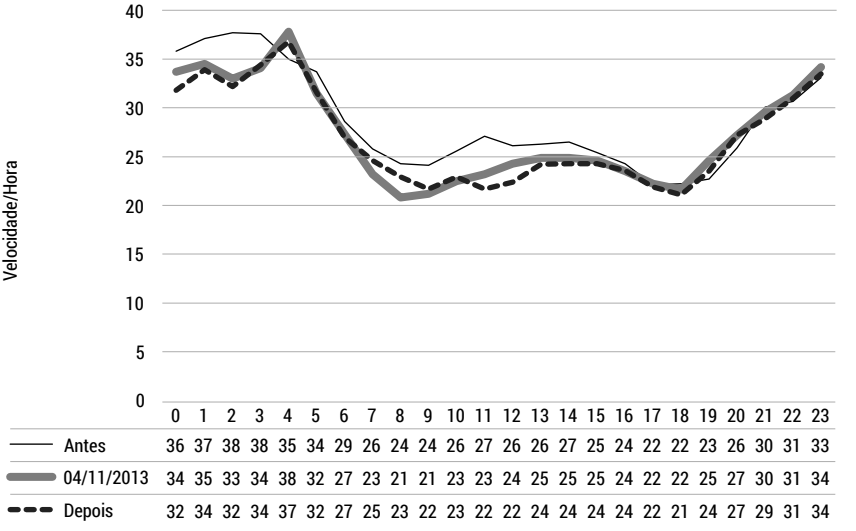
Já no segundo dia, 5 de novembro de 2013, independentemente do critério para cálculo da média de velocidade dos ônibus, não houve mais qualquer impacto nas médias de velocidade em comparação aos mesmos dias em semanas anteriores no entorno da Perimetral (dias 1, 8, 15, 22 e 29 de outubro). De fato, em alguns horários (entre 9h e 11h) a média de velocidade dos ônibus foi até mesmo superior ao histórico das últimas 5 semanas (até 10%).

Como mencionado, o estudo também se serviu de dados do aplicativo Waze para analisar os impactos da substituição da perimetral. Foram utilizados *reports* realizados pelos usuários e houve mais de 156.795 informes no período objeto da pesquisa.

No dia 4 de novembro, houve crescimento no registro de reclamações do tipo "Condições de Trânsito" por toda a cidade, com grande concentração às 8h, horário em que as reclamações aumentaram em quase 3 vezes. Fora dos horários de pico, os informes deste tipo ficaram dentro do normal. Já no dia 5 do mesmo mês, o impacto foi praticamente dentro da média das últimas 5 terças-feiras. O pico maior foi às 8h, quando esteve 20% acima da média. Contudo, no pico da tarde, entre 18h e 19h, as reclamações foram 280% acima do normal. O aumento mais expressivo nos relatos do Waze em razão da substituição da perimetral deu-se, no primeiro dia, em áreas específicas da cidade, como Maracanã, Largo da Segunda-Feira e Avenida Menezes Cortes, na região de Vila Isabel. No segundo dia, por sua vez, não houve comportamento fora do esperado em relação às terças-feiras anteriores. Algumas regiões apresentaram menor número de *reports*, como Linha Amarela, Linha Vermelha e Avenida Brasil.

Por fim, o estudo demonstrou que a velocidade média no entorno da Perimetral teve impactos muito baixos. A partir da comparação das velocidades médias nas quatro semanas anteriores e posteriores ao fechamento para testes, concluiu-se que o horário mais afetado negativamente foi o das 8h; o horário das 18h foi influenciado de forma positiva, com ganhos de velocidade. Contudo, o impacto para aqueles que circulam de carro é quase imperceptível. Confira-se, a título de exemplo, o gráfico referente à velocidade do dia 4 de novembro de 2013:

Figura 4 – Segunda-feira



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Antes	36	37	38	38	35	34	29	26	24	24	26	27	26	26	27	25	24	22	22	23	26	30	31	33
04/11/2013	34	35	33	34	38	32	27	23	21	21	23	23	24	25	25	25	24	22	22	25	27	30	31	34
Depois	32	34	32	34	37	32	27	25	23	22	23	22	22	24	24	24	24	22	21	24	27	29	31	34

Fonte: Pensa - Sala de Ideias. Elaboração própria.

O CASO DA AVALIAÇÃO DOS CUSTOS DE ENGARRAFAMENTOS

Para além do desmonte do Viaduto da Perimetral, o projeto Big Data: Pensa – Sala de Ideias também fez uso dos dados do Waze para localizar onde estão os engarrafamentos na cidade do Rio de Janeiro, identificando as trinta principais áreas da cidade nas quais esse problema é mais frequente. A análise indicou que 26% dos engarrafamentos são concentrados em determinados pontos principais, como no Centro da cidade e em bairros da Zona Sul, como Copacabana, representando um desperdício de 5.2 bilhões de reais.

A partir desses tipos de dados, o projeto começou a criar escalas: quanto custa cada um, quantas pessoas estão em cada engarrafamento, quanto tempo se está perdendo em cada engarrafamento, sendo possível, através dos dados do aplicativo, criar listas bem detalhadas para comparar os problemas da cidade e resolver os que mais afetam os cidadãos. Isso é de suma importância para que a decisão do administrador não seja uma decisão tomada apenas em razão de promessas feitas quatro anos antes.

Essas informações podem ser utilizadas para outras finalidades, tal como para definir investimentos, determinando com mais precisão quanto custa uma solução para o engarrafamento e em quanto tempo ela será paga.

Isso deve ser feito em relação a todos os pontos de engarrafamento. Esse método pode ser empregado para replanejar as áreas que os caminhões percorrem para jogar entulhos, por exemplo, pois são os mesmos dados já utilizados pelo aplicativo, mas sendo reaproveitados.

Com o uso desses dados, consegue-se um melhor planejamento urbano, colhendo novos locais para áreas de transferência que, ao mesmo tempo, cubram os pedidos e evitem os engarrafamentos, e não contribuam para seu agravamento. Confira-se a tabela a seguir:

Figura 5 – As 30 regiões mais engarrafadas no Rio de Janeiro

NOME	ALERTAS ENGARR.	% TOTAL ALERTAS	KM VIAS	% KM CIDADE	DENSIDADE (100m2)	CUSTO (R$ MI)
Lagoa-Barra	73,086	6.44	31.28	1.26	2.87	R$ 1,280.48
Bicalho – Vd. Eng. Freyssinet	48,033	4.23	31.00	1.25	4.21	R$ 841.06
Avenida Brasil com Linha Amarela	22,676	2.00	17.17	0.69	3.24	R$ 397.66
Pinheiro Machado – Presidente Vargas	15,775	1.39	14.91	0.60	2.59	R$ 276.38
Lagoa – Rebouças	14,648	1.29	8.43	0.34	3.66	R$ 256.49
Av. Ayrton Senna com Av. Abelardo Bueno	10,824	0.95	7.51	0.30	3.09	R$ 188.89
Linha Vermelha com Linha Amarela	10.716	0.94	3.10	0.12	3.83	R$ 186.90
Lagoa – Corte do Cantagalo	7,763	0.68	3.88	0.16	3.38	R$ 135.21
Humaitá – São Clemente	7,640	0.67	2.77	0.11	3.47	R$ 133.22
Avenida Brasil com Caju	6,931	0.61	6.70	0.27	3.15	R$ 121.29
Linha Amarela – Shopping Nova América	6,928	0.61	5.09	0.21	3.46	R$ 121.29
Vd. Santiago Dantas – Pinheiro Machado	6,595	0.58	3.26	0.13	4.71	R$ 115.32
Radial Oeste – Maracanã	6,492	0.57	4.30	0.17	3.42	R$ 113.33
Presidente Vargas	6,290	0.55	4.24	0.17	3.70	R$ 109.36
Mena Barreto – Aterro	6,040	0.53	3.41	0.14	3.55	R$ 105.38
Linha Vermelha com Brigadeiro Trompowski	5,617	0.49	3.90	0.16	3.51	R$ 97.43
Avenida Brasil com Rod. Presidente Dutra	5,029	0.44	6.16	0.25	3.14	R$ 87.49
Tunel Rebouças	4,875	0.43	4.03	0.16	3.05	R$ 85.50

Linha Amarela – Geremário Dantas	4,747	0.42	1.71	0.07	3.96	R$ 83.51
Av. Ministro Ivan Lins	3,946	0.35	1.67	0.07	4.38	R$ 69.59
Linha Amarela – Entrada do Túnel	3,472	0.31	0.99	0.04	3.86	R$ 61.64
Av. Brasil com Av. das Missões	3,262	0.29	2.72	0.11	2.72	R$ 57.66
Presidente Antonio Carlos com Beira Mar	3,137	0.28	2.08	0.08	4.48	R$ 55.67
Avenida Delfim Moreira – Av. Niemeyer	2,937	0.26	1.26	0.05	4.90	R$ 51.70
Av. das Amérias – Barra Shopping	2,842	0.25	2.19	0.09	4.06	R$ 49.71
Linha Amarela – Estrada do Gabinal	2,690	0.24	2.01	0.08	3.84	R$ 47.72
Av. Pastor Martin Luther King	1,989	0.18	0.61	0.02	4.97	R$ 35.79
Viaduto Cascadura	2,056	0.18	1.38	0.06	3.43	R$ 35.79
Almirante Barroso com República do Paraguai	1,426	0.13	0.45	0.02	3.57	R$ 25.85
Av. Lúcio Costa – Posto 3	1,173	0.10	0.50	0,02	3.91	R$ 19.88
TOTAL	**299,635**	**26.39**	**178.71**	**7.20**	**-**	**R$ 5,247.18**

Fonte: Pensa - Sala de Ideias. Elaborado pelos autores.

Note que o uso de dados para alterar a mobilidade urbana do Rio de Janeiro não foi por acaso. O município, assim como grande parte das cidades, observa a mobilidade urbana como o calcanhar de aquiles do administrador e parte das preocupações diárias do administrado. De acordo com estudo da FIRJAN (SISTEMA FIRJAN, 2015), as cidades perdem 9% do seu PIB com engarrafamentos. Para o Rio de Janeiro, isso representa em torno de 20 bilhões de dólares por ano.

Esse desperdício acontece ao mesmo tempo em que milhares de cidadãos fazem uso de aplicativos de direcionamento urbano, que indicam as possibilidades de caminhos existentes para o motorista e o fluxo de carros inerente a cada opção.[6]

6 O mesmo pode ser aplicado para os pontos de alagamento, em que a Prefeitura do Rio de Janeiro criou um ranking usando dados de ônibus sobre a quantidade de passageiros que passavam por cada ponto de alagamento. Esse ranking foi usado pelo Centro de Operações e pela Secretaria de Conservação para resolver os transtornos. A cidade ainda tem problemas de alagamento, mas esses problemas são menores do que os que existiam três anos atrás. De fato, houve redução durante anos e, até 2017, não foram verificados grandes alagamentos.

MEGAEVENTOS

Uma outra situação em que os dados dos cidadãos foram utilizados para a realização de políticas públicas foi no processo de planejamento dos grandes eventos que a cidade recepcionou. Quando os jogos olímpicos foram pensados, percebeu-se que as vias urbanas do Rio de Janeiro estavam absolutamente congestionadas. Isso ocorria porque se tinham mais carros do que as vias comportavam, sendo necessária a mudança do projeto de mobilidade da cidade. Na época, seiscentos carros eram emplacados por dia, em média, no município. Com esse número, seria preciso não só construir quatro quilômetros de via todos os dias apenas para comportar esses carros parados, sem que isso fosse feito em uma área isolada, como também que esses novos quilômetros de vias fossem criados nas áreas que mais comportam pessoas (ÇOLAK; LIMA; GONZÁLEZ, 2016).

Dessa forma, ao receber grandes eventos, tal como os Jogos Olímpicos, a disposição dos locais em que se teria grande aglomeração de pessoas, como as competições, não foi aleatória. A escolha foi baseada no perfil de mobilidade do cidadão carioca, tendo em vista o já conturbado tráfego nas vias urbanas.

CICLOVIAS

A Prefeitura do Rio de Janeiro também fez uso de dados para acompanhar a movimentação de bicicletas na cidade. Uma iniciativa interessante nesse sentido foi a utilização de informações do Twitter (NETTO, 2015). Observou-se que esses dados eram representativos e correspondiam às informações do IBGE e, com isso, conseguiu-se fazer o mapeamento dos trajetos que os grupos de pessoas de cada classe social faziam. Com isso, foi possível identificar qual seria o perfil de deslocamento da cidade. Uma vez conhecendo os trajetos realizados pela população, a Prefeitura fez uso de dados do Mapeando,[7] um projeto do LAB Rio, para que as pessoas sugerissem os locais em que elas desejavam que as ciclovias se localizassem. Esses movimentos foram cruzados com as ciclovias existentes e com os meios de transporte de massa. Como resultado, 90 quilômetros de ciclovias foram alterados, integrando especialmente as classes média-baixa e baixa com o transporte de massa por ciclovia, para fazer a ligação mais

7 Confira o site do projeto disponível em: <http://mapeando.rio.gov.br/#/>. Acesso em: 23 jun. 2017.

complicada, que é a da última milha. Tal processo também passou pela adaptação do transporte público para receber bicicletas.[8]

DENGUE

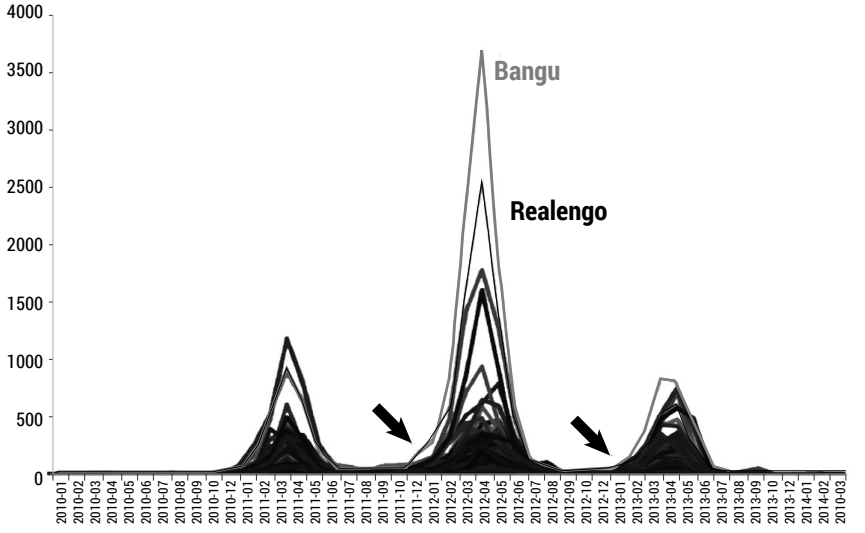
A utilização de dados gerados e disponibilizados pelo cidadão para efetivar políticas públicas não foi aplicada somente na seara da mobilidade urbana, mas também na saúde pública. No caso da dengue, por exemplo, referenciaram-se os números de infectados dentro da cidade e identificaram-se os dois bairros em que os casos começavam a subir antes de todo o resto. Em Bangu e em Realengo, os casos aumentavam quinze dias antes em relação aos demais bairros da cidade.

Usando esses dados, empreendeu-se um esforço para diminuir a incidência dos casos nos locais em que a doença havia se espalhado. O sucesso desse projeto deu-se por conta da atuação conjunta da Secretaria de Educação para trabalhar com as escolas do local, com a Comlurb – para limpar todos os terrenos dessa região –, e com os profissionais da área da saúde, que trabalharam com a distribuição de material especialmente nessas regiões, para diminuir a incidência de dengue na cidade.

Como consequência, em um ano, os casos de dengue da cidade caíram de 1294 por 100 mil habitantes para 41.7, o que representa uma queda de 98% dos casos de um ano para outro.

8 Outra questão é que o Rio de Janeiro é uma cidade com temperaturas muito elevadas e o transporte de bicicleta se torna complicado, principalmente quando se percorre partes da ciclovia localizadas na orla e que não contam com cobertura alguma. Desse modo, elaborou-se outro projeto, buscando associar isso com o uso de bicicletas elétricas ou patinetes elétricas, as quais seriam alugadas para fazer trajetos de um a dois quilômetros, com o objetivo de sanar o problema da última milha. A patinete elétrica se mostrou muito barata, tendo, atualmente, o mesmo custo de uma bicicleta comum. Porém, na apresentação desse projeto, surgiu uma incompatibilidade: o projeto da bicicleta possui um viés de estimular a prática de atividade física, incompatível com a ideia do aluguel de patinetes elétricas. De todo modo, pode haver interesse em um projeto de patinetes elétricas para a integração de pequenos trechos. Afinal, elas têm o mesmo custo que a bicicleta normal, o que pode resolver alguns problemas, como o caso das pessoas que preferem evitar transpirar.

Figura 6 – Gráfico com taxas de crescimento dos casos de dengue



Fonte: Pensa - Sala de Ideias.

É necessário explicitar, no entanto, que há outros fatores que intervêm nessa mudança, como a sazonalidade e a criação de anticorpos pelas pessoas, mas uma queda do índice de infectados de 98% é um valor demasiadamente expressivo para ter como causa somente esses fatores. Na realidade, esse índice torna-se ainda mais significativo quando se observa que várias matérias de jornal anunciavam o rápido crescimento da dengue em São Paulo, enquanto no Rio de Janeiro ela quase desaparecia (BETIM, 2015).[9]

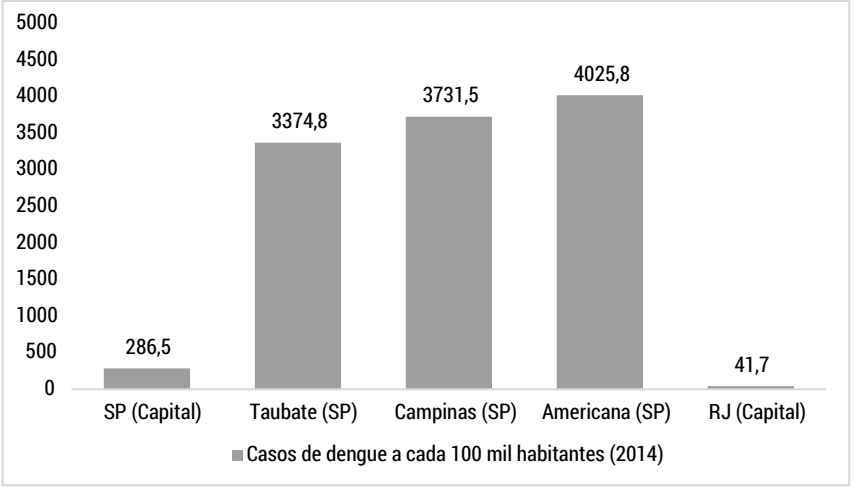
9 Como pontua a reportagem: "O Rio de Janeiro foi pioneiro no ano passado ao realizar um experimento: em um pequeno território, cruzou mosquitos Aedes Aegypti com outros geneticamente modificados para impedir o ciclo biológico da espécie. 'Foi um teste e ainda não temos conclusões. O que sim fazemos é, todos os meses, instalar 3.450 armadilhas em toda a cidade, para que os mosquitos coloquem seus ovos. Levamos para o laboratório e analisamos a densidade vetorial, entre outras coisas', conta Marcus Vinícius, coordenador da Vigilância Ambiental em Saúde da Secretaria Municipal de Saúde do Rio de Janeiro.

A cidade também vem fazendo melhor uso da tecnologia para, por exemplo, investigar possíveis focos do Aedes Aegypti. 'Usamos a mesma metodologia do Ministério de Saúde, mas antes avaliávamos um quinto dos quarteirões da cidade. Aproximamos ainda mais a investigação e, agora, avaliamos todos os quarteirões, 1/20 de cada um. Existem menos espaços vazios', explica".

Figura 7 – Mapa com destaque para cidades estudadas

Fonte: Google Maps.

Figura 8 – Casos de dengue a cada 100 mil habitantes em 2013



Fonte: Pensa - Sala de Ideias; Elaboração própria.

CONSIDERAÇÕES FINAIS: A IMPORTÂNCIA DA TRANSPARÊNCIA E DA COMUNICAÇÃO PARA UMA GESTÃO DA COISA PÚBLICA EFICIENTE E PRÓXIMA DO CIDADÃO

A comunicação e a transparência são elementos essenciais para garantir a estabilidade do governo. A insatisfação geral com o estado de coisas no cenário político decorre dentre outros fatores, da falta de proximidade entre representantes e representados.

As experiências de utilização de dados para a formulação de políticas públicas e para a melhoria da gestão estatal têm se mostrado de grande

valia. Além de os dados servirem como uma forma de *input* para a atuação dos governantes em áreas que carecem de melhorias, serve, também, como forma de *output*, na medida em que os resultados das análises de dados podem ser transformados em ações concretas. Ademais, o uso das informações aumenta a transparência, a comunicação e, sobretudo, a proximidade entre a prefeitura e os cidadãos. É possível imaginar que, na medida em que um cidadão usa um aplicativo e passa a receber retorno da prefeitura – sobre ruas fechadas ou alterações no sentido das vias, por exemplo –, especialmente na preparação para os jogos olímpicos, começa-se a desfazer o isolamento que o deixava apartado da administração pública. O mesmo é verdade quando ele começa a reportar no aplicativo – seja o Waze, seja qualquer outro – informações sobre o que ele está enfrentando ou os engarrafamentos que encontra (GONZÁLEZ; LIMA, 2016).[10]

Através desses recursos para melhorar a administração da cidade, a prefeitura busca uma maior interação entre governo e cidadão. Evita-se que a relação entre esses atores aconteça apenas a cada quatro anos, no momento das eleições. Certamente, isso tem um impacto significativo. Os blocos de carnaval aparecem no Waze, por exemplo, assim como, em grandes eventos, as informações sobre a organização das vias são atualizadas com considerável rapidez.

Note-se que o presente artigo se trata de uma primeira análise de experiências em que o governo se valeu de dados dos cidadãos. Não se trata de um ode ao uso indiscriminado de dados. A utilização destes deve ser feita com cautela e com a adoção de medidas que evitem o abuso contra os cidadãos e contra políticos. Em relação aos cidadãos, o uso de dados por parte do governo deve se dar com a implementação de medidas de segurança dos dados e dos sistemas informáticos, com a busca pela proteção da privacidade[11] e sem que haja distanciamento da finalidade da coleta quando da utilização dos dados (BRASIL, 2010; FEDERAL TRADE COMISSION, 2015). Além disso, deve-se evitar o abuso contra outros políticos. Em períodos de reeleição, o candidato que se encontra no exercício de seu mandato possui vantagens pelo uso da máquina estatal, o que é

10 "Drivers' apparent flexibility on route choices may provide an opportunity to alleviate overall congestion. For instance, smartphone apps could offer points and vouchers to drivers who are willing to take longer routes that avoid congested areas. Navigation app Waze has already changed drivers' habits in some cities, so it's not so far-fetched to imagine a gamification system that reduces congestion".

11 No Brasil, o Senado Federal aprovou, recentemente, a lei geral de proteção de dados pessoais e, no momento em que este artigo foi finalizado, o projeto aguardava apenas a sanção presidencial.

potencializado pelo acesso aos dados de cidadãos. Assim, é preciso que os dados sejam abertos à sociedade, a acadêmicos e a outros políticos para que haja comparação de resultados e críticas às medidas adotadas. Observe que não se trata de um simples acesso à *informação*, já assegurado pela Lei de Acesso à Informação (Lei nº 12.527/2011), mas de acesso efetivo aos *dados*.[12] Com isso, evita-se, ainda, que os governos concentrem o poder – o que poderia abrir caminhos para a tirania –, tendo em vista o elevado valor que se atribui aos dados atualmente.[13]

Esse tipo de análise com uso de dados que aproxima o governo do cidadão será importante não apenas para melhorar a administração, como também para introduzir um novo modelo de governo, que entende o que está acontecendo e responde às demandas da sociedade conforme elas aparecem, de acordo com as demandas de cada dia ou cada hora dos cidadãos. Uma cidade inteligente requer atuação proativa dos administradores e mecanismos efetivos e de fácil acesso para que os cidadãos possam comunicar suas insatisfações e suas necessidades aos governantes. Instalar sensores ao longo da cidade não esgota a noção de *smart cities*. Este conceito significa entender o impacto que isso promove na forma como os governos funcionam e como interagem com os cidadãos.

REFERÊNCIAS

ABRANCHES, Sérgio Henrique Hudson de. Presidencialismo de coalizão: o dilema institucional brasileiro. ***Revista de Ciências Sociais***, Rio de Janeiro, v. 31, n. 1, p. 5-34, 1988.

ACKERMAN, Bruce. The new separation of power. ***Harvard Law Review***, v. 113, n. 3, p. 633-725, jan. 2000.

AGÊNCIA EFE. Trump registra níveis mais baixos de popularidade desde que foi eleito. G1, ago. 2017. Disponível em: <https://g1.globo.com/mundo/noticia/trump-registra-niveis-mais-baixos-de-popularidade-desde-que-foi-eleito.ghtml>. Acesso em: 22 nov. 2017.

BETIM, Felipe. A dengue explode em São Paulo enquanto no Rio quase desaparece. El País, São Paulo, 17 abr. 2015. Disponível em: <http://brasil.elpais.com/brasil/2015/04/17/politica/1429296266_761323.html>. Acesso em: 23 jun. 2017.

12 Sobre o tema, ver o PL nº 7.804/2014, que busca a aprovação de uma Lei de Dados Abertos.

13 Afirma-se que, no presente século, os dados equivalem ao que o petróleo significou no século passado. Cf. THE ECONOMIST. Data is giving rise to a new economy. Disponível em: <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>. Acesso em: 3 jul. 2017.

BRASIL. Escola Nacional de Defesa do Consumidor. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010.

CHOURABI, Hafedh, ***et al***. Understanding Smart Cities: An Integrative Framework. IEEE Xplore, 2012. Disponível em: <http://ieeexplore.ieee.org/document/6149291/>. Acesso em: 20 set. 2017.

ÇOLAK, Serdar; LIMA, Antonio; GONZÁLEZ, Marta C. Understanding Congested Travel in Urban Areas. ***Nature Communications***, n. 7, p. 1-8, mar. 2016.

DAHL, Robert A. ***Sobre a democracia***. Tradução de Beatriz Sidou. Brasília: Editora Universidade de Brasília, 2001.

DATA IS GIVING Rise to a New Economy. Economist, 6 maio 2017. Disponível em: <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>. Acesso em: 3 jul. 2017.

DIAS, Roberto. Aplicativo Waze é usado pela Prefeitura do Rio. Folha Uol, 4 jan. 2016. Disponível em: <http://www1.folha.uol.com.br/mercado/2016/01/1725398-aplicativo-waze-e-usado-pela-prefeitura-do-rio.shtml>. Acesso em: 20 jun. 2017.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

FEDERAL TRADE COMISSION. Internet of Things: Privacy & Security in a Connected World. [S.l]: FTC Staff Report, 2015.

FREITAS, Andréa. O presidencialismo de coalizão. Rio de Janeiro: Fundação Konrad Adenauer, 2016.

GLAESER, Edward. Triumph of the City: How Our Greatest Invention Makes Us Richer, Smarter, Greener, Healthier, and Hap Pier. London: Penguin Books, 2012.

GONZÁLEZ, Marta C.; XU, Yanyan. Collective Benefits in Traffic During Mega Events Via the Use of Information Technologies. ***Journal of the Royal Society Interface***, v. 14, n. 129, p. 1-10, abr. 2017.

GONZÁLEZ, Marta; LIMA, Antonio. Recalculating! By Not Driving the Optimal Route, You're Causing Traffic Jams. ***The Conversation***, 15 mar. 2016. Disponível em: <http://theconversation.com/recalculating-by-not-driving-the-optimal-route-youre-causing-traffic-jams-56135>. Acesso em: 20 jun. 2017.

IRISH, John. Macron diz a Trump que acordo nuclear com Irã é "bom", seria irresponsável desrespeitá-lo. UOL Notícias, 19 set. 2017. Disponível em: <https://noticias.uol.com.br/ultimas-noticias/reuters/2017/09/19/macron-diz-a-trump-que-acordo-nuclear-com-ira-e-bom-seria-irresponsavel-desrespeita-lo.htm>. Acesso em: 19 set. 2017.

LAFUENTE, Javier. Colômbia diz 'não' ao acordo de paz com as FARC. El País, Bogotá, 3 out. 2016. Disponível em: <http://brasil.elpais.com/brasil/2016/10/02/internacional/1475420001_242063.html>. Acesso em: 19 jun. 2017.

MANIN, Bernard. The principles of representative government. Cambridge: Cambridge University Press, 1997.

MAPEANDO. Disponível em: <http://mapeando.rio.gov.br/#/>. Acesso em: 23 jun. 2017.

MIGUEL, Luís Felipe. Impasses da *Accountability*: dilemas e alternativas da representação política. ***Revista de Sociologia e Política***, n. 25, p. 25-38, nov. 2005.

MOUNK, Yascha; FOA, Roberto Stefan. The Signs of Deconsolidation. ***Journal of Democracy***, v. 28, n. 1, p. 5, jan. 2017.

NETTO, Vinicius M. ***et al***. Digital Footprint in the Cityspace: Finding Networks of Segregation Through Big Data. In: International Conference on Location-Based Social Media Data, Athens, GA, USA, mar. 2015, p. 1-15. Disponível em: <https://www.researchgate.net/publication/272408306_Digital_footprints_in_the_cityscape_Finding_networks_of_segregation_through_Big_Data>. Acesso em: 23 jun. 2017.

NIKOLAEVA, Maya; IRISH, John. Macron diz estar confiante de que Trump verá que acordo de Paris é do interesse dos EUA. Extra, 19 set. 2017. Disponível em: <https://extra.globo.com/noticias/mundo/macron-diz-estar-confiante-de-que-trump-vera-que-acordo-de-paris-do-interesse-dos-eua-21842102.html>. Acesso em: 19 set. 2017.

QUEM GANHOU e quem perdeu nas eleições britânicas. BBC Brasil, 8 mai. 2015. Disponível em: <http://www.bbc.com/portuguese/noticias/2015/05/150508_eleicoes_ganhaeperde_vj_pu>. Acesso em: 19 set. 2017.

REDAÇÃO BBC BRASIL. Brexit: o que derrota judicial de governo britânico significa para processo de saída da UE. BBC Brasil, 24 jan. 2017. Disponível em: <http://www.bbc.com/portuguese/internacional-38729810>. Acesso em: 19 set. 2017.

REDAÇÃO BBC BRASIL. O que é 'Brexit' – e como pode afetar o Reino Unido e a União Europeia? BBC Brasil, 17 jun. 2016. Disponível em: <http://www.bbc.com/portuguese/internacional-36555376>. Acesso em: 19 set. 2017.

REDAÇÃO BLOOMERANG. Macron quer lembrar ao mundo que França é potência nuclear. InfoMoney, 18 set. 2017. Disponível em: <http://www.infomoney.com.br/bloomberg/mercados/noticia/6962462/macron-quer-lembrar-mundo-que-franca-potencia-nuclear>. Acesso em: 19 set. 2017.

REDAÇÃO. Popularidade de Trump registra queda no interior dos EUA, aponta pesquisa. Reuteurs, out. 2017. Disponível em: <https://br.reuters.com/article/topNews/idBRKBN1CE1KC-OBRTP>. Acesso em: 22 nov. 2017.

SISTEMA FIRJAN. O custo dos deslocamentos nas principais áreas urbanas do Brasil. [S.l.]: Publicações Sistema FIRJAN – Pesquisas e Estudos Socioeconômicos, set. 2015. Disponível em: <http://www.firjan.com.br/lumis/portal/file/fileDownload.jsp?fileId=2C908A8F4F8A7DD3014FB26C8F3D26FE&inline=1>. Acesso em: 23 jun. 2017.

THORP, Jer. Big Data is Not the New Oil. Harvard Business Review, 30 nov. 2012. Disponível em: <https://hbr.org/2012/11/data-humans-and-the-new-oil>. Acesso em: 23 jun. 2017.

WEBER, Max. ***Ensaios de Sociologia***. 5. ed. Tradução de Waltensir Dutra. Rio de Janeiro: LTC, 1982.

PADRÕES DE MOBILIDADE HUMANA NA REGIÃO METROPOLITANA DO RIO DE JANEIRO

JULIO C. CHAVES
GABRIEL S. D. CARVALHO
MOACYR A. H. B. SILVA
ALEXANDRE G. EVSUKOFF

INTRODUÇÃO

A coleta de dados para o planejamento de transporte urbano tem sido realizada por questionários sobre padrões de viagens dos usuários, pesquisas domiciliares, contagens volumétricas de tráfego, informações de uso do solo e rede de transporte. A coleta de dados para o planejamento de transporte é custosa e demanda um longo período de planejamento e execução e também possuem um tamanho amostral limitado, tendo em vista os custos envolvidos (CHEN *et al.,* 2016; IVEY; BADOE, 2011).

Metodologias alternativas vêm sendo desenvolvidas para utilizar dados de registros de chamadas de telefones celulares, ou Call Detail Records (CDR), em modelos de transporte. Os dados de CDR são gerados em grande quantidade como subproduto da bilhetagem e contêm, dentre outras informações, a localização aproximada do local de realização da chamada telefônica assim como a data e a hora dessa ligação (SMOREDA; OLTEANU-RAIMOND; COURONNÉ, 2013). Apesar das limitações em aferir a escolha modal e as rotas escolhidas, a utilização de CDR permite identificar os principais deslocamentos da população em estudo.

Estudos recentes apresentam a utilização de dados de CDR em diferentes áreas (CHEN *et al.*, 2016; TOOLE *et al.*, 2015; BLONDEL; DECUYPER; KRINGS, 2015) como descoberta de padrões (JÄRV; AHAS; WITLOX, 2014; JIANG; FERREIRA JR.; GONZÁLEZ, 2015), simulações de mobilidade da população (KERAMAT JAHROMI *et al.*, 2016; PAPANDREA *et al.*, 2016) modelos de mobilidade urbana e migratória (SIMINI *et al.*,

2012; WESOLOWSKI *et al*., 2015), descoberta de agrupamentos a partir de perfis de mobilidade (ZHONG *et al*, 2015; DOUGLASS *et al*, 2014), medidas de mobilidade humana e de eficiência dos sistemas de transporte (WANG *et al*., 2015; DONG *et al*., 2016), identificação de áreas densas (RUBIO; SANCHEZ; FRIAS-MARTINEZ, 2013; KANG *et al*., 2012), além da elaboração de matrizes de origem-destino (IQBAL *et al.,* 2014), de particular interesse para o planejamento de transportes.

Este trabalho apresenta uma modelagem espaço-temporal da região de estudo em unidades geográficas que permite a integração com dados de CDR agregados com dados demográficos e de outras fontes. A identificação de residência presumida dos usuários permite a conexão da base de CDR com dados demográficos e socioeconômicos para inferir o percentual de habitantes de cada unidade geográfica visitando cada uma das unidades geográficas do estudo. Foram utilizados algoritmos para estimativa de matrizes Origem Destino (OD) a partir dos dados de CDR. Os resultados foram validados com os resultados do levantamento realizado pelo Plano Diretor de Transporte Urbano (PDTU) da Região Metropolitana do Rio de Janeiro realizado em 2013.

A próxima seção apresenta a descrição da área de estudo e a base de dados de CDR utilizada no trabalho. A seção 2 também apresenta o particionamento espacial da área de estudo em 55 unidades geográficas e o processamento para estimativa de domicílio presumido. A seção 3 descreve o algoritmo de estimativa da matriz Origem – Destino (OD). A seção 5 apresenta os resultados obtidos e a seção 6 as conclusões do trabalho.

DESCRIÇÃO E MODELAGEM DO PROBLEMA

A adoção da tecnologia de telefonia móvel no Brasil segue a tendência mundial. A Tabela 1 mostra o percentual da população com telefone celular, por regiões no Brasil. Em 2005 o percentual da população brasileira que possuía acesso ao telefone celular era de 36,6% chegando a 78,3% em 2015. Em nível regional, a utilização de telefone celular chega a 82,6% nas regiões Sul e Sudeste e 86,9 % na região Centro-Oeste. Em grandes centros urbanos, este percentual atinge mais de 90%. Segundo o site Teleco,[1] em 2016 havia no Brasil 1,18 aparelhos de celular por habitante.

1 Cf.: TELECO. Estatísticas do Brasil - Geral. Disponível em: <http://www.teleco.com.br/estatis.asp>. Acesso em: 9 ago. 2017.

Tabela 1: Percentual de pessoas com telefone móvel celular para uso pessoal, na população de 10 anos ou mais de idade (%) por grandes regiões

Ano	Brasil	Norte	Nordeste	Sudeste	Sul	Centro-Oeste
2005	36.6	26.4	23.9	40.9	47.5	47.5
2008	53.7	43.9	41.2	58.6	62.7	64.3
2013	75.2	66.7	66.1	79.5	79.8	83.8
2015	78.3	68.6	69.6	82.6	82.8	86.9

Fonte: PNAD IBGE – Pesquisa Nacional por Amostra de Domicílios.

Os dados usados neste estudo foram fornecidos por uma das maiores companhias telefônicas do Brasil. Os dados foram coletados ao longo do ano de 2014 na Região Metropolitana do Rio de Janeiro, conforme apresentado a seguir.

O CONJUNTO DE DADOS

A área de estudo compreende a Região Metropolitana do Rio de Janeiro (RMRJ),[2] a segunda maior área urbana do Brasil, se estendendo por 6744 km² com 12.085.108 habitantes distribuídos em 23 cidades, sendo a cidade do Rio de Janeiro, com 6.323.037 habitantes em 1200 km² a mais importante.

Foram coletados os dados de tráfego gerado – apenas chamadas de voz – originado em todas as 1078 antenas localizadas código de área 21,[3] que corresponde à Região Metropolitana do Rio de Janeiro incluindo os municípios de Teresópolis e Mangaratiba. Em geral, pelo menos três antenas são posicionadas a 120º em cada torre, de forma que a cobertura por torre pode ser aproximada por polígonos de Voronoi.[4] A Figura 1 mostra a área de estudo no detalhe e uma visão geral da distribuição espacial das antenas na área de estudo e polígonos de Voroni correspondentes.

O posicionamento das torres segue objetivos mercadológicos e técnicos e sua distribuição é bastante irregular, como pode ser observado na Figura 1. A distribuição espacial das antenas é mais densa nas áreas de maior

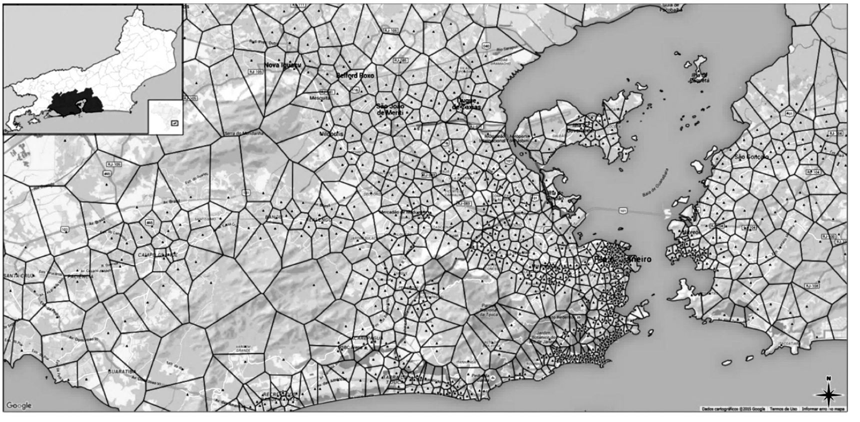
2 Cf.: WIKIPÉDIA. Greater Rio de Janeiro. Disponível em: <https://en.wikipedia.org/wiki/Greater_Rio_de_Janeiro>. Acesso em: 6 abr. 2017.

3 Cf.: TELECO. Numeração Telefônica. Disponível em: <http://www.teleco.com.br/num.asp>. Acesso em: 6 abr. 2017.

4 Os polígonos de Voronoi delimitam a área mais próxima de cada antena. Ver: WIKIPÉDIA. Diagrama de Voronoy. Disponível em: <https://pt.wikipedia.org/wiki/Diagrama_de_Voronoy>. Acesso em: 12 ago. 2017.

renda e oferta de empregos. Nas áreas Norte e Oeste, de menor densidade demográfica, a distribuição das antenas é menos densa, assim como nos demais municípios da Região Metropolitana, exceto o centro da cidade de Niterói, do lado oeste da Baia de Guanabara. É possível verificar também área com pouca cobertura no meio da zona urbana, devido às montanhas. A geografia da cidade do Rio de Janeiro causa um grande impacto nas rotas de mobilidade da cidade.

Figura 1: Visão geral da área de estudo com foco na distribuição espacial das antenas com seus respectivos polígonos de Voronoi. No detalhe, a localização da Região Metropolitana do Rio de Janeiro



Fonte: Elaboração dos autores e do mapa de localização da RMRJ da Wikipedia.[5]

A base de dados cobre o período entre 31 de dezembro de 2013 e a 1 de janeiro de 2015, somando 2.1 bilhões de registros referentes a 2.9 milhões de assinantes. Os dados foram cedidos pela operadora com as identificações dos usuários criptografadas para assegurar a anonimização dos dados.

Apenas os dados de chamadas de voz realizadas foram disponibilizados para o estudo, de forma que o conjunto de dados não contém informações adicionais de tráfego como chamadas recebidas e mensagens de texto (SMS). As informações de cada registro são mostradas na Tabela 2. Os dados foram pré-processados para eliminar usuários com comportamento anômalo, com mais de 100 chamadas por dia ou menos de dez chamadas por ano.

5 Ver: WIKIPÉDIA. Região Metropolitana do Rio de Janeiro. Disponível em: <https://pt.wikipedia.org/wiki/Região_Metropolitana_do_Rio_de_Janeiro>. Acesso em: 6 abr. 2017.

Os dados coletados neste projeto foram utilizados para análise dos padrões de mobilidade no Rio de Janeiro. Para o desenvolvimento da metodologia foi realizado um particionamento espacial e temporal da área de estudo, como descrito a seguir.

Tabela 2: Dados de um registro de chamada telefônica (CDR)

Campo	Descrição
Dia	O dia do registro
Hora	A hora do registro
Duracao	A duração da chamada
Ddd_orig	O DDD da estação de origem da chamada
Num_orig	O ID criptografado da estação origem da chamada
Ddd_dest	O DDD da estação do destino
Num_dest	O ID criptografado da estação destino da chamada
Cell_id_orig	O código da antena que atendeu a chamada na origem
Tp_trafego	Tipo de tráfego: roaming internacional sms etc.
Hold_orig	Nome da operadora que processou a chamada na origem.
Hold_dest	Nome da operadora que processou a chamada no destino

Fonte: Elaboração dos autores.

UNIDADES GEOGRÁFICAS

O desenho da amostra e sua representatividade em relação ao universo tem um impacto decisivo na qualidade dos resultados de inferências estatísticas. Métodos tradicionais de coleta de dados realizam um planejamento criterioso da amostra. No Plano Diretor de Transportes Urbanos (PDTU) da RMRJ (C. E. DE ENGENHARIA DE TRANSPORTE E LOGÍSTICA, 2015), realizado em 2013 e publicado em 2015, a área de estudo é particionada em zonas de tráfego, definidas em função das características demográficas e da infraestrutura viária existente.

Os dados de CDR, por outro lado, não representam uma amostra planejada. A distribuição espacial das antenas irregular, como mostrado na Figura 1, a distribuição temporal do número de chamadas pode variar muito ao longo do dia e as pessoas não realizam chamadas a intervalos de tempo regulares. Os dados de CDR precisam ser corrigidos para representar estatisticamente as grandezas de interesse.

Os polígonos individuais de cada torre nos dados de CDR não são adequados para o cálculo de estatísticas consistentes sobre os dados além de exigir alto custo computacional. Em geral, a maioria de trabalhos com dados de CDR, a região é particionada num grid regular sobre a área de estudo (TOOLE *et al*., 2015; BARLACCHI *et al*., 2015). Esta solução é mais simples e de fácil generalização, mas é de difícil interpretação e exige um ajuste de geometria para que os resultados possam ser integrados com dados demográficos e de outras fontes.

O particionamento espacial proposto leva em consideração as características demográficas e socioeconômicas da população e pode ser facilmente integrado com dados de outras fontes. No Brasil, o Instituto Brasileiro de Geografia e Estatística (IBGE) já tem um particionamento definido, pela agregação dos setores censitários em níveis de Subdistrito, Distrito, Município e Estado e País. Esta hierarquia, de setor censitário a país, é utilizada para o código de identificação das unidades. O IBGE utiliza padrões mundiais para este tipo de particionamento, de forma que a metodologia pode ser reproduzida em outras cidades e regiões metropolitanas.

O particionamento espacial agrega os resultados das consultas à base de CDR por unidades geográficas representativas dos locais de interesse no estudo. Uma unidade geográfica é definida por um conjunto de antenas localizado no interior do limite geográfico de um subdistrito, distrito ou município. O limite geográfico de cada unidade geográfica é aproximado pela união dos polígonos de Voronoi das antenas correspondentes. O resultado deste particionamento espacial é um conjunto de regiões que podem ser relacionadas com subdistritos da área de estudo e, consequentemente, aos dados de todas as pesquisas realizadas pelo IBGE.

A Figura 2 ilustra o particionamento espacial realizado neste estudo, com foco nos locais de maior concentração de registros e maior densidade populacional. O particionamento apresentado na Figura 2 não representa as fronteiras geográficas dos locais, mas os limites da aproximação por unidades geográficas definidas pela agregação dos polígonos de Voronoi.

Figura 2: Visão do particionamento espacial com a ênfase nos locais com maior número de registros

Fonte: Elaboração dos autores.

A análise foi realizada com subdistritos da cidade do Rio de Janeiro em conjunto com os demais municípios da RMRJ, um total de 55 unidades geográficas. Este particionamento espacial permite uma visão simplifica da RMRJ para o planejamento de transportes, tendo em vista o foco nos grandes eventos em Copacabana. Cada unidade geográfica representa uma região mais ou menos homogênea em termos de características socioeconômicas e os resultados estatísticos das consultas à base de dados de CDR podem ser relacionados com os dados correspondentes do IBGE e outras fontes.

As distâncias entre os centros das unidades geográficas foram calculadas em função da malha rodoviária. A área de estudo tem uma geografia peculiar, dada pelas formações montanhosas em torno da baia de Guanabara, de tal forma que áreas geograficamente próximas, podem ser consideradas distantes através das vias expressas. As distâncias entre os centros das unidades geográficas foram calculadas por uma interface programável (API) fornecida pelo Google Maps chamado Distance Matrix API,[6] com a distância percorrida entre os dois pontos utilizando a malha rodoviária.

A base de dados CDR foi armazenada num banco de dados incluindo na tabela dos registros de chamada (cf. Tabela 2) a posição geográfica (Latitude e Longitude) da antena. A base de dados é uma tabela com 2 bilhões de registros de ligação. A conexão dos dados de mobilidade com

6 Cf.: GOOGLE MAPS PLATFORM. Get Started. Disponível em: <https://developers.google.com/maps/documentation/distance-matrix/>. Acesso em: 9 ago. 2017.

dados censitários, a partir da identificação do domicilio de cada usuário, como descrito a seguir.

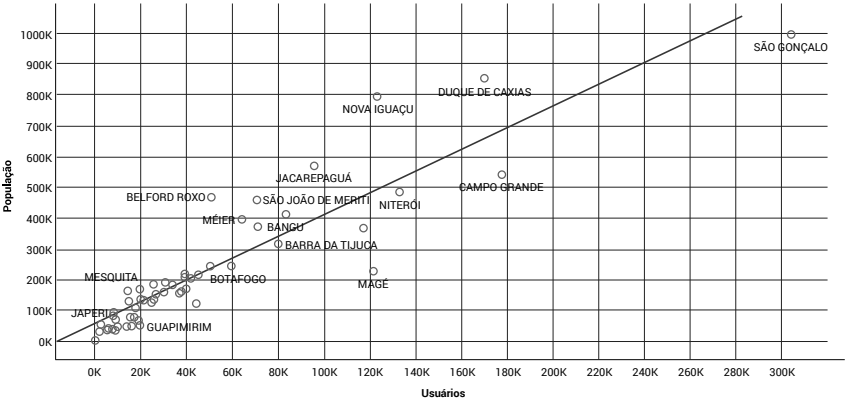
IDENTIFICAÇÃO DE RESIDÊNCIA PRESUMIDA

O domicílio presumido do usuário é a unidade geográfica mais visitada entre 20:00 horas e 06:00 horas do dia seguinte, ou todo o dia nos domingos e feriados em toda a base de dados, i.e. durante todo o ano de 2014. Restrições adicionais foram impostas para identificar como domicílio presumido um local visitado frequentemente pelo usuário no período selecionado. É necessário que o usuário tenha sido detectado no local um certo número de vezes e número de observações no local mais frequente deve sem maior que o segundo local mais frequente.

O domicilio presumido de cada usuário na base é um local de residência definido por uma unidade geográfica do particionamento espacial da área de estudo. Os usuários que não tiveram seus domicílios presumidos identificados foram descartados. A base contendo apenas usuários com domicílio identificado contém 2,5 milhões de usuários.

A validação do cálculo de domicílio presumido foi feita com os dados do censo IBGE 2010, como mostra a Figura 3, onde algumas unidades geográficas populosas estão identificadas. A relação linear obtida estima uma média 3.5 pessoas para cada usuário da base, com correlação de 90.9%.

Figura 3: Comparação do número de usuários com domicílio presumido com a população de cada unidade geográfica. A partir da definição do domicílio presumido de cada usuário, é possível estimar o número de pessoas presentes num determinado evento, como descrito a seguir.



Fonte: Elaboração dos autores.

MATRIZ ORIGEM-DESTINO

O método de quatro etapas (MCNALLY, 2007) é um dos mais utilizados na modelagem de demanda de viagens para o planejamento de transportes. O processo é composto de quatro etapas: a primeira etapa é a geração de viagens, que estima o número de viagens produzidas e atraídas por cada zona de tráfego. A segunda etapa é a distribuição de viagens, onde se calcula o fluxo de transporte entre zonas de tráfego representado pela matriz Origem-Destino (OD), em geral com base num modelo de previsão de demandas como o modelo de gravitação (TSEKERIS; STATHOPOULOS, 2006). A terceira etapa é a repartição modal, a partir da definição da rede de transporte, os fluxos são distribuídos pelos diversos modais. A última etapa é a alocação de viagens em que os fluxos da matriz OD por cada modal são alocados na rede de transporte, indicando os gargalos e necessidades de expansão. O modelo de quatro etapas foi utilizado na elaboração do Plano Diretor de Transportes Urbanos (PDTU) da RMRJ (C. E. DE ENGENHARIA DE TRANSPORTE E LOGÍSTICA, 2003 e 2015).

Os dados de CDR permitem estimar as duas primeiras fases do modelo de quatro etapas: a geração e a distribuição de viagens. Os dados de CDR permitem realizar diretamente a estimativa da matriz OD, de forma que a etapa de geração de viagens é realizada a partir da matriz OD. A base de dados de CDR utilizada neste trabalho contêm apenas registros de chamadas realizadas. Os dados não fornecem informação sobre a repartição modal. Bases de dados de CDR mais completas, com registros de acesso à rede de internet – 2G, 3G e 4G – permitem acompanhar a trajetória de usuários, possibilitando assim inferir o meio de transporte utilizado (CALABRESE *et al.*, 2010; MOREIRA-MATIAS, 2015).

Há na literatura diversos algoritmos de geração de matriz OD com dados de celulares (TOOLE *et al.*, 2015; ALEXANDER *et al.*, 2015). No algoritmo utilizado neste trabalho, proposto em (TOOLE *et al.*, 2015), duas chamadas telefônicas sucessivas em locais diferentes são utilizadas para estimar um deslocamento entre a localização das torres que processaram a chamada. Este método captura deslocamentos efetivamente realizados, mas é possível que as chamadas tenham sido realizadas em trânsito, e o deslocamento real tenha ocorrido entre locais diferentes. O algoritmo foi testado em cinco cidades: Rio de Janeiro, Boston, São Francisco e Lisboa. Os resultados mostram que o algoritmo realiza boas estimativas da matriz OD diretamente de dados de CDR (TOOLE *et al.*, 2015).

O cálculo da estimativa da matriz OD ainda precisa levar em conta que a amostra é determinada pelo conjunto de usuários que realizaram

chamadas e as estimativa de viagens deve ser na escala da população. A maneira mais simples de realizar esta expansão é utilizar um fator k_i para cada unidade geográfica *i*.

O algoritmo é parametrizado por constantes que definem uma viagem como um trajeto com percurso mínimo de L_{min} km e realizado no intervalo de tempo $T_{\min} \leq \Delta T \leq T_{\max}$. O procedimento utilizado neste trabalho é apresentado no Algoritmo 1.

Algoritmo 1: Estimativa de matriz OD a partir de dados de CDR.

Entrada:	Base de registros de chamada (cf. Tabela 2), as constantes L_{min}, T_{min} e T_{max}, e tabela de distâncias entre unidades geográficas
Saída:	Matriz OD
01	**Início**
02	Matriz OD = NULL
03	**Para** cada dia da base de dados
04	**Para** cada viagem detectada por dois registros sucessivos do mesmo usuário, com distância l_{ij} e no intervalo de tempo ΔT
05	**Se** $l_{ij} > L_{\min}$ *e* $T_{\min} \leq \Delta T \leq T_{\max}$
06	Identificar domicílio presumido *i*
07	Matriz $OD_{ij} \leftarrow$ Matriz $OD_{ij} + k_i$
08	**Fim Se**
09	**Fim Para**
10	**Fim Para**
11	Retorna Matriz *OD*
12	**Fim**

Fonte: Elaboração dos autores.

O laço entre as linhas 04 e 09 foi colocado de forma a facilitar a leitura do algoritmo. Este laço pode ser implementado de diferentes formas, dependendo da estrutura de dados recursos da linguagem de programação. Neste trabalho todos os algoritmos foram implementados em linguagem SQL utilizando funções analíticas de banco de dados colunares.

Os índices *ij* para o cálculo da Matriz OD_{ij} referem-se às unidades geográficas Origem e Destino do vigem detectada *lij*. É possível que $i = j$ e neste caso o deslocamento acontece no interior da mesma unidade geográfica. As constantes para detecção de viagens utilizadas neste trabalho são $L_{\min}$ = 2 km, e o intervalo de tempo 30 min $\leq \Delta T \leq T$ 4h.

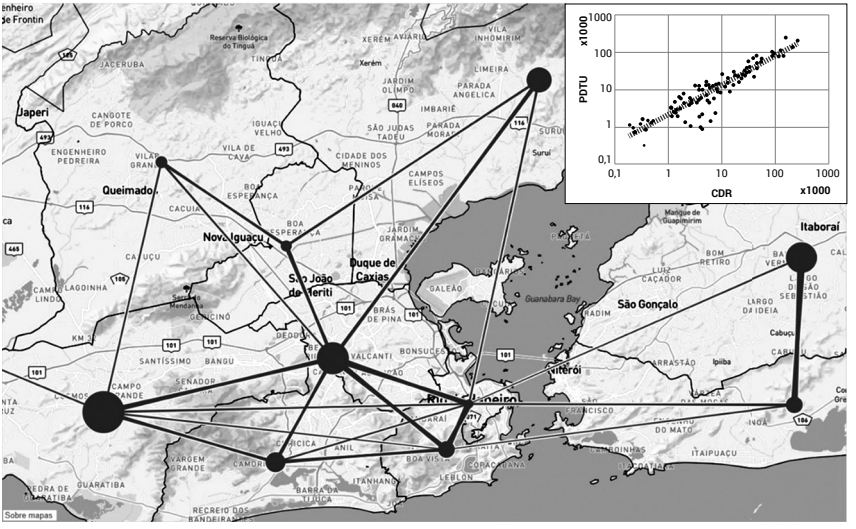
O fator de conversão *ki* no passo 06 é calculado de forma que o número de usuários detectados seja expandido para a escala da população. Neste trabalho o fator de conversão de cada unidade geográfica é calculado pela razão entre o número de usuários com domicílio presumido no local e a população do subdistrito correspondente.

O algoritmo de estimativa da matriz OD foi aplicado à base de dados de CDR em estudo gerando uma matriz OD por dia para os 360 dias presentes na base do ano de 2014. Os resultados são apresentados a seguir.

RESULTADOS

A validação da estimativa da matriz OD pelo Algoritmo 1 foi feita pela comparação com os resultados publicados no PDTU (C. E. DE ENGENHARIA DE TRANSPORTE E LOGÍSTICA, 2015). A Figura 4 mostra a o grafo chamado de linhas de desejo com a conexão de os pares OD, onde apenas as ligações mais importantes são mostradas. A espessura das ligações é proporcional à média anual do número de viagens entre as macrozonas, calculado pelo Algoritmo 1. O diâmetro dos nós é proporcional ao número de viagens dentro da mesma macrozona, calculado pelo mesmo algoritmo. No detalhe no alto a direita da Figura 4 é mostrada a comparação, para todos os pares OD, entre os resultados obtidos pelo Algoritmo 1 (CDR) e os resultados do PDTU agregados pelas macrozonas (C. E. DE ENGENHARIA DE TRANSPORTE E LOGÍSTICA, 2015). Os eixos do gráfico comparativo de CDR e PDTU estão em escala logarítmica e apresentam uma correlação linear de 92,5%. Pode-se observar que os resultados de CDR têm maior aderência para os pares OD com maior fluxo, sendo que realiza uma subestimação nos de menor fluxo. Os resultados mostram que a estimativa com dados de CDR é menos confiável com menos de 1000 viagens detectadas.

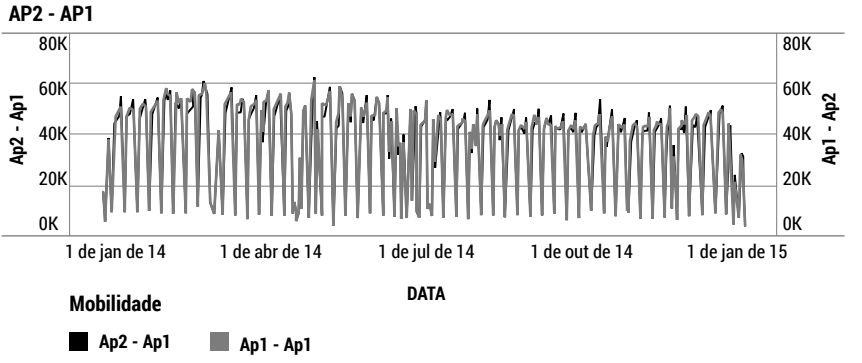
Figura 4: Matriz OD calculada pelo Algoritmo 1 agregada nas macrozonas do PDTU. No detalhe, a comparação dos resultados do PDTU com os resultados obtidos a partir dos dados CDR



Fonte: Elaboração dos autores.

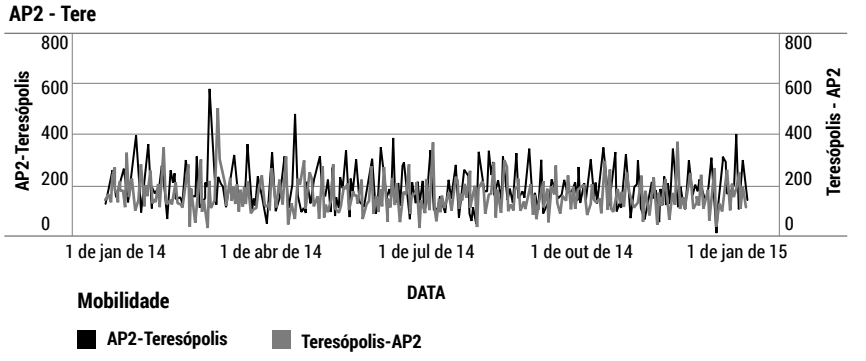
A análise dos resultados por dia revelou dois padrões de mobilidade bem característicos. O padrão mais comum é o que representa a mobilidade Casa – Trabalho, exemplificado na Figura 5 pelo trajeto AP2 – AP1 (Zona Sul – Centro). Neste padrão, os deslocamentos mais frequentes são nos dias úteis com uma queda nos domingos. O padrão é altamente repetitivo e os dias de comportamento irregular são, geralmente, os feriados prolongados. O padrão Casa – Trabalho também é simétrico, isto é, os deslocamentos AP1 – AP2 (Centro – Zona Sul) são praticamente idênticos aos deslocamentos AP2 – AP1 (Zona Sul – Centro).

Figura 5: Padrão de mobilidade Casa – Trabalho e Trabalho – Casa



Fonte: Elaboração dos autores.

Figura 6: Padrão de mobilidade Casa – Lazer e Lazer – Casa

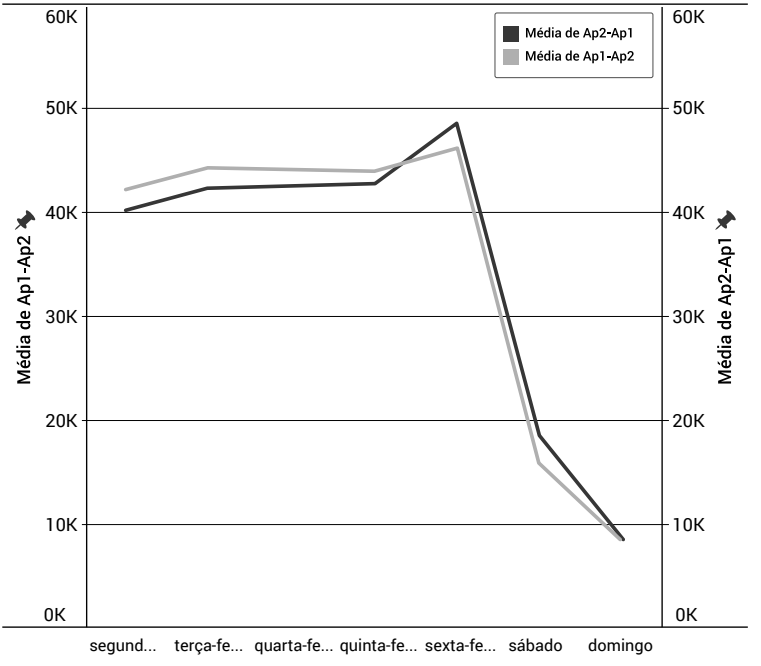


Fonte: Elaboração dos autores.

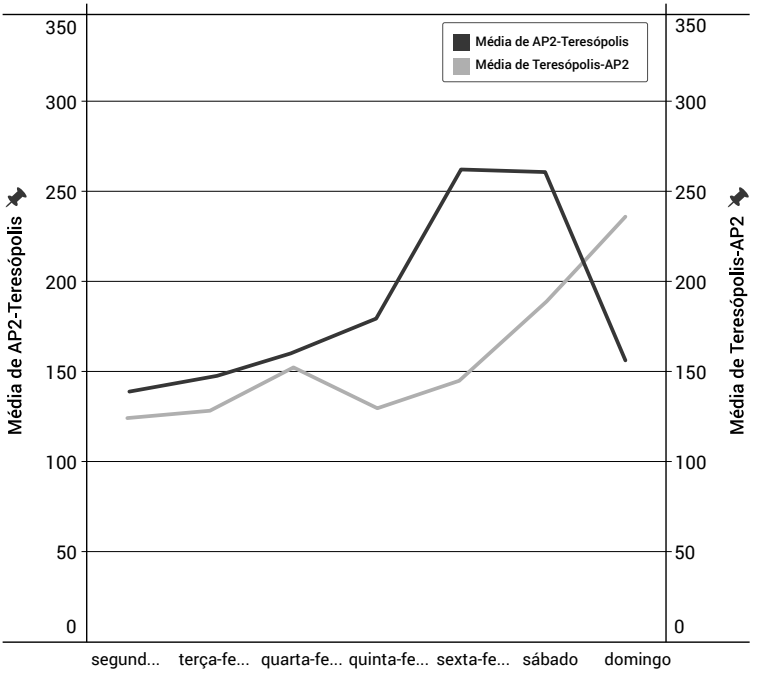
O segundo padrão de mobilidade encontrado é o padrão de deslocamento Casa – Lazer. Este padrão de mobilidade é exemplificado na Figura 6 pelos deslocamentos entre Zona Sul - Teresópolis, cidade da região serrana, muito procurada para veraneio. Neste caso, os deslocamentos mais intensos acontecem nos fins de semana. Pode-se observar que o máximo ocorre no início de feriados, como a sexta feira anterior ao carnaval em 28 de abril 2014 e a sexta-feira santa em 18 de abril 2014. No exemplo observado, o padrão de volta, isto é, Lazer – Casa (Teresópolis – Zona Sul), apresenta pequena defasagem temporal em relação ao padrão de ida, de forma que os deslocamentos mais intensos da ida e volta acontecem na sexta e sábado e a maioria dos deslocamentos da volta acontece no domingo.

A comparação entre os dois padrões de mobilidade pode ser feita pela média de deslocamentos por dia da semana, apresentada na Figura 7. A Figura 7(a) mostra o padrão Casa – Trabalho, com alto número de deslocamentos durante a semana, com um volume maior na sexta feira, e poucos deslocamentos no fim de semana. A Figura 7(b) mostra o padrão Casa – Lazer e Lazer – Casa, que representa o comportamento inverso, com um número relativamente baixo de deslocamentos durante a semana e número elevado de deslocamento no fim de semana.

Figura 7: Comparação dos deslocamentos médios por dia da semana



Casa – Trabalho



Casa – Lazer

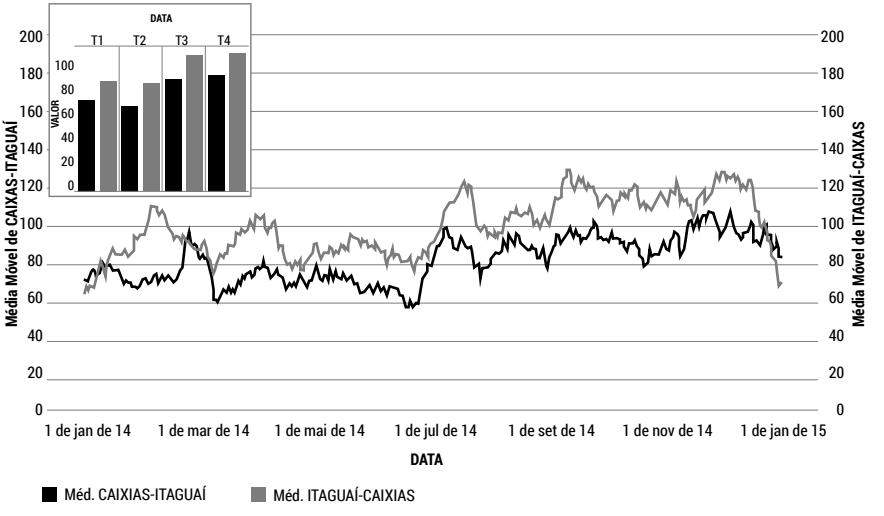
Fonte: Elaborado pelos autores.

Em geral levantamentos como o PDTU têm custo muito elevado e são realizados uma vez a cada década, ou mais. A possibilidade de cálculo de uma matriz OD por dia representa um grande potencial para a operação e monitoramento de uma grande cidade como o Rio de Janeiro. No ano de 2014 o Rio de Janeiro passou por diversas transformações viárias. Uma das alterações viárias importantes foi a inauguração da rodovia Rafael de Almeida Magalhães, conhecida como o Arco Metropolitano do Rio de Janeiro,[7] em 1 de julho de 2014. O trecho inaugurado em 2014 liga a rodovia BR 101 (Rio – Santos) no município de Itaguaí com a rodovia BR 040 (Washington Luiz) em Duque de Caxias, conectando com o trecho já existente da BR 493 até a BR 101 em Manilha. O Arco Metropolitano conecta as principais vias de acesso ao Rio de Janeiro, evitando que veículos precisem atravessar a cidade, reduzindo assim o tráfego nas vias expressas.

7 Cf.: WIKIPÉDIA. Arco Metropolitano do Rio de Janeiro. Disponível em: <https://pt.wikipedia.org/wiki/Arco_Metropolitano_do_Rio_de_Janeiro>. Acesso em: 9 ago. 2017.

A mudança de comportamento provocada pela oferta da nova via foi detectada nos deslocamentos diários entre os municípios de Duque de Caxias e Itaguaí, estimados pelos dados de CDR. A Figura 8 mostra os deslocamentos entre Duque de Caxias e Itaguaí e entre Itaguaí e Duque de Caxias, onde os dados foram filtrados pela média móvel centralizada de quatorze dias dos para facilitar a visualização. No detalhe da Figura 8 o gráfico de barras apresenta as médias trimestrais, onde pode-se observar que houve um aumento consistente do fluxo nos dois sentidos a partir de julho de 2014. Verifica-se também que o fluxo entre Itaguaí e Duque de Caxias é consistentemente maior que o fluxo entre Duque de Caxias e Itaguaí. Este resultado comprova o potencial da utilização de dados de CDR para planejamento de transportes, bem como o monitoramento e operação de grandes cidades.

Figura 8: Mudança de comportamento da média móvel dos deslocamentos entre Duque de Caxias – Itaguaí e Itaguaí – Duque de Caxias. No gráfico de barras, as médias trimestrais



Fonte: Elaboração dos autores.

CONCLUSÕES

Este trabalho apresenta um método de representação espacial por unidades geográfica, geradas pela agregação de um conjunto de antenas de telefonia celular. Esta representação facilita o cruzamento de dados de mobilidade com dados de outras fontes. Foi utilizada uma base de dados de CDR coletada durante o ano de 2014 para a geração de uma estimativa da matriz Origem – Destino (OD) por dia.

Os resultados mostram que a metodologia de cálculo de matriz OD com base nos dados de CDR é compatível com as estimativas obtidas pelo PDTU realizado em 2013. O método com fator de correção simples apresenta uma tendência a subestimar o número de viagens, principalmente para valores pequenos. Métodos alternativos de estimativa do fator de correção, bem como a utilização de estatísticas de transportes públicos para calibração dos modelos podem melhorar a precisão das estimativas.

Foram identificados dois padrões principais de mobilidade: Casa – Trabalho e Casa – Lazer (e vice-versa), a partir de suas principais características. Os resultados mostram outras aplicações possíveis que incluem o monitoramento dos fluxos urbanos e a detecção de mudanças de comportamento da mobilidade em função de alterações viárias importante. A utilização de dados de CDR também permite diversas outras aplicações em diferentes áreas.

Os resultados apresentados comprovam a aplicabilidade da utilização de dados de CDR para o planejamento e monitoramento de transportes em grandes cidades. O monitoramento da mobilidade durante todo o ano permite o acompanhamento dos resultados da implementação de políticas públicas e o planejamento mais eficiente de novas intervenções.

A utilização de dados de CDR para estimativas populacionais e de mobilidade têm aplicação em diversas setores como turismo, transporte regional, e saúde, em estudos sobre a propagação de epidemias.

AGRADECIMENTOS

Os autores agradecem a Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) e a Fundação Getulio Vargas pelo apoio financeiro para realização do projeto. O projeto foi realizado em colaboração com técnicos da Prefeitura do Rio e pesquisadores do Massachusetts Institute of Technology (MIT).

REFERÊNCIAS

ALEXANDER, L.; JIANG, S.; MURGA, M.; GONZÁLEZ, M. C. Origin-Destination Trips by Purpose and Time of Day Inferred from Mobile Phone Data. *Transp. Res. Part C Emerg. Technol.*, v. 58, p. 240-250, 2015.

BARLACCHI, G. et al. A Multi-Source Dataset of Urban Life in the City of Milan and the Province of Trentino. *Sci. Data*, v. 2, p. 150055, out. 2015.

BARNETT, I.; KHANNA, T.; ONNELA, J. Social and Spatial Clustering of People at Humanity's Largest Gathering. *PLoS One*, v. 11, n. 6, p. e0156794, 2016.

BLONDEL, V. D.; DECUYPER, A.; KRINGS, G. A Survey of Results on Mobile Phone Datasets Analysis. *EPJ Data Sci.*, v. 4, n. 10, dez. 2015.

C. E. DE ENGENHARIA DE TRANSPORTE E LOGÍSTICA. PDTU 2003. Plano Diretor de Transporte Urbano da Região Metropolitana do Rio de Janeiro. Governo do Rio de Janeiro: Secretaria de Transportes, RJ, 2003.

C. E. DE ENGENHARIA DE TRANSPORTE E LOGÍSTICA.PDTU 2013. Plano Diretor de Transporte Urbano da Região Metropolitana do Rio de Janeiro. Relatório Técnico 4, Planejamento e execução das pesquisas Parte III, Governo do Rio de Janeiro: Secretaria de Transportes, RJ, 2015.

CALABRESE, F.; COLONNA, M.; LOVISOLO, P.; PARATA, D.; RATTI, C. Real-Time Urban Monitoring Using Cellular Phones: a Case-Study in Rome. *IEEE Trans. Intell. Transp. Syst.*, v. 12, n. 1, p. 1-11, 2010.

CANDIA, J.; GONZÁLEZ, M. C.; WANG, P.; SCHOENHARL, T.; MADEY, G.; BARABÁSI, A. L. Uncovering Individual and Collective Human Dynamics from Mobile Phone Records. *J. Phys. A Math. Theor.*, v. 41, n. 22, p. 224015, 2008.

CHEN, C.; MA, J.; SUSILO, Y.; LIU, Y.; WANG, M. The Promises of Big Data and Small Data for travel Behavior (Aka Human Mobility) Analysis. *Transportation Research Part C: Emerging Technologies*, v. 68, p. 285-299, 2016.

DONG, H. et al. Traffic Zone Division Based on Big Data from Mobile Phone Base Stations. *Transp. Res. Part C Emerg. Technol.*, v. 58, p. 278-291, 2015.

DONG, L.; LI, R.; ZHANG, J.; DI, Z. Population-Weighted Efficiency in Transportation networks. *Sci. Rep.*, v. 6, n. 26377, 2016.

DOUGLASS, R. W.; MEYER, D. A.; RAM, M.; RIDEOUT, D.; SONG, D. High resolution Population estimates from Telecommunications Data. *EPJ Data Sci.*, v. 4, n. 1, p. 1-13, 2014.

GOOGLE MAPS PLATFORM. Get Started. Disponível em: <https://developers.google.com/maps/documentation/distance-matrix/>. Acesso em: 9 ago. 2017.

HOTEIT, S.; SECCI, S.; SOBOLEVSKY, S.; RATTI, C.; PUJOLLE, G. Estimating Human Trajectories and Hotspots through Mobile Phone Data. *Comput. Networks*, v. 64, p. 296-307, 2014.

IQBAL, M. S.; CHOUDHURY, C. F.; WANG, P.; GONZÁLEZ, M. C. Development of Origin-Destination Matrices Using Mobile Phone Call Data. *Transp. Res. Part C Emerg. Technol.*, v. 40, p. 63-74, 2014.

IVEY, S. S.; Badoe, D. A. Review of Policies on Access to Transportation Planning Data and Models: Implications for Transportation Planning Agencies. *J. Urban Plan. Dev.*, v. 137, n. 4, p. 438–447, 2011.

JÄRV, O.; AHAS, R.; WITLOX, F. Understanding Monthly Variability in Human Activity Spaces: A twelve-Month Study using Mobile Phone Call Detail Records. *Transp. Res. Part C Emerg. Technol.*, v. 38, p. 122-135, 2014.

JIANG, S.; FERREIRA JR., J.; GONZÁLEZ, M. C. Activity-Based Human Mobility Patterns Inferred from Mobile Phone Data: A Case Study of Singapore. *The 4th International Workshop on Urban Computing*, 2015.

KANG, C.; MA, X.; TONG, D.; LIU, Y. Intra-Urban Human Mobility Patterns: An Urban Morphology Perspective. *Phys. A Stat. Mech. its Appl.,* v. 391, n. 4, p. 1702–1717, fev. 2012.

KERAMAT JAHROMI, K.; ZIGNANI, M.; GAITO, S.; ROSSI, G. P. Simulating Human Mobility Patterns in Urban Areas. *Simul. Model. Pract. Theory*, v. 62, p. 137-156, 2016.

LIU, F.; JANSSENS, D.; WETS, G.; COOLS, M. Annotating Mobile Phone Location Data with activity Purposes Using Machine Learning Algorithms. *Expert Syst. Appl.*, v. 40, n. 8, p. 3299-3311, 2013.

MCNALLY, M. G. The Four-Step Model. In *Handbook of Transport Modelling*, v. 1, 2007, p. 35-53.

MOREIRA-MATIAS, L.; GAMA, J.; FERREIRA, M.; MENDES-MOREIRA, J.; DAMAS, L. Time-Evolving O-D Matrix Estimation using high-speed GPS data streams. *Expert Syst. Appl.*, 2015.

PAPANDREA, M.; JAHROMI, K. K.; ZIGNANI, M.; GAITO, S.; GIORDANO, S.; ROSSI, G. P. On the Properties of Human Mobility. *Comput. Commun.*, v. 87, p. 19-36, 2016.

RUBIO, A.; SANCHEZ, A.; FRIAS-MARTINEZ, E. Adaptive Non-Parametric Identification of Dense Areas Using Cell Phone Records for Urban Analysis. *Eng. Appl. Artif. Intell.*, v. 26, n. 1, p. 551-563, 2013.

SCHNEIDER, C. M.; BELIK, V.; COURONNÉ, T.; SMOREDA, Z.; GONZÁLEZ, M. C. Unravelling Daily Human Mobility Motifs. *J. R. Soc. Interface*, v. 10, n. 20130246, 2013.

SIMINI, F.; GONZÁLEZ, M. C.; MARITAN, A.; BARABÁSI, A. L. A Universal Model for Mobility and Migration Patterns. *Nature*, v. 484, n. 7392, p. 96-100, fev. 2012.

SMOREDA, Z.; OLTEANU-RAIMOND, A. M.; COURONNÉ, T. Spatiotemporal Data from Mobile Phones for Personal Mobility Assessment. In: [S.a]. *Transport Survey*

Methods: Best Practice for Decision Making. [S. l.]: Emerald Group Publishing Limited, 2013, p. 745-767.

TELECO. Estatísticas do Brasil - Geral. Disponível em: <http://www.teleco.com.br/estatis.asp>. Acesso em: 9 ago. 2017.

TELECO. Numeração Telefônica. Disponível em: <http://www.teleco.com.br/num.asp>. Acesso em: 6 abr. 2017.

TSEKERIS, T.; STATHOPOULOS, A. Gravity Models for Dynamic Transport Planning: Development and Implementation in Urban Networks. *J. Transp. Geogr.*, v. 14, n. 2, p. 152-160, 2006.

TOOLE, J. L.; ÇOLAK, S.; STUART, B.; ALEXANDER, L. P.; EVSUKOFF, A.; GONZÁLEZ, M. C. The Path Most Traveled: Travel Demand Estimation Using Big Data Resources. *Transp. Res. Part C Emerg. Technol.*, v. 58, p. 162-177, 2015.

WANG, W.; PAN, L.; YUAN, N.; ZHANG, S.; LIU, D. A Comparative Analysis of Intra-City Human Mobility by Taxi. *Phys. A Stat. Mech. its Appl.*, v. 420, p. 134-147, 2015.

WIKIPÉDIA. Arco Metropolitano do Rio de Janeiro. Disponível em: <https://pt.wikipedia.org/wiki/Arco_Metropolitano_do_Rio_de_Janeiro>. Acesso em: 9 ago. 2017.

WIKIPÉDIA. Diagrama de Voronoy. Disponível em: <https://pt.wikipedia.org/wiki/Diagrama_de_Voronoy>. Acesso em: 12 ago. 2017.

WIKIPÉDIA. Greater Rio de Janeiro. Disponível em: <https://en.wikipedia.org/wiki/Greater_Rio_de_Janeiro>. Acesso em: 6 abr. 2017

WIKIPÉDIA. Região Metropolitana do Rio de Janeiro. Disponível em: <https://pt.wikipedia.org/wiki/Região_Metropolitana_do_Rio_de_Janeiro>. Acesso em: 6 abr. 2017.

WESOLOWSKI, A. et al. Evaluating Spatial Interaction Models for Regional Mobility in Sub-Saharan Africa. *PLoS Comput. Biol.*, v. 11, n. 7, p. 1-16, 2015.

YANG, Y.; JIANG, S.; VENEZIANO, D.; ATHAVALE, S.; GONZALEZ, M. C. TimeGeo: Modeling Urban Mobility Without Travel Surveys. *Proc. Natl. Acad. Sci. U. S. A.*, v. 104, n. 51, pp. 20167-20172, 2007.

ZHONG, C.; MANLEY, E.; MÜLLER ARISONA, S.; BATTY, M.; SCHMITT, G. Measuring Variability of Mobility Patterns from Multiday Smart-Card Data. *J. Comput. Sci.*, v. 9, p. 125-130, 2015.

PORTO MARAVILHA, DEMOLIÇÃO DA PERIMETRAL E QUEBRA DE PARADIGMAS URBANOS: OS DESAFIOS DA GESTÃO DAS MUDANÇAS

ALBERTO SILVA

INTRODUÇÃO

O Rio de Janeiro é mundialmente conhecido por suas belezas naturais. No entanto, à exemplo do que vemos nas grandes cidades, a sua evolução urbana produziu vários efeitos negativos em termos sociais, ambientais e econômicos. O fato é que estas cidades existem, com suas complexidades e contradições objetivas e subjetivas. Transformá-las em cidades melhores representa um dos grandes desafios atuais. Na busca de soluções não basta apontar o que fazer. É preciso considerar a seguinte pergunta: como fazer a transição desta cidade que existe, para a cidade que garanta um futuro melhor para o meio ambiente e para as pessoas? Esta é a questão para a qual este artigo pretende dar alguma contribuição a partir da análise da experiência de gestão da implantação das obras de infraestrutura urbana na região central da cidade do Rio de Janeiro, no âmbito da Operação Urbana Consorciada da Região do Porto do Rio de Janeiro, conhecida como Porto Maravilha, que, dentre várias outras intervenções, implicou na demolição de cinco quilômetros de viaduto, conhecido como elevado da Perimetral.

Atualmente, mais da metade da população mundial vive em áreas urbanas. Serão perto de 66% até 2050, de acordo com estimativas das Nações Unidas (UN, 2014). É nas cidades, sobretudo nas megalópoles, onde ocorre a maior parte do consumo de recursos naturais e manufaturados e das emissões que impactam para as mudanças climáticas. Elas são os polos dinâmicos da economia global[1] e é nelas, que as desigualdades sociais se manifestam de forma bastante acentuada, sobretudo nos chamados países em desenvolvimento (UN-HABITAT, 2010; IPCC, 2014).

1 Ver também: MORI, CHRISTODOULOU, 2012; HAMMER *et al.*, 2011; ALBINO; BERARDI; DANGELICO, 2015, p. 3.

A urbanização segue crescendo com base em paradigmas que precisam ser revistos, para que possamos promover um padrão de desenvolvimento urbano sustentável, entendido aqui como um processo em que as dimensões ambiental, social e econômica sejam mutuamente equilibradas (ELKINGTON, 1999; BECKS, 1992; LEMKOW e TÀBARA, 2006), conforme apontado pelo 11º Objetivo do Milênio das Nações Unidas, que orienta a Nova Agenda Urbana defendida pela UN-HABITAT.[2]

Uma gestão urbana comprometida com esta agenda necessita contemplar os processos de transformação das cidades para se adequarem aos novos paradigmas, o que representa um imenso desafio, pois envolve mudanças objetivas (materiais) e subjetivas (culturais). As cidades, com suas intrincadas e complexas funções e redes de relações não podem simplesmente parar para que ajustes sejam feitos. Sobretudo se considerarmos que esta troca de paradigmas tende a ocorrer em tempos e ritmos diferentes. Ao processo de manter a cidade funcionando ao mesmo tempo em que se promovem as necessárias transformações com base em novos paradigmas é o que chamo aqui de gestão da mudança. Algumas mudanças, como instalação de novos equipamentos de monitoramento e iluminação pública, por exemplo, pouco ou nada afetam as rotinas das cidades. No entanto, mudanças estruturantes, como implantar uma infraestrutura viária ou novo padrão de ocupação e uso do solo, tendem a interferir intensamente no dia a dia dos grandes centros urbanos. O planejamento das soluções estruturantes, além de definir "o que deve ser feito", necessita tomar em conta "o como será feito" para que o remédio não cause outros problemas. É preciso ter em conta os impactos na vida da cidade e na prestação dos serviços urbanos – públicos e privados. A gestão da mudança, nestes casos é crucial para que prazos, custos e, principalmente, objetivos sejam cumpridos e os transtornos sejam os mínimos possíveis. Além disso, o próprio processo de transformações físicas, pode servir também para promover necessárias mudanças culturais.

Há várias abordagens visando compreender a questão urbana e instrumentalizar processos de transformação.[3] Dentre estas, a que trata das chamadas

2 UN, Resolution adopted by the General Assembly, 2016.

3 Há várias nominações atualmente: Green Growth, Smart Growth, Smart Grid. Destacamos o Desenvolvimento Orientado ao Transporte Sustentável. Com forte cunho instrumental, muito bem elaborado pelo ITDP e Embarq Brasil, busca alinhar mobilidade urbana, com foco no transporte público com ocupação e uso do solo; e o Direito à Cidade, de cunho primordialmente analítico, utilizado por autores como David Harvey, tem foco na crítica à mercantilização da cidade e nos seus efeitos negativos que ampliam as desigualdades espaciais e sociais e produzem a gentrificação. Defendem a participação e a gestão democrática como forma de reverter tais situações.

cidades inteligentes – *smart cities* –, confere grande ênfase à questão da gestão urbana. Inicialmente baseada no uso das Tecnologias da Informação (TI) para operação de serviços urbanos (ANTTIROIKO, A.V *et. al.*, 2013; NAPHADE, M. *et.al.*, 2011; HARRISON, DONNELLY, 2011; IBM, 2009), para vários autores, esta abordagem estaria evoluindo como forma de contribuir para uma cidade sustentável (ABDALA *et al.*, 2014; LEIGH, N.G., HOELZEL, N.Z, 2012), entendida aqui, conforme definido por Romero:

> […] cidade sustentável é o assentamento humano constituído por uma sociedade com consciência de seu papel de agente transformador dos espaços e cuja relação não se dá pela razão natureza-objeto e sim por uma ação sinérgica entre prudência ecológica, eficiência energética e equidade socioespacial. (ROMERO, 2007, p. 51).

A abordagem de cidade inteligente tem evoluído para uma concepção sistêmica e integrada, incorporando governança e participação da sociedade civil como elementos relevantes:

> Uma cidade inteligente se forma quando investimentos em capital humano e social e tradicional (transporte) e moderna (TIC) infraestruturas tecnologias de comunicação alimentam um crescimento econômico sustentável e qualidade de vida, com uma gestão sábia dos recursos naturais por meio de uma governança participativa. (CARAGLIU; DEL BO; NIJKAMP, 2011)

Em estudo recente, o BID defende que:

> Uma Cidade Inteligente é aquela que coloca as pessoas no centro do desenvolvimento, incorpora tecnologias da informação e comunicação na *gestão urbana* e utiliza esses elementos como ferramentas que estimulam a formação de um governo eficiente, que engloba o planejamento colaborativo e a participação cidadão. *Smart Cities* favorecem o desenvolvimento integrado e sustentável tornando-se mais inovadoras, competitivas, atrativas e resilientes, melhorando vidas. (BID, 2016, p. 16, grifo nosso)

Assim, as TI não constituem um fim em si. Elas passam a ser tomadas como suporte para uma gestão urbana que propicie melhor qualidade para o meio ambiente e para a vida das pessoas, conforme defendido por Weiss (2016) ao analisar a importância das TI para melhorar a gestão das cidades. Nesse sentido, não se trata de melhorar o modo como as cidades são atualmente. Conforme já dito, é preciso romper com paradigmas atuais. E a gestão da mudança de paradigmas é fundamental, como parte do processo formação das cidades inteligentes e sustentáveis.

No Brasil, de acordo com o Instituto Brasileiro de Geografia e Estatística, já são mais de 84% da população vivendo em áreas urbanas (IBGE, 2013), convivendo com problemas de infraestrutura, mobilidade urbana, sanea-

mento e habitação, com reflexos negativos para o desenvolvimento social e econômico e gerando problemas ambientais. Nas grandes cidades do país, a situação é ainda mais grave, com o espaço urbano expressando as grandes disparidades sociais do país, de acordo com Índice de Bem-Estar Urbano dos Municípios Brasileiros (IBEU-Municipal) (OBSERVATÓRIO DAS METRÓPOLES, 2016).

Na região metropolitana do Rio de Janeiro, que abriga mais de doze milhões de habitantes, a situação não é diferente. Ao longo de décadas, um padrão de urbanização que empurrou as populações para as periferias, mesmo sem dotação de infraestrutura adequada, produz efeitos negativos para a economia, o meio ambiente e a qualidade de vida da maioria da população (SEBRAE, 2013). De acordo com uma pesquisa da Federação das Indústrias do Rio de Janeiro (FIRJAN), os trabalhadores da região metropolitana gastam em média 141 minutos entre casa e trabalho todos os dias, no "engarrafamento nosso de cada dia". A mesma pesquisa estima que os engarrafamentos diários custaram R$ 17.425.491, 5,9% do PIB do Estado do Rio de Janeiro, em 2012 (FIRJAN, 2015).

Somada a esta trajetória, uma grande parte da área central da cidade, que servia ao Porto do Rio de Janeiro, veio perdendo suas funções desde os anos de 1960. A região portuária tornou-se um vazio urbano, fruto de um processo de degradação e abandono, apesar de sua localização estratégica. Por ela passam os principais acessos rodoviários ao centro cidade e de conexão entre a Zona Sul e as zonas Norte e Oeste e a Região Metropolitana, além da proximidade com os dois aeroportos da cidade.

Entre 2012 e 2016 a Prefeitura da Cidade do Rio de Janeiro fez importantes investimentos para reverter as tendências de evolução desta situação por meio da implantação da Operação Urbana Consorciada da Região do Porto do Rio de Janeiro, conhecida como Porto Maravilha, e do VLT Carioca. Executar estas transformações urbanísticas e viárias, que tiveram como principal evento a demolição dos cinco quilômetros do elevado da Perimetral, representou um gigantesco esforço de gestão para mitigar os impactos das obras sobre o precário trânsito, os transportes públicos e a prestação de serviços públicos e privados na área central da cidade.

Este artigo é um relato sobre as inovações na condução do processo de mudanças, que deixam importantes lições para uma gestão urbana inteligente, e serve para aqueles que queiram aprofundar uma análise informada sobre a implantação do Porto Maravilha. Para tanto, faremos:

ii. uma caracterização das mudanças pretendidas pela Operação Urbana Porto Maravilha e pelo VLT Carioca e sua relação com a Nova Agenda Urbana e a abordagem das Cidades Inteligentes;

iii. uma apresentação sobre o contexto, os desafios e os objetivos do Plano de Mitigação para a Demolição da Perimetral;

iv. uma análise do processo de implantação do Plano como um exercício de ação integrada de vários atores, o que permitiu a otimização de seus recursos;

v. algumas reflexões e lições deixadas por este processo para a geração de uma gestão urbana inteligente.

AS MUDANÇAS PRETENDIDAS: OS OBJETIVOS DO PORTO MARAVILHA E A COMPLEMENTARIEDADE DO VLT

A Operação Urbana Consorciada Porto Maravilha, criada pela Lei Complementar Municipal (LMC) 101/2009, com vigência de 30 anos, está sendo implementada na Área de Especial Interesse Urbanístico (AEIU) da região do Porto. Seus princípios, diretrizes e objetivos apresentam forte alinhamento com os parâmetros defendidos pela Nova Agenda Urbana e pela abordagem cidades inteligentes. Tanto no que se refere às intervenções, quanto do ponto de vista do processo de gestão das mudanças que vem sendo implementado. O planejamento estratégico da operação é baseado em três eixos de intervenção complementares entre si: requalificação urbana, desenvolvimento sócio econômico e desenvolvimento imobiliário.

De acordo com a LMC 101/2009, em seu artigo 2º, a Operação Urbana Consorciada Porto Maravilha tem por finalidade:

> Promover a reestruturação urbana da AEIU (Área de Especial Interesse Urbanístico), por meio da ampliação, articulação e requalificação dos espaços livres de uso público da região do Porto, visando à melhoria da qualidade de vida de seus atuais e futuros moradores, e à sustentabilidade ambiental e socioeconômica da região (LCM 101/2009).

O parágrafo 1º deste mesmo artigo estabelece um conjunto de princípios para o Porto Maravilha, o primeiro dos quais é "a priorização do transporte coletivo sobre o individual". Já o quinto princípio refere-se "à integração da área com a área central da Cidade e o estímulo ao uso residencial, possibilitando melhor aproveitamento da estrutura urbana existente" (LCM 101/2009).

No parágrafo 2º são estabelecidas dezessete diretrizes que apontam para a ocupação e uso sustentável do solo, a valorização do patrimônio e dos espaços públicos, a integração da área com o restante do centro da cidade, a promoção da igualdade social e a mobilidade urbana. (LCM 101/2009)

A LCM 101/2009 declara a AEIU como de uso misto e estabelece novos índices de ocupação dos terrenos, parâmetros de sustentabilidade para as edificações e cria um estoque de potencial adicional de construção a ser utilizado de forma onerosa, por meio da compra dos Certificados de Potencial Adicional de Construção (Cepacs). O novo plano de ocupação reconhece e reforça a Área de Proteção do Ambiente Cultural dos Bairros da Saúde, Gamboa e Santo Cristo (APAC – SAGAS), e mantem o desenho urbano existente, apenas alterando as funções e características de algumas vias para adequação ao novo padrão de mobilidade urbana.

A Lei estabelece que a Operação Urbana deve promover ações de desenvolvimento social e delimita um programa de requalificação urbana de uma área de cinco milhões de metros quadrados, do qual constam renovação da infraestrutura urbana adequação do sistema viário e um novo padrão de urbanização com prioridade para o pedestre e o transporte público em detrimento do transporte individual motorizado, em concordância com os princípios legais estabelecidos.

Este programa, executado por meio de um contrato de Parceria Público-Privada entre a Companhia de Desenvolvimento Urbano da Região do Porto do Rio de Janeiro (CDURP) e a Concessionária Porto Novo, com duração de quinze anos e valor de R$ 7,6 bilhões, inclui as obras de requalificação e os serviços de manutenção e operação da região, pagos com os recursos advindos da venda dos Cepacs.[4]

Além da prestação de serviços de manutenção e conservação de vias, praças, monumentos, sinalização vertical e horizontal, limpeza urbana, coleta domiciliar de lixo, operação e manutenção da iluminação pública e operação do trânsito em toda a área, até dezembro de 2016 foram construídos (CDURP, 2016):

- redes de drenagem, água, esgotos, gás, energia elétrica, telecomunicações e iluminação pública em aproximadamente setenta quilômetros de ruas e avenidas;
- demolição da perimetral e sua substituição por uma nova via expressa, a construção de uma nova avenida, três quilômetros de pista para o futuro BRT Transbrasil e de nove quilômetros de túneis;
- ampliação de calçadas e praças e um novo passeio público com três quilômetros e meio de extensão, com o plantio de mais de cinco mil arvores.

Como parte dos preparativos para a Operação Urbana Porto Maravilha, o Estudo de Impacto de Vizinhança (EIV) de 2010, considerando o cenário de

4 Para mais informações sobre Cepacs, ver: SILVA. Lei Federal 10.257/2001; Resoluções CVM 400, 401 e 472. 2015.

adensamento da região, apontou a necessidade de qualificar a mobilidade urbana na região central da cidade. Para responder à esta questão foram utilizados estudos preliminares feitos pelo Instituto Pereira Passos (IPP) para implantação do Veículo Leve sobre Trilhos (VLT), que, em grande medida se baseavam na ideia da recuperação da malha dos antigos bondes que circulavam pelas ruas da cidade até os anos 50.

Projetado como modal de média capacidade, o VLT foi também viabilizado por meio de um contrato de PPP entre o Município do Rio de Janeiro e a Concessionária VLT Carioca, tendo a CDURP como agente fiscalizador da implantação e operação, com duração de 25 anos e investimentos de R$ 1,157 bilhão, sendo R$ 625 milhões do Privado e R$ 532 milhões do Programa de Aceleração do Crescimento (PAC) da Mobilidade.[5] Ele tem como objetivo principal integrar os diversos serviços de transporte público que chegam ou cruzam a área do Porto Maravilha e o Centro da Cidade.[6] Sua malha de 28 km de trilhos e 31 paradas, ligam a estação das barcas, Central do Brasil, Rodoviária Novo Rio, várias estações do Metrô e terminais de ônibus, incluindo do futuro BRT Transbrasil, além do Aeroporto Santos Dumont e do Terminal Marítimo de Passageiros. Quando em operação plena terá capacidade para transportar até 300 mil passageiros por dia.

Suas características técnicas, além do conforto para os usuários, foram projetadas para valorizar o espaço público e a paisagem histórica da região. O sistema de alimentação não utiliza catenárias, o que evita a poluição visual dos cabos aéreos. Por ser elétrico, o nível de emissões e ruído são próximos de zero. As obras de infraestrutura tiveram início em 2014. A primeira etapa, entre a Rodoviária Novo Rio ao Aeroporto Santos Dumont entrou em operação em julho de 2016, já integrado ao Bilhete Único Carioca. Um segundo trecho, entre o Campo de Santana e a Praça XV (Estação das Barcas) começou a operar em março de 2017. O sistema já transporta mais de sessenta mil passageiros por dia.

As intervenções do Porto Maravilha e a implantação do VLT se reforçam mutuamente, para fortalecer a atratividade do lugar e torná-lo referência

5 Para informações sobre o VLT, ver: PORTO MARAVILHA. Porto Maravilha. Disponível em:<http://www.portomaravilha.com.br/veiculolevesobretrilhos>. Para informações sobre o contrato de PPP, ver: <http://www.portomaravilha.com.br/documentos>. Acesso em: 05 dez. 2018.

6 Os serviços de transporte público no Rio de Janeiro são prestados por meio de ônibus, que transportam o maior número de passageiros, seguido pelos trens, metrô e barcas. Estes serviços, historicamente, atuam numa lógica de concorrência, com baixo grau de integração. Principalmente no que se refere aos operadores de ônibus, que concorrem entre si e com os demais serviços.

de espaço urbano sustentável. Eles demonstram aderência aos princípios e diretrizes de uma cidade inteligente e sustentável, com a consequente quebra de paradigmas que vêm orientando a urbanização da cidade por décadas. A renovação urbana promove o acesso a melhores serviços urbanos e ao mesmo tempo, cria oportunidades de geração de emprego e renda, melhorando condições sociais dos atuais moradores (SILVA, 2013). A isto se acrescenta o trabalho de valorização da identidade e da cultura da região, o que fortalece autoestima dos moradores. Este processo de inclusão social induz objetiva e subjetivamente a sua permanência, uma vez que a valorização do patrimônio e da memória, que tem relevância singular (SILVA, 2015), se soma à sua localização estratégica para estimular a vinda de novos moradores e empresas. A prioridade para o adensamento populacional e o uso misto contribui, tanto do ponto de vista conceitual, quanto em termos práticos, para melhorar a mobilidade urbana, uma vez que cria oportunidade para que mais pessoas vivam próximas do local de trabalho, além de constituir um ambiente urbano mais equilibrado. O incremento do transporte público e as mudanças no sistema viário constituem um novo padrão de mobilidade urbana e permitem a maior integração desta região com o restante da cidade, também contribuindo para sua maior atratividade.

A intervenção mais marcante para a nova mobilidade urbana e do Porto Maravilha em geral foi a demolição dos cinco quilômetros do elevado da Perimetral. Construído ao longo das décadas de 1960 e 1970, o viaduto, além de não atender às suas funções para a mobilidade urbana, era o principal elemento urbano responsável pela degradação do patrimônio histórico e ambiental da região e o símbolo de um paradigma urbano que pensa mais nos carros do que nas pessoas.

Sua retirada possibilitou a implantação de uma nova via expressa e do Binário do Porto, gerando um aumento estimado de 25% na capacidade de tráfego, em relação à configuração original. (SILVA, 2014; SINERGIA, 2013). Além disso, permitiu a criação da Orla Conde, uma área de pedestres com 3,5 km de extensão valoriza o ambiente urbano e o patrimônio da região e reconecta o centro da cidade com a Baia de Guanabara.

O PLANO DE MITIGAÇÃO

Para executar as obras de infraestrutura urbana e viárias do Porto Maravilha seria necessária a interdição de vias já saturadas, o que prejudicaria ainda mais o já bastante congestionado trânsito do centro do Rio, com reflexos em toda a Região Metropolitana. A principal ferramenta neste

processo foi o Plano de Mitigação para a Demolição da Perimetral, que promoveu a otimização do sistema viário, e estimulou mudanças culturais em relação à mobilidade urbana em articulação com a gestão das obras e a prestação de serviços.

O Plano envolveu a ação coordenada de diversos órgãos da prefeitura, principalmente: CDURP, Secretaria Municipal de Transportes (SMTR), Companhia de Engenharia de Tráfego da Cidade do Rio de Janeiro (CET Rio), Secretaria de Ordem Pública (SEOP), Guarda Municipal e das concessionárias Porto Novo (CPN) e VLT Carioca. E também com colaboração da Secretaria de Transportes do governo estadual, e de todas as concessionárias de transporte público e serviços de água e esgoto, fornecimento de energia, gás e telecomunicações. Logo de início, ficou claro que a articulação entre estes vários agentes era praticamente inexistente e que cada um operava dentro de suas próprias lógicas e interesses. Para executar as mudanças desejadas era preciso construir uma visão estratégica de conjunto em torno dos princípios e objetivos do Porto Maravilha e de futuro para a cidade.

CONTEXTO

Em 2010 o Rio de Janeiro tinha pela frente um intenso calendário de grandes eventos que culminaria com os Jogos Olímpicos e Paralímpicos de 2016, passando pelos Jogos Mundiais Militares (2011), A Rio+20 (2012), a visita do Papa Francisco e a Copa das Confederações da Fifa (2013), a Copa do Mundo da Fifa (2014) e as comemorações pelos 450 anos da Cidade Maravilhosa (2015). A cidade já estava habituada a grandes eventos, como o Réveillon em Copacabana, que reúne cerca de dois milhões de pessoas todos os anos, e o Carnaval, com os desfiles no Sambódromo e os blocos carnavalescos, que nos últimos anos apresentaram um crescimento fantástico, ampliando os dias de festa dos tradicionais quatro dias para mais de dez, levando mais de um milhão e meio de pessoas todos às ruas todos os dias. No entanto, estes são eventos que, embora modifiquem o sistema viário da cidade, ocorrem em feriados e com grande parte da população participando das festas.

Um fato importante foi a inauguração do Centro de Operações Rio (COR), já como parte para os preparativos para os Jogos de 2016. O COR é uma central de informações e monitoramento de alta tecnologia com a função de integrar as ações e orientar as decisões da prefeitura com relação à mobilidade, prevenção e resposta a situações de emergência. Ele viria cumprir importante papel para a implementação do Plano, que por sua vez, também contribuiu para aprimorar seu funcionamento.

Em 2009, a situação do trânsito nos horários de pico da manhã e da tarde na região central era de congestionamentos diários, com as principais vias saturadas (CDURP, 2010, p. 125-126). Uma delas, o elevado da Perimetral, representava importante conexão das principais vias de chegada ao centro, como Avenida Brasil, Linha Vermelha e Ponte Rio Niterói, com o Centro e a Zona Sul, concentrando o transporte individual. A Avenida Rodrigues Alves, sob o elevado, absorvia principalmente o fluxo de ônibus vindos das zonas norte, oeste e da baixada fluminense ao centro e linhas ligando a Rodoviária Novo Rio à zona sul. Estas duas vias deveriam ser interditadas para a execução das obras do novo sistema viário definido no âmbito do Porto Maravilha. A outra via com a função de fazer esta ligação, a Avenida Francisco Bicalho, também bastante saturada, não tinha capacidade para absorver o fluxo das outras duas vias. Para fazer as obras, era necessário repensar toda a mobilidade da região central e seus reflexos para o cotidiano do centro administrativo e financeiro da segunda maior região metropolitana do país (SINERGIA, 2013).

PREMISSA, OBJETIVO E AÇÕES

A premissa fundamental do Planejamento foi a priorização do transporte público em detrimento do individual – carros. Naquela altura já tínhamos claro que, para além do período de obras, estávamos a construir uma nova mobilidade urbana, em consonância com as finalidades da Operação Urbana. (LMC 101/2009; SINERGIA, 2013; ARRAES, SILVA, 2014; SINERGIA, 2016).

A partir do reconhecimento de que era inevitável a piora da situação, o objetivo principal era reduzir o impacto das obras sobre o já precário trânsito na área central da cidade. Foram estabelecidas metas de limite de incremento dos congestionamentos para os principais eixos de trafego, para os horários de pico da manhã e da tarde (SINERGIA, 2013).

Para a definição das metas, o uso de tecnologias de planejamento e gestão de tráfego foram fundamentais. Para coleta de informações atualizadas, a Prefeitura ampliou a quantidade de equipamentos de contagem de fluxos (OCRs). As informações coletadas foram utilizadas em *softwares* de simulação de tráfego, o que permitiu uma melhor compreensão da situação inicial e serviu para visualizar virtualmente as propostas de ajustes do trânsito, antes de testá-las na prática.

As propostas buscavam principalmente: otimizar o uso do sistema viário, priorizar o fluxo dos ônibus, introduzir e/ou intensificar a integração dos modais de transporte público, potencializar a oferta de capacidade em cada

um deles, restringir o uso de automóveis e estabelecer intenso canal de comunicação sobre as ações junto à população. Um grande desafio deste exercício era conciliar as necessidades do trânsito a nível macro – fluxos da região metropolitana – com o micro – fluxos internos dos bairros onde as obras estavam sendo executadas.

A otimização do sistema viário passou por rever a capacidade e funcionalidade das ruas e avenidas e também o sistema de operação, adequando sinalização semafórica. A prioridade para o fluxo dos ônibus ocorreu por meio da criação de corredores de BRS.[7] Esta ação foi concomitante com medidas de racionalização de linhas e seus trajetos, e a intensificação da integração operacional entre os ônibus e destes com trem, metrô e barcas. Houve ainda esforço destas concessionárias para aumentar sua oferta de viagens (SINERGIA, 2016). Estas ações envolveram também os ônibus fretados por condomínios – em sua maioria da Barra da Tijuca – que transportam seus moradores para o centro da cidade.

A restrição aos automóveis se deu objetivamente pela redução drástica do número de vagas de estacionamento na área central da cidade, de 4.333 para 2.170, grande parte ofertada por estabelecimentos clandestinos. E subjetivamente pela campanha de comunicação para incentivar o uso dos transportes públicos. Outra medida foi a restrição dos horários de circulação de caminhões, alterando a logística do comércio e dos serviços públicos, incluindo a prestação de serviços da Porto Novo e também das obras.

O trabalho de comunicação foi realizado principalmente pela CDURP e pela Concessionária Porto Novo, contou também com o Site Cidade Olímpica, da Prefeitura, e mais tarde, com a Concessionária VLT Carioca. Foram produzidos diversos materiais de divulgação, impressos e eletrônicos. Estes, sob a forma de vídeos e postagens, foram divulgados nas mídias sociais da CDURP, Porto Novo, Cidade Olímpica e também das concessionárias de transporte público. Houve também campanhas com anúncios nas principais emissoras de rádio. Quanto aos materiais impressos, foram produzidos folhetos com distribuição por equipes treinadas, nos edifícios, nos locais de grande concentração de pessoas, como terminais e pontos de ônibus e estações das barcas, trem e metrô, onde também foram fixados painéis informativos para a população em toda região central. Cada

7 Vale lembrar que em dezembro de 2009 foi criado o Bilhete Único Carioca e em fevereiro de 2010 o Bilhete Único Intermunicipal. Ainda que com lacunas, ambos representaram um grande avanço na integração tarifária dos transportes públicos no Rio de Janeiro. Em fevereiro de 2013, a Prefeitura adotou o sistema de tarifa única para os ônibus. Essas medidas foram importantes para estimular o uso do transporte público.

alteração no trânsito e na circulação dos ônibus era precedida de coletiva de imprensa liderada pelo prefeito, para marcar a importância das ações.

Para dar conta do equilíbrio dos impactos das mudanças entre os níveis macro e micro, a CDURP e as Concessionária Porto Novo e VLT Carioca mantinham equipes dedicadas ao contato permanente com os moradores para informar sobre as alterações e coletar contribuições e críticas para eventuais ajustes das ações, tanto referentes ao cronograma das obras, quanto às medidas mitigadoras, para minimizar os impactos sobre o cotidiano da região.

A GESTÃO DO PROCESSO DE IMPLANTAÇÃO

A CDURP, juntamente com a SMTR, a CET Rio, o COR e a Concessionária Porto Novo vinham atuando de modo coordenado no Planejamento das obras e das ações de mitigação de impactos sobre o trânsito (SINERGIA, 2013).[8] Na medida em que as obras avançavam, o planejamento ganhava maior complexidade, servindo com aprendizagem para a fase de interdição da Perimetral e da Avenida Rodrigues Alves.

O planejamento estabeleceu um conjunto de fases para a implantação das obras e das medidas de mitigação.[9] A definição das alternativas passava pelo crivo dos vários atores envolvidos e os debates sempre confrontavam as perspectivas e interesses de cada setor. Nos casos em que não havia consenso, a solução passava pela mediação do prefeito. Esse método deixava claro o entendimento de que as soluções não tinham somente uma dimensão técnica. Era sempre necessário "medir o pulso da população", no sentido de avaliar se, apesar de dada solução técnica se apresentar como a melhor, naquele momento, em função da dinâmica da cidade, ela seria a mais adequada. Por outro lado, o ritmo das obras servia de forte lastro para um comportamento compreensivo por parte da maioria da população.

O plano estabeleceu um sistema de monitoramento bastante rigoroso e mecanismos para ajustes permanentes, para garantir sua eficácia. As medições eram feitas a cada duas semanas para verificar a eficácia das ações,

8 Ver capítulo 6.2 do "Relatório de Atualização do Estudo de Impacto de Vizinhança (EIV) da Operação Urbana Consorciada da Região do Porto do Rio de Janeiro", elaborado pela Sinergia Estudos e Projetos. Cf.: SINERGIA. Relatório de atualização do estudo de impacto de vizinhança (EIV) da operação urbana consorciada da região do Porto do Rio de Janeiro. Rio de Janeiro: Cdurp, 2013. http: <//www.portomaravilha.com.br/conteudo/estudos/atualizacao-eiv-e-de-trafego/volume-1.pdf>. Acesso em: 05 abr. 2017.

9 *Ibidem*, p. 106.

no sentido de manter o trânsito dos eixos selecionados dentro das metas estabelecidas. Caso contrário, novas ações deveriam ser implementadas.

As interdições foram sempre precedidas da implantação de alternativas viárias de mitigação, que eram testadas antes de serem implantadas, primeiro por meio simulações e, depois, nas ruas. Desse modo, havia tempo tanto para a população se adaptar, como para que eventuais ajustes e correções fossem feitos antes de efetivar as mudanças. Isso exigiu também preparação muito intensa, para que as medidas fossem eficazes e não comprometessem o cronograma de obras. Vale lembrar que naquele momento a CPN, responsável pela execução das obras, já havia assumido a prestação dos serviços urbanos na área do Porto Maravilha, que incluía a operação do trânsito, limpeza urbana e coleta de lixo domiciliar. Este é aspecto que demonstrou a adequação do modelo de PPP adotado. A CPN logo percebeu a necessidade de qualificar a coordenação entre gestão e o monitoramento das obras e dos serviços. Um exemplo era o impacto das obras sobre a limpeza urbana. A concessionária tomou medidas tanto nos canteiros, para evitar sujeira dos veículos das obras nas ruas, quanto nas rotinas dos serviços de limpeza, para evitar sólidos em suspensão, de modo a evitar queda da sua nota de desempenho. Resultado, ruas limpas mesmo durante o intenso período de obras.

Uma vez encaminhadas as interdições, começavam os desafios para a execução das obras de infraestrutura de água, esgoto, drenagem, energia elétrica, gás e telecomunicações e de urbanização. Para não gerar interrupções na prestação destes serviços, a nova infraestrutura tinha que ser feita e entrar em funcionamento antes de desativar a existente. Em função do espaço físico, da sobreposição destas redes e das condições do subsolo, este foi um imenso desafio enfrentado.

Os projetos de infraestrutura dependiam da aprovação de cada concessionária. Estas, por sua vez, forneciam suas especificações técnicas e seus cadastros de rede para elaboração dos projetos. No entanto, quando as ruas eram escavadas, a situação encontrada era bastante diversa do que aqueles apresentavam, sendo necessário rever o que havia sido projetado. Isso ocorreu inúmeras vezes ao longo das obras.

Além desses fatores, em conformidade com as normas brasileiras, as obras eram acompanhadas por arqueólogos sob orientação do Instituto do Patrimônio Histórico Nacional (IPHAN). Essa regra se aplica à toda área do Porto Maravilha e das obras do VLT. Durante as escavações para construção das infraestruturas, caso fosse encontrado algo de potencial valor arqueológico, as obras somente podiam avançar após aprovação daquele órgão sobre as medidas a serem tomadas em relação aos achados. E

nestes casos, o grande problema era a total falta de previsibilidade.[10] Dentre tantos, o Cais do Valongo declarado em julho de 2017 como Patrimônio da Hunanidade, é o maior exemplo mais relevante, que demandou mudanças importantes nos projetos de infraestrutura e urbanização.

Cada avanço da obra dependia do entendimento entre este conjunto de atores. Exigências técnicas e cronogramas com lógicas diferentes tinham que ser conciliados a cada passo das obras.

Somando as diferentes características e exigências técnicas de cada tipo de rede – água, esgoto, drenagem, gás, energia elétrica, telecomunicações –, várias vezes, na hora de compatibilizar os projetos no campo, simplesmente não havia espaço no subsolo para todas estas infraestruturas. Cabia à CDURP reunir a todos para encontrar soluções que atendessem aos diversos interesses e necessidades.

Este quebra-cabeças era montado e remontado em várias reuniões com os diferentes atores envolvidos, num esforço permanente de construção de soluções e consensos. Foi um processo intenso de *aprender-fazendo*. Foram inúmeras reuniões com longas discussões técnicas e também muitos encontros do prefeito e da diretoria da CDURP com os dirigentes destas empresas para sensibilizá-los e comprometê-los com o processo de mudanças em curso. Muitas vezes, essas reuniões ocorreram *na beira da vala*. Este processo implicava também na articulação com as obras viárias propriamente ditas, cujo avanço dependia do ritmo da reconstrução das infraestruturas. Isso tudo sob a pressão dos prazos contratados e, principalmente do compromisso de deixar a cidade pronta para os jogos olímpicos. Neste período pesou, sobretudo, a capacidade técnica e o comprometimento de trabalhadores e dirigentes em torno das mudanças pretendidas. O que permitiu um novo olhar sobre recursos técnicos e materiais disponíveis para construir soluções para os desafios enfrentados.

BREVE REFLEXÃO E ALGUMAS LIÇÕES

Neste processo de gestão da mudança no centro do Rio de Janeiro, percebemos que muitas adaptações poderiam ter ocorrido mesmo sem o acontecimento do Porto Maravilha. A revisão e otimização de diversas ruas e avenidas, o ordenamento de espaços públicos, as restrições aos estacionamentos como forma de inibir o uso dos automóveis, o ordenamento da circulação de caminhões pelo centro da cidade. Todas estas ações derivam de um olhar amplo e integrado da gestão da cidade.

10 O Diagnóstico do Potencial Arqueológico do Porto Maravilha e os Programas de Gestão do Patrimônio Arqueológico. Cf.: PORTO MARAVILHA. Disponível em: <http://portomaravilha.com.br/estudos_tecnicos>. Acesso em: 05 dez. 2018.

E esta é a grande lição aprendida. O conhecimento dado pelo uso das tecnologias da informação foi potencializado ao trocarmos de paradigma. Passar de uma perspectiva setorial para um olhar integrado e coordenado foi a receita do sucesso. Os mecanismos de diálogo e participação que envolveram principalmente a população da região foram parte importante. Para além de formatos genéricos, que levam a debates intermináveis e impasses, o contato direto com os atores para tratar de problemas que os afetam, conferiu objetividade e resultados concretos, sobretudo do ponto de vista do interesse público.

A concessão da área do Porto Maravilha para execução do conjunto de serviços e obras mostra-se um modelo bastante adequado, uma vez que facilitou muito a coordenação da elaboraçao de planos e projetos, e a sua implantação, tendo em conta o dia a dia da cidade.

Conforme o último Relatório de Monitoramento, de outubro de 2016, verificamos que entre novembro/2014 e setembro/2016, houve um aumento de cerca de 400 mil passageiros/dia nos transportes de massa; aumento da velocidade média dos ônibus nos 12 corredores no Centro da cidade de 11, 8%, no período de pico da manhã e aumento nas velocidades em 4 eixos de acesso ao Centro – Linha Vermelha +35%, Caju- Aterro + 38%, Aterro do Flamengo + 75%, Túnel S Barbara +80% e Av. Radial oeste + 106%.

De acordo com a CET Rio, em matéria publicada pelo Jornal O Globo em 04/08/2017, houve aumento de 8,3% em relação a 2013 – início da demolição da Perimetral – e de 10,6% em relação à 2009. Ainda de acordo com os técnicos da companhia, os dados apontam que a melhoria na fluidez no tráfego se tornou mais expressiva em 2017, com quase todas as obras entregues (O GLOBO, 2017), o que sugere que as transformações físicas estão sendo acompanhadas por mudanças culturais.

A integração e a troca de informações entre os operadores dos diferentes modais de transporte, bem como dos serviços urbanos, foram práticas inovadoras fundamentais para a gestão da mudança e um ótimo exemplo de como dotar a cidade de uma gestão urbana inteligente. Na medida em que as fases do planejamento avançavam, a percepção dos ganhos com o trabalho integrado foi ficando cada vez mais clara. O processo beneficiou bastante o COR, que estava nascendo exatamente como órgão de integração e coordenação. Um ganho fundamental verificado foi o convencimento entre os quadros técnicos em relação à priorização do transporte público em detrimento do individual como paradigma a ser adotado. Outro foi o enfrentamento e superação – ao menos parcial – da lógica concorrencial entre os diferentes operadores de transporte público. Além disso, agora, além de novas redes, há um cadastro fidedigno, que certamente facilita a operação e manutenção por parte das operadoras.

Transformar as cidades que existem em cidades sustentáveis é um desafio imenso. Depende de muita determinação. Envolve habilidade de dialogar, articular, coordenar, convencer. Implica em reconhecer a diversidade de olhares e interesses presentes no tecido social, cultural e econômico que cobrem a cidade e descobrir formas de fazer novas costuras, novos bordados. A isto, chamamos de gestão inteligente da mudança.

REFERÊNCIAS

[S.a]. Lei Complementar n. 101 de 23 de novembro de 2009. Rio de Janeiro.

ALBINO, V; BERARD, U.; DANGELICO, R. M. Smart cities: definitions, dimensions, and performance. *Journal of Urban Technology*, v. 22, n. 1, 2015.

ANTTIROIKO, A. V *et al*. *Smart Cities in the New Service Economy:* building Platforms for Smart Services. London: Ó Springer-Verlag, 2013.

ARRAES, J; SILVA, A. Porto Maravilha: permanências e mudanças. In: SHLUGER, Ephim; DANOWSKI, Miriam (Org.). *Cidades em transformação*. Disponível em: <http://portomaravilha.com.br/artigosdetalhes/cod/15>. Acesso em: 11 fev. 2016.

BECKS, U. *The risk society*. London: [S.n.], 1992.

BID. *Caminho para as Smart Cities:* da gestão tradicional para a cidade inteligente. [S.l.: s.n.], 2016.

BRASIL. Lei 5788/90, Estatuto da Cidade. Presidência da República em 10 de julho de 2001.

CARAGLIU, A. *et al*. Smart Cities in Europe. *Journal of Urban Technology*, v. 18, n. 2, p. 65-82, 2011.

CDURP. Circuito da celebração da herança africana, novembro 2012. 2016. Disponível em: <www.portomaravilha.com.br/circuito>. Acesso em: 05 abr. 2017

CDURP. Estudo de impacto de vizinhança da OUC da região do Porto do Rio de Janeiro. p. 125-126. 2010. Disponível em: <http://www.portomaravilha.com.br/conteudo/estudos/impacto-a-vizinhaca/V.%20Situacao%20Atual%20e%20Futura%203.%20Transporte%20-%20Demanda%20de%20Transporte%20e%20Trafego%20Viario.pdf>. Acesso em: 05 abr. 2017

CDURP. Relatório trimestral outubro-dezembro de 2016. 2016. Disponível em: <http://www.portomaravilha.com.br/conteudo/relatorios/2016/RelatorioTrimestral.pdf>. Acesso em: 05 abr. 2017

CVM, Instrução 400. 2003.

CVM, Instrução 401. 2003.

CVM, Instrução 472. 2008.

ELKINGTON, J. *Triple Bottom Line Revolution*: Reporting for the Third Millennium. Australian: CPA, 1999.

EMBARQ Brasil. *DOTS CIDADES:* manual de desenvolvimento urbano orientado ao transporte sustentável. Porto Alegre: EMBARQ Brasil, 2014.

HAMMER, S. *et al*. Cities and Green Growth: A Conceptual Framework, OECD Regional Development Working Papers 2011/08, OECD Publishing, 2011. Disponível em: <http://dx.doi.org/10.1787/5kg0tflmzx34-en>. Acesso em: 10 maio 2017.

HARRISON, Colin; DONNELLY, Ian Abbott. A Theory of Smart Cities. Proceedings of the 55th Annual Meeting of the ISSS, 2011.

HARVEY, D. *Cidades rebeldes:* do direito à cidade à revolução urbana. São Paulo: Martins Fontes, 2014.

HOLLANDS, R. G. Will The Real Smart City Please Stand Up? Intelligent, Progressive Or Entrepreneurial? *City*, v. 12, n. 3, p. 303-320, 2008.

HOURABI, H. *et al*. Understanding Smart Cities: An Integrative Framework. Proceedings of the Annual Hawaii International Conference on System Sciences, art. n. 6149291, p. 2289-2297, 2011.

IBM. Smarter Cities: New York 2009. Disponível em: <http://www.ibm.com/smarterplanet/us/en/smarter_cities/article/newyork2009.html>. Acesso em: 20 mar. 2017.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). Atlas do Censo Demográfico de 2010. IBGE, Rio de Janeiro, 2013. Disponível em http:<//censo2010.ibge.gov.br/apps/atlas/>. Acesso em: 05 abr. 2017.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA – IPEA. Dinâmica populacional e sistema de mobilidade nas metrópoles brasileiras. IPEA, Brasília, 2011. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/comunicado/110728_comunicadoipea102.pdf>. Acesso em: 06 abr. 2017.

IPCC. Climate Change 2014: Synthesis Report. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change, Geneva, 2014. Disponível em: <http://www.ipcc.ch/report/ar5/syr/>. Acesso em: 10 abr. 2017.

ITDP. Padrão de Qualidade TOD v2.0. 2013 Nam, T.; PARDO, T. A, Smart City as Urban Innovation: Focusing on Management, Policy, and Context Center for Technology. In Government University at Albany, State University of New York, U.S. 2011.

LEIGH, N. G.; HOELZEL, N. Z. Smart Growth's Blind Side: Sustainable Cities need Productive Urban Industrial Land. *Journal of the American Planning Association*, v. 78, n. 1, 2012.

LEMKOW, L.; TÀBARA, J. D. Environmental Sociology, Papers. *Revista de Sociologia*, n. 82, 2006.

MORI, K.; CHRISTODOULOU, A. Review of sustainability indices and indicators: Towards a new City Sustainability Index (CSI). *Environmental Impact Assessment Review*, v. 32, n. 1, p. 94-106, 2012.

NAPHADE, M. *et al*. Smarter Cities and Their Innovation Challenges. IEEE Computer Society, IBM, 2011.

PORTO MARAVILHA. Porto Maravilha. Disponível em:<http://www.portomaravilha.com.br/veiculolevesobretrilhos>. Para informações sobre o contrato de PPP, ver: <http://www.portomaravilha.com.br/documentos>. Acesso em: 05 dez. 2018.

RAMALHO, G.; GALDO, R. Um ano após Olimpíada, o que ficou de legado para o Rio. O Globo, 2017. Disponível em: <https://oglobo.globo.com/rio/um-ano-apos--olimpiada-que-ficou-de-legado-para-rio-21666449>. Acesso em: 04 ago. 2017.

RIBEIRO, L. C. Q.; RIBEIRO, M. G (Orgs.). Índice de Bem-Estar Urbano dos Municípios Brasileiros (IBEU-Municipal). Observatório das Metrópoles, IPPU, UFRJ, 2016.

ROMERO, Marta A. B. Frentes do urbano para a construção de indicadores de sustentabilidade intra urbana. In: [S.a]. *Paranoá:* cadernos de arquitetura e urbanismo da FAU-UnB. Brasília: FAU–UnB, ano 6, n. 4, nov. 2007.

SEBRAE. Desenvolvimento socioeconômico na metrópole e no interior do Rio de Janeiro. Estudo Estratégico nº 5. SEBRAE/RJ Serviço de Apoio às Micro e Pequenas Empresas do Estado do Rio do Janeiro, Rio de Janeiro, 2013.

SILVA, A. De onde vem o dinheiro do Porto Maravilha. Disponível em: <https://albertosilvacom.files.wordpress.com/2017/01/de-onde-vem-o-dinheiro-do-porto-maravilha.pdf>. Acesso em: 05 abr. 2017.

SILVA, A. Inclusão socioprodutiva, 2013. Disponível em: <https://albertosilvacom.files.wordpress.com/2017/01/o-porto-maravilha-e-inclusc3a3o-socioprodutiva-i.pdf>. Acesso em: 05 abr. 2017.

SILVA, A. Porto Maravilha, onde passado e futuro se encontram, 2015. Disponível em: <https://albertosilvacom.files.wordpress.com/2017/01/porto-maravilha-onde-o-passado-e-o-futuro-se-encontram.pdf>. Acesso em: 05 abr. 2017.

SINERGIA. Relatório de atualização do estudo de impacto de vizinhança (EIV) da operação urbana consorciada da região do Porto do Rio de Janeiro. Rio de Janeiro: Cdurp, 2013. Disponível em http: <//www.portomaravilha.com.br/conteudo/estudos/atualizacao-eiv-e-de-trafego/volume-1.pdf>. Acesso em: 05 abr. 2017.

SINERGIA. *Três anos de monitoramento das obras do Porto Maravilha:* a derrubada da Perimetral e a implantação do VLT. Rio de Janeiro: Sinergia Estudos e Projetos, 2016.

UNITED NATIONS HUMAN SETTLEMENT PROGRAMME / UN- HABITAT. State of the World's Cities: 2010. Disponível em: <http://mirror.unhabitat.org/pmss/listItemDetails.aspx?publicationID=2917>. Acesso em: 10 maio 2017.

UNITED NATIONS, Department of Economic and Social Affairs, Population Division (2014).

WEISS, M. C. *Cidades inteligentes:* proposição de um modelo avaliativo de prontidão das tecnologias da informação e comunicação aplicáveis à gestão das cidades. São Paulo: Centro Universitário FEI, 2016. Disponível em: <https://goo.gl/j2bTZH>. Acesso em: 05 ago. 2017.

World Urbanization Prospects: The 2014 Revision, Highlights (ST/ESA/SER.A/352). Disponível em https: <//esa.un.org/unpd/wup/publications/files/wup2014-highlights.pdf>. Acesso em: 10 maio 2017.

COMPUTAÇÃO EM NUVEM E CIDADES INTELIGENTES: DAS CONVICÇÕES TECNOLÓGICAS ÀS PRECAUÇÕES JURÍDICAS

CRISTIANO THERRIEN

INTRODUÇÃO À CIDADE NAS NUVENS AMPARADA EM REDES JURÍDICAS

É razoável supor que qualquer leitor humano (GUÉDON, 2014; MIT, 2015)[1] que percorra estas linhas iniciais já possua algum conhecimento prévio, em maior ou menor amplitude, sobre os temas que compõem o título deste artigo. Na segunda metade dos anos 10 do século XXI, já não é necessário admitir qualquer ignorância sobre os inúmeros temas sobre os quais somos expostos na diária superexposição à informação (LEVITIN, 2009), sobretudo por dispormos de amplos meios de pesquisa instantânea e discreta mediante algum "lapso" momentâneo. Ironicamente, caso confrontados com uma dúvida sobre do que se trata a tal "nuvem" – por exemplo, em uma entrevista de emprego ou um primeiro encontro (MCKENDRICK, 2012)[2] – como ato quase reflexo, primeiramente buscamos respostas na mesma "nuvem computacional" que chamamos de Internet.

Talvez uma busca no Google sobre "computação em nuvem" e seus mais 900 mil resultados,[3] ou ainda sobre o termo *cloud computing* e mais

1 A leitura "não-humana" de artigos científicos e jurídicos publicados on-line torna-se cada vez mais relevante e estratégica para empresas de alta tecnologia: "For example, people involved in the Google Books project have argued that making books available for human reading… is a minor and secondary objective of mass digitization".

2 Em uma pesquisa sobre o conhecimento de estadunidenses sobre computação em nuvem, 14% dos entrevistados fingiram saber o que é e como funciona "a nuvem" durante uma entrevista de emprego, além de 17% que fizeram o mesmo em um primeiro encontro.

3 Pesquisa textual sobre "computação em nuvem" no buscador Google: <https://goo.gl/wDVHL0>.

de 50 milhões de *links*,[4] exiba demasiadas informações que faria qualquer pessoa duvidar dos seus conhecimentos sobre este assunto de natureza "nebulosa". Esta significativa complexidade técnica e a elevada diversidade de dados sobre o tema, a princípio, pode se mostrar desafiadora para qualquer profissional do Direito – mesmo quando usuário assíduo de serviços e aplicativos baseados na nuvem – que se encontre diante das muitas dúvidas derivadas das problemáticas jurídicas quando da adoção deste modelo tecnológico por instituições públicas ou privadas.

Apesar da computação em nuvem não possuir regulação relevante no país, figurar de forma escassa na doutrina jurídica brasileira e seguir praticamente inexistente na jurisprudência nacional, não cabe a qualquer jurista se abster devido a dificuldades frente a temas inovadores. Os aspectos jurídicos do *cloud computing*, que seguem insuficientemente enquadrados por um Direito pautado pela pirâmide kelseniana, encontram-se adequadamente compreendidos por um Direito baseado no paradigma da rede. A flexibilidade de um "Direito em rede" (OST; VAN DE KERCHOVE, 2002), permite perceber o Direito pela sua interconectividade com outros campos do conhecimento – por exemplo, tecnologia da informação –, sua composição proteiforme de normatividades estatais e não-estatais – como padrões ISO relativos a *cloud computing* –, bem como seu entrelaçamento multi-hierárquico de sentidos e distribuído de ancoragens (BAILLEUX, 2005) que o mantém entre a ordem e a desordem da sociedade pós-moderna.

Entre os vários sentidos que assume, de acordo com o ponto da rede de onde se parte, o Direito é uma racionalidade prática de adaptação, normalização e imaginação que busca compor conhecimentos pragmáticos onde, quando e como se fizerem necessários. Neste diapasão, os acúmulos internacionais devem ser aproveitados pelo Direito ao nos debruçarmos sobre o modelo tecnológico do *cloud computing,* visto que é parte fundamental dos instrumentos de globalização (HODSON, 2008) que afetam e mobilizam ordens jurídicas nacionais em todo o mundo (BENYEKHLEF, 2016), e que as experiências e soluções não devem ser desperdiçadas, mas compartilhadas. Para tanto, este texto analisará funções que as nuvens computacionais vêm desempenhando para tornar as cidades mais "inteligentes", observará semelhanças e distinções de seus modelos de aplicação em governos municipais, visando assim avaliar seus reflexos no Direito.

4 Pesquisa textual sobre "cloud computing" no buscador Google: <https://goo.gl/SIYbzf>.

DOS POSSÍVEIS CONCEITOS DE CIDADE INTELIGENTE E COMPUTAÇÃO EM NUVEM

No mesmo compasso globalizante e tecnológico em que as grandes cidades de referência local tornaram-se cidades globais (SASSEN, 2013) interconectadas em uma sociedade em rede (CASTELLS, 2000), há mais de 25 anos que testemunhamos a aplicação do termo "cidade inteligente" ou *smart city* passar de algumas experiências localizadas – como Barcelona, Londres, Nova York, Singapura etc. – para uma massificação de projetos em centenas[5] de cidades por todo o mundo. A popularização do termo *smart city* impede uma única definição hegemônica sobre que se trata uma cidade inteligente, ainda que muitos esforços acadêmicos (ALBINO; BERARDI; DANGELICO, 2015) sejam feitos para mapear seus sentidos em comum. Uma das hipóteses informais aceitas no meio é que existem tantas definições de *smart city* quanto cidades envolvidas, empresas contratadas e pesquisadores atuantes neste tema.

Poderíamos usar muitas outras expressões para cidades inteligentes como: cidades digitais, cidades conectadas, cidades ciborgues, cidades virtuais, cidades da informação, cidades em rede, cidades responsivas, cidades do futuro, entre muitas outras nomenclaturas[6] que não formam perfeitos sinônimos. Optamos aqui pelo termo cidade inteligente como melhor correspondente à nomenclatura genérica e internacionalizada de *smart cities*, cujo uso se relaciona mais estreitamente a dados e teorias que trazem mais imediatismo (BATTY, 2013) ao nosso interesse de entender as problemáticas jurídicas geradas pelas Tecnologias da Informação (TI) quando aplicadas na gestão e planejamento urbanos.

Se por um lado deixamos intencionalmente em aberto uma definição de *smart city* e logo no início do texto sugerimos uma busca na Internet por um conceito de *cloud computing*, parece-nos fundamental apresentar uma definição de computação em nuvem, visto que este é o principal ponto de referência para as interpretações possíveis de cidade inteligente para este texto, bem como o foco jurídico pretendido. Neste sentido, ainda que também encontremos uma grande variedade de definições de *cloud computing*, a literatura técnica e jurídica estrangeira frequentemente se

5 Ou milhares de projetos, de acordo com a definição ou ranking utilizados como parâmetros.

6 A título de exemplo, diversas expressões no mesmo sentido são usadas em mais de uma centena de palestras TED. YOUTUBE. Smart, future, sustainable cities - TED Talks. Disponível em: <https://www.youtube.com/playlist?list=PLKmOxeqpQCzp-dR7pUoL__eb_06_jSipW1>. Acesso em: 30 abr. 2017.

utiliza da definição do National Institute of Standards and Technology[7] (NIST), órgão ligado ao Departamento de comércio do governo dos EUA:

> Computação em nuvem é um modelo para permitir acesso ubíquo, conveniente, sob demanda e conectado a um conjunto compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente fornecidos e liberados com o mínimo esforço de gerenciamento ou interação do provedor de serviços (GRANCE; MELL, 2011, p. 2, tradução nossa).[8]

Uma das razões da computação em nuvem dispor de uma definição mais pacífica – ou menos polêmica – do que cidade inteligente se dá pelo fato de não se tratar necessariamente de uma novidade, pois suas primeiras atribuições (NEWMAN, 2014) remontam à década de 1960. Em si, a computação em nuvem não é necessariamente revolucionária, mas um acúmulo de tecnologias pré-existentes que apenas recentemente se tornaram economicamente viáveis, tecnicamente realizáveis (GASSER, 2014) e amplamente difundidas na sociedade. Passado o período inicial em que gerou grandes expectativas – o alto da curva de *hype* tecnológico – (KOMNINOS; SCHAFFERS; PALLOT, 2011), a computação em nuvem já não causa qualquer febre profissional ou acadêmica – como inteligência artificial, robôs, *drones* –, pois esta já se consolidou (MCKENDRICK, 2015) como uma mudança de paradigma tecnológico, pela capacidade disruptiva (SATELL, 2014) demonstrada de inovar os processos (*downstream innovation*) das instituições.

De todas as inovações provocadas pelo que alguns autores chamam de revolução industrial (ELLIOT, 2016) gerada pela convergência de TI, o *cloud computing* é aquela que pode ser considerada tão disruptiva para a sociedade quanto foi a própria computação em si, pois hoje é a principal base de geração para novas inovações tecnológicas. A computação em nuvem se revela como a pedra fundamental sobre a qual a maioria das atividades da Internet se baseiam e pela qual passam a ser caracterizadas (TRUDEL, 2014). Por vezes também chamada de "computação infinita" (BASS, 2012), por suas características de alta disponibilidade e fácil acesso a um poder computacional praticamente ilimitado – armazenamento,

7 Instituto nacional de padrões e tecnologia. (tradução nossa)

8 No original: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models".

processamento, etc. – a qualquer indivíduo ou coletivo com conexão à Internet, a computação em nuvem se apresenta hoje como o modelo tecnológico que melhor permite o desenvolvimento e aplicação de inovações relacionadas a cidades inteligentes.

DOS MODELOS DE COMPUTAÇÃO EM NUVEM PARA CIDADES INTELIGENTES

Há várias maneiras de descrever os modelos de serviço de *cloud computing*, mas há suficiente concordância sobre três modelos: infraestrutura como serviço – Infrastructure as a Service (IaaS) –, plataforma como serviço – Platform as a Service (PaaS) – e *software* como serviço – Software as a Service (SaaS) (MANZOUR, 2015). Os três modelos de serviço podem e são utilizados de formas distintas e potencialmente complementares em projetos de *smart city*, com problemáticas jurídicas diferentes que serão tratadas mais à frente.

O modelo de serviço SaaS provê acesso remoto a sistemas que ficam hospedados e mantidos pela provedora da nuvem, a qual também irá gerenciar o *software* básico e o *hardware* necessário. Neste modelo, prefeituras podem acessar aplicações padrão do tipo *office* – Google Docs, por exemplo – como sistemas de gestão municipal mais genéricos, o que pode ser muito útil para cidades de menor porte com dificuldades de investimento em TI.

O modelo PaaS permite o usuário instale e opere e mantenha seus próprios sistemas hospedados na nuvem, os quais se utilizarão do *software* básico – sistema operacional e outros programas necessários para o funcionamento do equipamento e de sistemas aplicativos – e o equipamento remoto necessários para funcionar. Pode ser muito adequado a sistemas municipais que exijam um nível maior de customização e até mesmo projetos-piloto de cidades inteligentes que não disponham de muitos recursos iniciais.

O modelo IaaS disponibiliza basicamente uma infraestrutura de equipamentos a serem usados à distância – processador, memória, armazenamento, rede etc. – para que o usuário implante plataformas e sistemas por conta própria. Prefeituras podem se valer dessas estruturas para substituir parte de sua demanda de datacenter próprio e seguro, por exemplo, evitando assim o dispendioso modelo de sala-cofre.

Ainda há que se considerar os modelos de implantação de *cloud computing*, cujos ambientes podem estar em nuvem pública, privada, comunitária ou híbrida. Há importantes diferenças entre os modelos que envolvem tratamentos jurídicos muito distintos entre si e que devem ser analisados em combinação ao modelo de serviço já apresentado.

O ambiente de nuvem mais conhecido e que mais cresce em adesão é o modelo público – que não significa governamental ou gratuito –, em que o serviço é prestado para um público geral, que irá compartilhar os recursos – servidores, armazenamento – em comum. Este modelo é voltado à economia de escala e visa um máximo de ganhos de eficiência, contudo costuma ser acompanhado de um menor grau de controle e supervisão de segurança por parte do usuário. Há vários exemplos de governos (ZWATTENDORFER; TAUBER, 2013), assim como de grandes bancos (NORTON, 2016), que começam a incorporar esse apelativo modelo, contudo persiste a forte e justificada resistência interna a esta adesão.

O ambiente de nuvem privada se distingue da nuvem pública por ser provido exclusivamente para um só usuário – não compartilha recursos com terceiros – e apresenta várias configurações que, a priori, podemos resumir a duas: na primeira, o usuário terceiriza os equipamentos e o gerenciamento para o provedor da nuvem; na segunda, o provedor da nuvem apenas hospeda os equipamentos do usuário que irá operá-los e gerenciá-los à distância. Esta modalidade pode trazer a vantagem de maior controle e segurança – quando acompanhado de significativos investimentos de pessoal especializado –, mas perde em eficiência e economia. Prefeituras podem optar pela nuvem privada para hospedar aplicações de maior risco técnico e jurídico, como aquelas que envolvam bancos de dados sensíveis de cidadãos e exijam maior segurança.

O modelo de nuvem comunitária reúne organizações com semelhantes características e interesses, que irão compartilhar a mesma nuvem e colaborar para o seu desenvolvimento. Por exemplo, prefeituras podem colaborar através de consórcios para contratar uma nuvem comunitária em comum, ou ainda combinar esforços com governos estaduais para o compartilhamento de recursos de nuvem em formato IaaS, PaaS ou SaaS. Há muito espaço para elaboração técnica e esforço político e jurídico na formação de nuvens comunitárias.

Por fim, o modelo de implantação de nuvem híbrida, como o nome sugere, trata de uma combinação de ambientes em que irá compor atividades hospedadas em diferentes nuvens: pública, privada e/ou comunitária. No ambiente público, por exemplo, podem ficar serviços não-críticos – hospedagem do site de Internet e sistema de e-mail – e no ambiente privado irão operar os serviços críticos e com dados mais sensíveis. Este modelo combina as vantagens e desvantagens dos modelos, o que permite benefícios, mas também incrementa riscos técnicos e jurídicos pela maior complexidade da sua operação e manutenção (BLACK, 2012; YAMAMOTO; MATSUMOTO; NAKAMURA, 2012; NOWICKA, 2014; CLOHESSY; ACTON; MORGAN, 2014; SUCIU *et al.*, 2013; MITTON *et al.*, 2012; LEA; BLACKSTOCK, 2014).

DAS VANTAGENS E DESVANTAGENS DA COMPUTAÇÃO MUNICIPAL EM NUVEM

Apesar dos reconhecidos benefícios da computação em nuvem que se populariza cada vez mais na vida cotidiana de indivíduos e instituições usuários de seus serviços, o *cloud computing* compreensivamente ainda encontra uma grande resistência dos governos por seus riscos inerentes. Dada a importância da consciência das vantagens e desvantagens (CHEN, 2015), bônus e ônus que o jurista buscará equilibrar quando afrontado pelos desafios jurídicos da nuvem, cabe aqui uma breve descrição destes elementos.

Entre os principais benefícios da computação em nuvem para cidades inteligentes (CHEN, 2015), encontram-se: redução de custos de investimento e manutenção de recursos de infraestrutura, plataformas e/ou sistemas de TI; agilidade e simplicidade para responder mais rapidamente a necessidades presentes ou futuras; elasticidade e escalabilidade, que permitem aumentar ou diminuir a alocação de recursos de forma flexível e ajustável à demandas novas ou pontuais; disponibilidade e confiabilidade pelos níveis de segurança e redundância mais sofisticados; possibilidade de colaboração remota e acessibilidade global por meio da Internet que permite o trabalho conjunto por equipes fisicamente separadas; facilidade de migração para novas tecnologias, que permite atualizações sem necessidade de interrupção de serviços; maior sustentabilidade pela economia de consumo de energia e equipamentos; compartilhamento de recursos que podem ser dinamicamente distribuídos entre diferentes órgãos governamentais; serviços mensuráveis que permitam o acompanhamento das atividades e o monitoramento do seu desempenho em tempo real.

Em contrapartida, é fundamental apontar os desafios a serem enfrentados pelos gestores municipais, suas equipes técnicas e, neste caso enfatizados, suas assessorias jurídicas que estiverem incumbidas de reduzir os riscos – nunca erradicáveis – da computação em nuvem: a segurança da informação que sempre exigirá significativos esforços ampliados e planejados devido à sua centralidade; a proteção dos dados pessoais dos cidadãos que será central para o sucesso ou fracasso da migração às nuvens; o equacionamento de custos econômicos que tendem a crescer e possivelmente reverter as vantagens iniciais dos projetos; a interoperabilidade e a portabilidade dos dados que evitem uma possível situação de "refém contratual" frente a um provedor privado de serviços de nuvem; razoável adequação contratual de cláusulas Service Level Agreement (SLA) que atendam às premissas de qualidade, disponibilidade e performance que

respondam às inevitáveis urgências; a gestão de identidade e acesso que exigirá mais do que segurança, mas uma devida governança interna que muitas vezes muda os procedimentos costumeiros dos órgãos públicos; a transparência que permita realizar auditorias dos serviços, por equipe própria e terceiros que possam certificar as práticas em curso; e, em especial, as questões de jurisdição que sempre devem estar claras, sobretudo na contratação de provedoras de porte internacional.

Por fim, entre outros pontos fortes e frágeis da computação em nuvem para cidades inteligentes, há que se destacar que ambos benefícios e riscos são de delicado tratamento jurídico tanto nos procedimentos licitatórios para a contratação de serviços, quanto na gestão dos contratos de implantação, migração e manutenção. O cumprimento de boas práticas de compras governamentais na área de tecnologia é mundialmente reconhecido como um desafio institucional e jurídico de alta complexidade, bem como a dificuldade de encontrar os custos ocultos dos contratos e mantê-los sob controle frente a pressões de orçamentos limitados. Frente à pressão de avançar e mudar, há semelhante força para pesar e prevenir.

DAS CONVICÇÕES TECNOLÓGICAS ÀS PREOCUPAÇÕES JURÍDICAS

As projeções de cidades inteligentes futurísticas que figuravam como mera ficção científica no passado recente, passaram às atuais convicções de que já existem a maioria das tecnologias digitais necessárias para realizar estas cidades no presente (MARTIN, 2014). Esta potencial viabilidade se dá, em grande medida, por meio da computação em nuvem. A nuvem governamental tem se demonstrado cada vez mais onipresente, acessível e incontornável, fornecendo maior poder de processamento e armazenamento do que qualquer tipo de sistema de gestão municipal necessite no presente ou no futuro imaginados.

A princípio, qualquer prefeitura com razoável acesso à Internet já pode dispor da infraestrutura computacional mais avançada do mundo sem necessariamente ter que pagar por todos os altos custos de equipamentos e pessoal de TI, elementos que compõem gastos sempre crescentes em qualquer governo. Trata-se de uma oportunidade de inovação tecnológica singular em um setor conhecido pela inércia burocrática (MCKENDRICK, 2014), onde a adoção da nuvem pode melhorar a flexibilidade dos serviços públicos, apesar de seus idiossincráticos sistemas *back-end* fechados em silos (PEREPA, 2013). Entre um dos exemplos dessas práticas isolacionistas que o *cloud computing* permite modificar, encontram-se os reinci-

dentes procedimentos de determinados órgãos que exigem que o cidadão entregue documentos com dados que já são de posse de outros órgãos do mesmo governo.

Em todo o mundo, percebe-se que há pressão para que os governos superem as práticas arraigadas em uma cultura corporativa de "*bunkers* de TI" e "contêineres de dados isolados", e assim passem a prestar melhores serviços integrados. Contudo, a progressiva adoção governamental de computação em nuvem – que não se dá somente por razões logísticas e financeiras – envolve justificados receios que seus bancos de dados passarão a um ambiente onde os dados pessoais de seus cidadãos tornam-se mais acessíveis e sensíveis.

A crescente disponibilidade de acesso a dados públicos na nuvem informativa indica o avanço a uma era pós-transparência, onde a criatividade para propor e construir novas soluções tornou-se tão fértil quanto a capacidade de gerar e perceber novos perigos. Entre estes riscos amplamente apontados na produção acadêmica e midiática, figuram novos patamares de violação da privacidade, manipulação de informações, monitoramento ostensivo de cidadãos e movimentos sociais. Contudo, em contraste, merece atenção o notável fervor das secretarias municipais que frequentemente alegam proteção à privacidade dos cidadãos quando demandados a fornecer acesso à documentos públicos (TRUDEL, 2014). Outra classe de riscos, frequentemente ignorados, estão relacionados à exclusão digital de camadas da população (LERMAN, 2013) que não serão incluídas no planejamento e execução de projetos de cidades inteligentes.

Instituições públicas reticentes enfrentam a dupla pressão de aderir a serviços baseados em nuvem e de manter os dados públicos a salvo de violações de confidencialidade, integridade e disponibilidade, falta de controle da transmissão ou processamento de dados, impossibilidade de monitoramento (O. M.; V. F., 2014) e auditoria adequada, entre outros riscos potenciais. Frente a estes e outros riscos que não devem ter suas responsabilidades atribuídas apenas aos departamentos de TI, cabe um "compartilhamento em rede" do princípio de razoabilidade que o direito administrativo deve zelar nas especificidades da "nuvem municipal".

CONCLUSÃO E RECOMENDAÇÕES A QUEM TATEIA NAS BRUMAS COMPUTACIONAIS

O risco figura como elemento central da sociedade contemporânea (BECK, 1992), bem como encontra-se no coração dos fundamentos e das condições de efetividade do Direito (TRUDEL, 2013). Conforme

visto anteriormente, vários riscos estão envolvidos em todas as etapas de projetos de cidade inteligente baseados em nuvens computacionais. Os gerenciamentos técnico e jurídico destes riscos devem ser tratados atentiva e permanentemente para que o eixo custos/benefícios sopese para o lado desejado por gestores municipais, profissionais de TI e suas assessorias jurídicas.

Neste sentido, como uma modesta contribuição final do presente trabalho que visou compor literatura técnica e jurídica estrangeira sobre a computação em nuvem em cidades inteligentes, seguem algumas recomendações-chave para o seu gerenciamento de risco:

- definição de políticas municipais de proteção de dados, as quais não devem se restringir a leis federais sobre o tema, mas que podem se beneficiar dos intensos debates de projetos brasileiros no Congresso Nacional e da legislação europeia;
- cumprimento de melhores práticas de segurança (atenção especial às normas ISO 27017 e 27018) que estão sempre a avançar, visando assim superar as predominantes políticas municipais de segurança baseadas em obscuridade;
- promoção de confiança – que é diferente de segurança – dos usuários-cidadãos no uso da nuvem através de práticas de inteligibilidade que priorizem:
- transparência pública quanto às práticas de segurança da informação nos serviços municipais baseados em nuvens computacionais, pois só se confia no que se conhece;
- ampla acessibilidade (em sentido largo) aos serviços nas nuvens para que não restrinja a pequenas camadas da população, pois só se conhece aquilo que se tem acesso;
- utilidade flexível de serviços a indivíduos, setores e grande público, pois só se acessa aquilo que seja útil para si;
- participação popular no aprimoramento e ampliação dos serviços na nuvem, pois o custoso projeto de cidade inteligente só terá utilidade se tiver participação e repercussão ampla para que se tenha razão de prosseguir.

Ainda merece nota que se recomenda cautela técnica e jurídica – e sobretudo política – quanto à recente norma ISO 37120, considerada a "norma técnica para cidades inteligentes", haja vista a uma frequente tendência de adesão acrítica a estas normatividades plurais cada vez mais presentes em um Direito cada vez mais em rede e global. Em particular, esta norma

é significativamente pautada em paradigmas europeus e norte-americanos, portanto suas referências devem buscar uma composição com às experiências técnicas, relações jurídicas e percepções locais.

Por fim, todas as descrições, análises e proposições aqui expostas devem ser vistas com crítica, razoabilidade e adaptabilidade para que contribuam um pouco ao debate brasileiro.

REFERÊNCIAS

ALBINO, Vito; BERARDI, Umberto; DANGELICO, Rosa Maria. Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*, v. 22, n. 1, p. 3-21, 2015.

BAILLEUX, Antoine. A la recherche des formes du droit : De la pyramide au réseau ! *Revue interdisciplinaire d'études juridiques*, v. 2005, n. 55, p. 91-115, 2005.

BASS, Carl. We've reached infinity – so start creating. Wired, 22 fev.February 2012. Disponível em: <http://www.wired.co.uk/magazine/archive/2012/03/ideas-bank/weve-reached-infinity>. Acesso em: 13 maio 2017.

BATTY, Michael. Big data, smart cities and city planning. *Dialogues in Human Geography*, v. 3, p. 274, 2013.

BECK, Ulrich. *Risk Society, Towards a New Modernity*. London: Sage Publications, 1992.

BENYEKHLEF, Karim. *Vers un droit global*. Montreal: Thémis, 2016.

BLACK, Nicole. *Cloud Computing for Lawyers*. [S.l.]: Aba Book Publishing, 2012.

CASTELLS, Manuel. *The Rise of the Network Society*. Cambridge: Blackwell Publishers, 2000.

CHEN, Chin Kang; ALMUNAWAR, Mohammad Nabil. Cost Benefits of Cloud Computing for Connected Government. In: MAHMOOD, Zaigham. *Cloud Computing Technologies for Connected Government*. Hershey: IGI Global, 2015., p. 345-368.

CLOHESSY, Trevor; ACTON, Thomas; MORGAN, Lorraine. "Smart City as a Service (SCaaS) – A Future Roadmap for E-Government Smart City Cloud Computing Initiatives"., *IEEE/ACM 7th International Conference on Utility and Cloud Computing*, 2014.

COHEN, Reuven. Interest in Cloud Computing Has Peaked. Forbes, 2012. Disponível em: <https://www.forbes.com/sites/reuvencohen/2012/05/24/interest-in-cloud-computing-has-peaked/>. Acesso em: 13 maio 2017.

ELLIOT, Larry. Fourth Industrial Revolution brings promise and peril for humanity. The Guardian, 24th jan. January 2016. Disponível em: <https://www.theguardian.com/business/economics-blog/2016/jan/24/4th-industrial-revolution-brings-promise-and-peril-for-humanity-technology-davos>. Acesso em: 13 maio 2017.

GASSER, Urs. Cloud Innovation and the Law: Issues, Approaches, and Interplay. *Berkman Center Research Publication*., n. 2014-7. Disponível em: <https://ssrn.com/abstract=2410271>. Acesso em: 13 maio 2017.

GRANCE, Timothy; MELL, Peter. *The NIST Definition of Cloud Computing*: Recommendations of the National Institute of Standards and Technology. Gaithersburg: U.S. Department of Commerce, 2011.

GUÉDON, Jean-Claude. Sustaining the "Great Conversation": the future of scholarly and scientific journals. In: COPE, B.; PHILLIPS, A. (Orgs.). *The Future of the Academic Journal*. 2. ed. [S.l.]: Chandos Publishing, 2014, p. 106.

HODSON, Matthew. Computers without Borders: the Cloud May Be the Ultimate Form of Globalisation. The Economist, 2008. Disponível: <http://www.economist.com/node/12411854>. Acesso em: 30 abr. 2017.

KOMNINOS, Nicos; SCHAFFERS, Hans; PALLOT, Marc. Developing a Policy Roadmap for Smart Cities and the Future Internet Reuven Cohen. In: CUNNINGHAM, Paul; CUNNINGHAM, Miriam (Eds.). eChallenges e-2011 Conference Proceedings., *Paul Cunningham and Miriam Cunningham (Eds), IIMC International Information Management Corporation*, 2011.

LEA, Rodger; BLACKSTOCK, Michael. "City Hub: A Cloud-Based IoT Platform for Smart Cities"., *IEEE 6th International Conference on Cloud Computing Technology and Science*, Singapore, 2014, p. 799-804.

LERMAN, Jonas. Big Data and Its Exclusions. *Stanford Law Review*, v. 66, p. 55-63, 2013.

LEVITIN, Daniel J. The Organized Mind: Thinking Straight in the Age of Information Overload. [S.l.]: Dutton, 2014; HEMP, Paul. Death by Information Overload. *Harvard Business Review*, 2009. Disponível em: <https://hbr.org/2009/09/death-by-information-overload>. Acesso em: 30 abr. 2017.

MANZOUR, Amir. Cloud Computing Applications in the Public Sector. In: MAHMOOD, Zaigham (Org.). *Cloud Computing Technologies for Connected Government*. Hershey: IGI Global, 2015., p. 219.

MARTIN, Glen. Most Of What We Need For Smart Cities Already Exists. Forbes, 1 st Mmaioay 2014. Disponível em: <http://www.forbes.com/sites/oreillymedia/2014/05/01/most-of-what-we-need-for-smart-cities-already-exists/>. Acesso em: 13 maio 2017.

MCKENDRICK, Joe. Cloud Computing's Let's-Roll-Up-Our-Sleeves-And-Make-This-Stuff-Work Moment. Forbes, 15 dezembro December 2015. Disponível em: <https://www.forbes.com/sites/joemckendrick/2015/12/17/cloud-computings-lets-roll-up-our-sleeves-and-make-this-stuff-work-moment/#424608fa3f1d >. Acesso em: 13 maio 2017.

MCKENDRICK, Joe. Government as a Platform: How Cloud Computing Is Progressing Inside the Beltway. Forbes, 23 fFev.bruary 2014. Disponível em: <http://www.

forbes.com/sites/joemckendrick/2014/02/23/government-as-a-platform-how-cloud-computing-is-progressing-inside-the-beltway/>. Acesso em: 13 maio 2017.

MCKENDRICK, Joe. Most Americans Don't Understand Cloud Computing: Does It Really Matter? Forbes, 2012. Disponível em: <https://www.forbes.com/sites/joemckendrick/2012/08/29/most-americans-dont-understand-cloud-computing-does-it-really-matter/#11fe1e524ef7>. Acesso em: 30 abr. 2017.

MIT TECHNOLOGY REVIEW. Google DeepMind Teaches Artificial Intelligence Machines to Read, 2015. Disponível em: <https://www.technologyreview.com/s/538616/google-deepmind-teaches-artificial-intelligence-machines-to-read/>. Acesso em: 30 abr. 2017.

MITTON *et al*. Combining Cloud and Sensors in A Smart City Environment, *EURASIP Journal on Wireless Communications and Networking*, p. 247, 2012.

NEWMAN, Daniel. Cloud: Not New, Just A Big Disruption To How We Communicate. Forbes, 2014. Disponível em: <http://www.forbes.com/sites/danielnewman/2014/06/10/cloud-not-new-just-a-big-disruption-to-how-we-communicate/>. Acesso em: 13 maio 2017.

NORTON, Steven. Big Banks Starting to Embrace Public Cloud, Deutsche Bank Says. The Wall Street Journal. Disponível em: <https://blogs.wsj.com/cio/2016/06/09/big-banks-starting-to-embrace-public-cloud-deutsche-bank-says/>. Acesso em: 13 maio 2017.

NOWICKA, Katarzyna. Smart City Logistics on Cloud Computing Model. *Procedia – Social and Behavioral Sciences*, v. 151, p. 266 -281, 2014.

O. M., Fal; V. F., Kozak. Personal Data Protection Problems Associated with Cloud Computing. *Cybernetics and Systems Analysis*, v. 5, p. 768, 2014.

OST, François; VAN DE KERCHOVE, Michel. *De la pyramide au réseau?* Pour une théorie dialectique du droit. Bruxelas: Publications des Facultés Universitaires Saint-Louis, 2002.

PEREPA, Sujatha. "Why the U.S. Government is Moving to Cloud Computing". WIRED. Disponível em: <http://www.wired.com/2013/09/why-the-u-s-government-is-moving-to-cloud-computing/>. Acesso em: 13 maio 2017.

SASSEN, Saskia. *The Global City*. New York: Princeton University Press, 2013.

SATELL, Greg. "Why the Cloud Just Might Be the Most Disruptive Technology Ever". Forbes, 5th jJan. uary 2014. Disponível em: <http://www.forbes.com/sites/gregsatell/2014/01/05/why-the-cloud-just-might-be-the-most-disruptive-technology-ever/>. Acesso em: 13 maio 2017.

SUCIU, George et al. Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things, *19th International Conference on Control Systems and Computer Science*, 2013.

THE ECONOMIST Intelligence Unit. The Impact of the Cloud. Disponível em: <http://www.economistinsights.com/sites/default/files/The%20impact%20of%20cloud.pdf>. Acesso em: 13 maio 2017.

TRUDEL, Pierre. Gouvernement intelligent: quelques conditions, *Le Journal de Montréal*, 6 th nNov.ember 2014. Disponível em: <http://blogues.journaldemontreal.com/pierretrudel/droit/gouvernement-intelligent-quelques-conditions/>. Acesso em: 13 maio 2017.

TRUDEL, Pierre. L'infonuagique et la loi québécoise, *Le Journal de Montréal,* 16th abr. April 2014. Disponível em: <http://blogues.journaldemontreal.com/pierretrudel/droit/linfonuagique-et-la-loi-quebecoise/>. Acesso em 13 maio 2017.

TRUDEL, Pierre. Le risque, fondement et facteur d'effectivité du droit. In: BENYEKHLEF, Karim. *Gouvernance et risque* : – Les défis de la régulation dans un monde global. Montréal: Éditions Thémis, 2013.

YAMAMOTO, Shintaro; MATSUMOTO, Shinsuke; NAKAMURA, Masahide. Using Cloud Technologies for Large-Scale House Data in Smart City, *IEEE 4th International Conference on Cloud Computing Technology and Science*, 2012.

YOUTUBE. Smart, future, sustainable cities - TED Talks. Disponível em: <https://www.youtube.com/playlist?list=PLKmOxeqpQCzpdR7pUoL__eb_06_jSipW1>. Acesso em: 30 abr. 2017.

ZWATTENDORFER, Bernd; TAUBER, Arne. The Public Cloud for e-Government. *International Journal of Distributed Systems and Technologies*, v. 4, n. Issue 4, October 2013, p. 1-14, out. 2013..

O DIREITO À CIDADE (INTELIGENTE): TECNOLOGIAS, REGULAÇÃO E A NOVA AGENDA URBANA[1]

JHESSICA REIA

INTRODUÇÃO: O LUGAR DA CIDADE

Observar e estudar a cidade em suas mais variadas formas e perspectivas tem se tornado prática recorrente. Diante de taxas de urbanização crescentes e do papel central que as cidades vêm assumindo em diversas áreas do conhecimento, torna-se essencial pensar os centros urbanos a partir de abordagens variadas, que tenham um entendimento da cidade que vai além de suas estruturas físicas. Com o avanço de novas tecnologias da informação e da comunicação, somado à presença marcante dos meios de comunicação de massa, outras formas de gerir e viver a cidade acabam surgindo. A construção da cidade é um processo contínuo, fluido e conflituoso que atrai o interesse de cada vez mais pesquisadores.

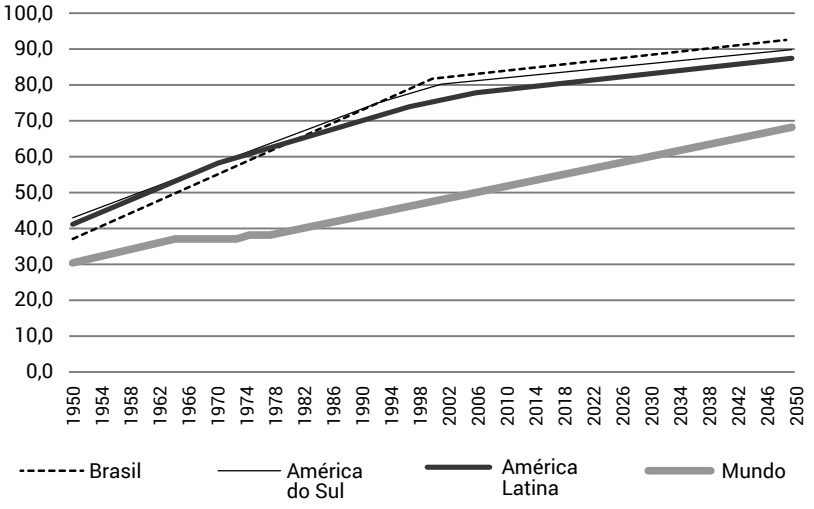
É comum ouvir que a população mundial tem se tornado progressivamente urbana. Segundo o relatório *World Urbanization Prospects: The 2018 Revision,*[2] publicado pela *Population Division of the Department of Economic and Social Affairs*, da Organização das Nações Unidas (ONU), 55% da população vive em áreas urbanas em 2018 – sendo que nos anos 1950 essa taxa era de 30% e provavelmente atingirá 68% da população mundial até 2050, segundo as projeções da ONU. Hoje, na América Latina e no Caribe, 81% das pessoas vivem em regiões urbanizadas (UNITED NATIONS, 2018).

1 Parte da discussão aqui apresentada vem de reflexões feitas ao longo dos últimos anos, da participação em eventos acadêmicos e da co-coordenação do projeto *Discrimination vs. Data Control in Brazilian Smart Cities*, financiado pela Open Society Foundations (OSF).

2 Ver: UNITED NATIONS. World Urbanization Prospects: The 2018 Revision, Online Edition, 2018. Disponível em: <https://esa.un.org/unpd/wup/Publications/Files/WUP2018-KeyFacts.pdf>. Acesso em: 10 jul. 2018.

Conforme pode ser visto na Figura 1 abaixo, a proporção da população urbana no Brasil vem aumentando de forma rápida, passando de 36,2% em 1950 para 86,6% em 2018 – e com uma projeção de 92,4% da população brasileira vivendo em regiões urbanas até 2050. Ao se comparar com a sub-região – América do Sul – e região – América Latina –, vê-se que o Brasil apresenta taxas de urbanização mais elevadas e tem uma projeção que tende a ultrapassar as taxas sub-regionais e regionais, sendo também consideravelmente maiores que o total global.

Figura 1 – Proporção da população urbana no Brasil em comparação à sub-região, região e total global, percentual (1950-2050)



Fonte: UNITED NATIONS, DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, POPULATION DIVISION. World Urbanization Prospects: The 2018 Revision, Online Edition, 2018. Tradução e adaptação minha.

No Brasil, a tendência de migrações cidade-campo e do crescimento urbano se acentuam a partir, principalmente, do século XX. De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), o Brasil possuía 5.570 municípios em 2013, e a taxa de urbanização saltou de 31,24% em 1940 para 84,36% em 2010, conforme pode ser visto no quadro 1. Atualmente, o país tem uma das maiores cidades do mundo: São Paulo, cuja região metropolitana tem em torno de 22 milhões de habitantes – sendo superada apenas por Tóquio – 37 milhões –, Nova Deli – 29 milhões – e Shanghai – 26 milhões –, em termos de aglomeração urbana e empatando com a Cidade do México em proporção populacional vivendo em áreas

urbanas (UNITED NATIONS, 2018). Ao mesmo tempo, é preciso ter em mente que quase metade da população mundial urbana vive em cidades com menos de 500.000 habitantes, enquanto uma em cada oito pessoas habita uma das 33 megacidades globais – que possuem mais de 10 milhões de habitantes –, de acordo com o relatório da ONU.

Quadro 1 – Evolução da taxa de urbanização no Brasil, percentual, 1940-2010

1940	1950	1960	1970	1980	1991	2000	2007	2010
31,24	36,16	44,67	55,92	67,59	75,59	81,23	83,48	84,36

Fonte: IBGE, Censo demográfico 1940-2010.

Diante desse cenário, vale também refletir para além dos números. Uma abordagem multidisciplinar das cidades é necessária para entender as muitas dinâmicas de poder que operam em diversos âmbitos urbanos. O peso crescente das iniciativas de desenvolvimento urbano sustentável se alia à complexificação das disputas pelos espaços públicos e os direitos de se viver e ocupar as cidades, que tem também se intensificado a partir da difusão de novas – e consolidadas – tecnologias, entranhadas nas cidades. Como será brevemente discutido ao longo deste trabalho, analisar os muitos papéis das tecnologias na cidade, a partir de sua materialidade e dentro de um contexto histórico, cultural e socioeconômico é imprescindível.

Outras formas de construir, prever, circular, gerir, viver, planejar, se mover, desfrutar e disputar a cidade vem surgindo e refletem as muitas forças que atuam sobre ela: do planejamento à regulação de seus usos, do controle dos espaços aos atos de desobediência civil, dos corpos que ocupam às ruas às suas afetividades. A partir, principalmente, da chamada "virada espacial" – *spatial turn* –, os temas relacionados ao espaço – especialmente ao espaço urbano – e seus desdobramentos acabam ganhando destaque em várias áreas do conhecimento – ver, por exemplo, a influência de Lefebvre (1991); Harvey (1989); e Jacobs (2011) –, inclusive no campo da comunicação, onde os estudos que conjugam mídia, processos comunicacionais, mediações e cidades vem se multiplicando.

O interesse crescente pelas cidades contemporâneas se reflete em eventos de magnitudes e propósitos diversos, que se multiplicam ao redor do mundo, atraindo representantes da sociedade civil, de governos, da iniciativa privada e da academia. Um caso emblemático foi a III Conferência das Nações Unidas sobre Habitação e Desenvolvimento Urbano Sustentável (Habitat III), que aconteceu em outubro de 2016, em Quito, na qual foi assinada a Nova Agenda Urbana (NAU), que estabelece as diretrizes para o planejamento urbano sustentável nos próximos vinte anos.

Tendo como ponto de partida a relevância das cidades em um contexto global, assim como os muitos desafios ligados ao planejamento urbano, o objetivo central do trabalho aqui apresentado é oferecer uma discussão preliminar sobre cidades inteligentes a partir da perspectiva do direito à cidade e com uma análise crítica da ideia de "inteligência" urbana (MATTERN, 2017). Tendo a comunicação urbana como enquadramento teórico, busca-se analisar a presença de tecnologias nas cidades para além do *hype* de *smart city* e em diálogo com a NAU.

A primeira parte traz à tona uma reflexão sobre inteligência urbana e o entrelaçamento entre tecnologias e cidades. Já a segunda parte foca no direito à cidade sendo incorporado na Nova Agenda Urbana e como ela deve dialogar com iniciativas de cidades inteligentes. A última parte analisa brevemente a participação do Brasil da NAU e alguns desafios da implementação de diretrizes da agenda, principalmente no que diz respeito às iniciativas de cidades inteligentes.

CIDADES E TECNOLOGIAS: SOBRE MÍDIAS E INTELIGÊNCIAS

Tecnologia e cidades são temas que tem aparecido cada vez mais entrelaçados e muito se fala sobre "inteligência urbana". Pesquisadores se debruçaram sobre relações entre mídia, tecnologias e cidade por décadas, levantando debates que valem ser mencionados. Nos últimos anos houve um aumento considerável das abordagens que estudam os impactos de novas tecnologias nas cidades, com conceitos como "computação ubíqua" (*ubicomp*), "cidade informacional" (*informational city*), "cidade midiática" (*media city*), "cidade comunicativa" (*communicative city*) e "cidade inteligente" (*smart city*), entre tantos outros, ganhando terreno na literatura acadêmica, no setor privado e nas esferas de *policymaking*.

Scott McQuire (2006; 2008), por exemplo, contribuiu para o entendimento do conceito de "cidades midiáticas" (*media city*), nas quais os meios de comunicação de massa habitam os espaços públicos, coexistindo com as novas tecnologias e criando outras maneiras de experimentar os espaços urbanos. McQuire (2006, n.p.) apresenta a ideia de "cidade midiática" em contraposição ao conceito amplamente usado de "cidade informacional" (CASTELLS, 1989), uma vez que defende ser preciso reconhecer uma história mais longa e diversificada da produção mediada do espaço urbano do que aquela concentrada nas novas tecnologias da comunicação e da informação. A cidade moderna transforma-se em um espaço complexo que envolve mídia e arquitetura, no qual a produção mediatizada do espaço urbano se torna um quadro constitutivo para um novo modelo de experiência social (McQUIRE, 2008).

Contudo, é importante ressaltar que a relação entre cidade e mídia nem sempre é muito evidente, à primeira vista, como no imaginário das cidades inteligentes. Pensar além dos meios de comunicação de massa e das novas tecnologias permite enxergar as relações mais profundas e não óbvias, através de outras estruturas, outros processos e mediações cotidianas. Na análise apresentada em *Deep Mapping the Media City*, Shannon Mattern (2015) propõe uma *urban media archaeology* – em referência à Kittler e Griffin (1996), que desenvolveram a ideia da "cidade como meio" (*city as a medium*), permeada por redes de informação – que busque em profundidade a história material da cidade, para além dos dispositivos e de encontro às redes e ondas que constituem (e sempre constituíram) as cidades:

> […] nós também reconhecemos que as cidades inteligentes da atualidade não possuem um monopólio sobre a inteligência urbana. As cidades vêm incorporando redes inteligentes e formas de inteligência 'ambiente' muito antes do digital e do que passamos a chamar de "a Rede". Nossas cidades vêm sendo mediadas, e inteligentes, por milênios. (MATTERN, 2015, p. xii-xiii, tradução livre)[3]

Questionando a busca por *data-driven urban efficiencies* e se baseando em uma análise das estruturas urbanas crítica às iniciativas *smart*, Shannon Mattern (2017) traz uma importante contribuição para o debate aqui proposto:

> Conforme caminhamos para um futuro que nos oferece o potencial cada vez maior para um controle mediado da paisagem urbana e que, ao mesmo tempo, nos faz ter uma sensação difusa da *perda* de controle sobre a proliferação e aplicação - muitas vezes acrítica - de tecnologias em rede e metodologias baseadas em dados, nos faria bem refletir sobre que tipo de 'inteligência' ou 'consciência' nós gostaríamos que nossas cidades incorporassem, para então encorajar seus líderes e habitantes. Fazer isso, argumento, também requer que reconheçamos o fato de que as cidades inteligentes da atualidade não possuem monopólio da inteligência urbana. Na verdade, podemos traçar esse genoma da 'inteligência' até sua origem nas antigas Roma, Uruk e Catalhöyük. As cidades, incluindo muitas que estão muito distantes dos nossos data hubs e laboratórios de P&D contemporâneos, já incorporavam redes inteligentes e formas de inteligência 'ambiente' muito antes de colocarmos sensores nas ruas. As cidades do passado – mesmo nossos primeiros assentamentos – eram tão inteligentes quanto, apesar de

3 No original: "[…] we also recognize that today's smart cities don't have a monopoly on urban intelligence. Cities have embodied networked smarts and forms of "ambient" intelligence since long before the digital and what we know today as "the network". Our cities have been mediated, and intelligent, for millennia."

> que sua inteligência era menos computacional e mais material e ambiental. (MATTERN, 2017, P. x-xi, grifos no original, tradução livre)[4]

A noção de que as cidades inteligentes de hoje não têm o monopólio da inteligência urbana, já que as cidades sempre criaram e usufruíram de diferentes formas de inteligência – mesmo que menos computacionais e mais materiais (para quem as construía, administrava ou habitava) – ajuda a descontruir a visão de que a inteligência é algo novo ou corporativo. Levar em conta o ambiente urbano como meio *(medium)* , uma vez que as paisagens físicas das cidades "inscrevem, transmitem e até incorporam informações" (MATTERN, 2017, p. xii, tradução livre). [5]

Ao retomar o argumento de que as cidades vêm sendo inteligentes por milênios, Mattern (2015, 2017) afirma que essa inteligência é não apenas tecnológica, mas também epistemológica e física, indo além de cabos, protocolos, leis e instituições:

> […] por milênios, nossas cidades já eram inteligentes e mediadas, fornecendo espaços *para* a mediação dessa inteligência. Essa inteligência é simultaneamente epistemológica, tecnológica e física; está codificada nas leis, conhecimentos cívicos e instituições das nossas cidades, conectadas em seus cabos e protocolos, enquadradas em suas ruas e arquiteturas, em seus padrões de desenvolvimento. A cidade é mediada entre essas várias materialidades de inteligência, entre o éter e o minério de ferro. O barro e o código, a sujeira e os dados estão misturados aqui, como sempre estiveram. (MATTERN, 2017, p. xii, grifos no original, tradução livre) [6]

---

4 No original: "As we head into a future offering ever more potential for mediated control of the urban landscape, and, at the same time, a pervasive sense of our *loss* of control over the proliferation and sometimes uncritical application of networked technologies and data-driven methodologies, we would do well to enlighten *ourselves* about what kind of "smartness" or "sentience" we want our cities to embody and to encourage in its leaders and inhabitants. And doing so, I argue, requires that we also recognize today's smart cities don't have a monopoly on urban intelligence. In fact, we can trace that "smart" genome all the way back to ancient Rome, Uruk, Çatalhöyük. Cities, including many far afield from our contemporary data hubs and R and D labs, embodied networked smarts and forms of "ambient" intelligence well before we implanted sensors in the streets. Yesterday's cities – even our earliest settlements –were just as smart, although theirs was an intelligence less computational and more material and environmental."

5 No original: "inscribe, transmit, and even embody information."

6 No original: "[…] our cities have been smart and mediated, and they've been providing spaces *for* intelligence mediation, for millennia. That intelligence is simultaneously epistemological, technological, and physical; it's codified in our cities' laws and civic knowledges and institutions, hard-wired into their cables and protocols, framed in their streets and architectures and patterns of development. The city mediates between these various materialities of intelligence, between the ether and the iron ore. Clay and code, dirt and data intermingle here, and they always have."

Mattern (2017a, n.p.), em artigo publicado no *Places Journal*, defende que não podemos deixar que a ideia da "cidade como um computador" (*the city as computer*) nos previna de enxergar inúmeras outras formas dos dados e lugares de geração de inteligência na cidade – ela menciona, por exemplo, departamentos municipais, hospitais, laboratórios, empresas, arquivos municipais, bibliotecas, museus, etc.

Em um texto de 2016, publicado no *Mediapolis Journal*, Myria Georgiou questiona especificamente as relações existentes entre conectividade digital e o direito à cidade, especialmente no que diz respeito à cidade e ao urbanismo inteligente. Partindo de trabalhos como os de Greenfield (2013), Townsend (2013) e Niaros (2016), Georgiou afirma que:

> Os estudos críticos sobre o urbanismo inteligente já discutiram extensivamente sobre as conexões entre o utopismo digital e o capitalismo neoliberal, a vigilância e o determinismo tecnológico. Esses estudos apresentaram alternativas às apropriações que as políticas urbanas neoliberais fizeram do digital, propondo 'cidades (de dados) abertos/as'; 'cidades inteligentes voltadas para o bem comum'; e o 'direito à cidade híbrida'. Ainda assim, nessa literatura crítica, a vida digital é tomada como se fosse algo ordinário, e não só isso, mas como um quadro normativo para pensar o *direito à cidade*. Direta ou indiretamente, essa literatura confirma que o *direito à se comunicar (digitalmente)* é um caminho para o *direito à cidade*. (GEORGIOU, 2016, n.p., grifos no original, tradução livre)[7]

Para Georgiou, a falta de universalização da conectividade apropriada pode acabar excluindo as pessoas de processos participativos que acontecem digitalmente. Para ela:

> A conexão é política. Ela toca nos principais desafios da desigualdade nas cidades. Conforme o digital se tornou um espaço de muitas lutas sobre acesso e controle de recursos materiais e simbólicos, e também da regulação algorítmica da vida cotidiana, a conexão também é sobre exclusão e desigualdade. (GEORGIOU, 2016, n.p., tradução livre)[8]

7 No original: Critical scholarship on smart urbanism has discussed extensively the links between digital utopianism and neoliberal capitalism, surveillance, and techno-determinism. Such scholarship has proposed alternatives to the corporate and neoliberal urban policies' appropriations of the digital, by instead proposing "open (data) cities"; "commons-oriented smart city"; and the "right to the hybrid city." Yet, in this critical literature, digital life is still assumed as ordinary, and not only ordinary, but also a normative frame to think of the *right to the city*. Directly or indirectly, this literature confirms that the *right to (digitally) communicate* is a pathway to the *right to the city*".

8 No original: "Connection is political. It touches upon the core challenges of inequality in the city. As the digital has become a space for many struggles around access and control of symbolic and material resources, but also for algorithmic regulation of everyday life, connection is also about exclusion and inequality."

Uma área que vale destacar, e com a qual esse trabalho dialoga, é a "comunicação urbana" (*urban communication*). As discussões em torno da comunicação urbana são relativamente recentes[9] e se somam a outros debates que traçam as relações entre mídia e cidade. Nas palavras de Giorgia Aiello e Simone Tosoni (2016, p. 1253), a comunicação urbana se dedica a estudar as formas pelas quais as pessoas se conectam ou não com os outros e com o espaço urbano através de meios materiais, tecnológicos e simbólicos:

> De modo geral, os estudos de comunicação urbana estão preocupados com os modos pelos quais as pessoas nas cidades se conectam (ou não) com os outros e com o ambiente urbano, por meios simbólicos, tecnológicos e/ou materiais. Ao tentar entender essas relações mais amplas e suas dinâmicas, no entanto, é necessário manter um olhar holístico sobre as várias formas que esses estudos de fato assumem. Conforme nos mantemos observando o crescimento e o alcance da comunicação urbana como uma área de interesse independente, também é preciso parar e refletir o modo como nós, pesquisadores de mídia e comunicação, tratamos a cidade. (AIELLO; TOSONI, 2016, p. 1254, tradução livre) [10]

O espaço urbano construído também é comunicativo (DICKINSON; AIELLO, 2016, p. 1295) e se exacerba ao ser ocupado por diferentes práticas cotidianas.[11] Para Ferrara (2008, p. 43), "enquanto construção, a cidade é meio, enquanto imagem e plano, a cidade é mídia, enquanto mediação, a cidade é urbanidade". No Brasil, trabalhos interessantes que entrelaçam cidades, meios e mediações vêm sendo realizados. Vale citar Lucrécia D'Alessio Ferrara (2008), que coloca a cidade como a "maior experiência

9 Ver, por exemplo, a edição especial *Urban Communication: Going About the City: Methods and Methodologies for Urban Communication Research* do International *Journal of Communication*, organizada por Giorgia Aiello e Simone Tosoni, volume 10 de 2016. Ver também as coletâneas do *Urban Communication Reader*, em dois volumes: BURD *et al*., 2007 e JASSEM *et al*., 2010.

10 No original: "Generally speaking, urban communication scholarship is concerned with the ways in which people in cities connect (or do not connect) with others and with their urban environment via symbolic, technological, and/or material means. In trying to understand these broader relationships and dynamics, however, it is necessary to maintain an ecumenical view on the various forms that this kind of scholarship may in fact take. As we keep observing the growth and outreach of urban communication as an area of inquiry in its own right, we also need to take time to reflect on how we, as media and communication researchers, go about the city."

11 Ver, por exemplo, o conceito de "cidade comunicativa" (*communicative city*), cujos desdobramentos impulsionaram a criação de um prêmio e de uma área específica de estudo e atuação política (GUMPERT; DRUCKER, 2008; BURD, 2008; MATSAGANIS *et al*., 2013).

comunicativa da humanidade" (FERRARA, 2008, p. 42), cuja funcionalidade e comunicação são dois parâmetros básicos, induzidos através de sua forma construída, a arquitetura (FERRARA, 2008, p. 41-42).

Como mencionado anteriormente, esse trabalho está centrado na crescente disseminação de conceitos e inciativas vinculadas à uma ideia de "cidade inteligente" – e sua relação com o direito à cidade. Além de olhar de forma crítica para a associação entre inteligência urbana e novas tecnologias, é preciso também ter em mente as narrativas criadas em torno dos múltiplos conceitos de cidades inteligentes (ver, por exemplo, KITCHIN, 2014, 2015; KITCHIN *et al*, 2017; NIAROS, 2016; SHELTON *et al*, 2015). Para Söderström *et al* (2014), é relevante considerar a atividade discursiva em torno desses conceitos, uma vez que ela é performativa e "[…] molda os imaginários e práticas de uma miríade de atores construindo concretamente a cidade através de estudos de caso particulares ou projetos-piloto, decisões e ações cotidianas […]." (SÖDERSTRÖM *et al*, 2014, p. 307, tradução livre).[12] Os autores colocam o enredo dominante de cidades inteligentes como uma "[…] ferramenta estratégica para ganhar uma posição dominante em um mercado enorme." (SÖDERSTRÖM *et al*, 2014, p. 316, tradução livre)[13] ao se debruçarem sobre as narrativas construídas por grandes empresas como IBM, assim como o discurso em torno de cidades inteligentes é entendido por eles como um "*framing device*" (SÖDERSTRÖM *et al*, 2014, p. 317). Outros pontos que valem ser ressaltados – e que são resultado desse discurso – consistem na consolidação de um discurso tecnocrático e informacional da gestão urbana, na qual dados e softwares seriam suficientes; e na mentalidade de que os assuntos urbanos seriam apolíticos ou politicamente neutros (SÖDERSTRÖM *et al*, 2014, p. 317).

As questões levantadas por Söderström *et al* (2014) são de grande relevância para o debate aqui apresentado, já que oferecem uma perspectiva crítica para a adoção de inciativas de cidades inteligentes – e para o uso de rankings na avaliação de inteligência urbana:

> A aparente neutralidade política da narrativa dominante sobre cidades inteligentes é reforçada pela produção de critérios de avaliação e rankings, pelos quais as cidades são classificadas de acordo com seu grau de inteligência […]. Esses rankings e incentivos financeiros, alimentados por conversas inteligentes, levam à desenvolvimentos tecnológicos necessários, mas ao mesmo tempo podem ofuscar necessidades mais urgentes. Tornar-se uma

12 No original: "[…] shapes the imaginaries and practices of a myriad of actors concretely building the city through particular case studies or pilot projects, decisions and everyday action […]."

13 No original: […] strategic tool for gaining a dominant position in a huge market."

> cidade mais inteligente implica em dar prioridade a investimentos em tecnologia, enquanto moradias de baixo custo e sistemas de esgoto que não exigem altos investimentos em tecnologia são na verdade mais urgentes para muitas cidades no mundo. A prioridade na tomada de decisões não é, obviamente, um assunto apolítico, mas o núcleo duro das políticas municipais. (SÖDERSTRÖM *et al*, 2014, p. 317, tradução livre).[14]

Outras questões também devem ser levadas em conta ao se pensar em cidades inteligentes e o direito à cidade. O tema da privacidade tem aparecido com maior destaque na literatura técnica e acadêmica, no debate público e nos documentos da sociedade civil. Vale destacar brevemente o relatório da Privacy International intitulado *Smart Cities: Utopian Vision, Dystopian Reality* (2017), que parte da afirmação de que mesmo que se encare a *smart city* como um conceito mercadológico, as iniciativas de cidades inteligentes já estão moldando as ruas de cidades ao redor do mundo, e "[…] o que todas essas iniciativas têm em comum é que a inteligência é entendida como coleta de dados, facilitada pelo cada vez mais capazes sensores tecnológicos. Muitas daquelas iniciativas também focam intensamente em segurança." (PRIVACY INTERNATIONAL, 2017, p. 11, tradução livre).[15] Analisando casos de algumas cidades – incluindo o Rio de Janeiro – acabam identificando algumas tendências que devem ser mais amplamente discutidas: o crescimento da coleta de grande volume de dados[16] e dos propósitos de vigilância (ver também CARDOSO, 2014; BRUNO *et al*, 2015), assim como a necessidade de supervisão pública da questão, principalmente pelos cidadãos (PRIVACY INTERNATIONAL, 2017, p. 19-21).

A transferência da inteligência para os cidadãos – *smart citizens* e *smart citizenship* – e para o papel da participação cidadã no enquadramento teórico, técnico e prático das cidades inteligentes também vale ser mencionada, nem sempre funcionando como esperado, conforme mostram

---

14 No original: "The apparent political neutrality of the dominant smart city story is reinforced by the production of evaluation criteria and rankings where cities are classified according to their degree of smartness […]. Such rankings and financial incentives fueled by smart talk can of course lead to necessary technological developments, but they might also obfuscate more urgent needs. Becoming a smarter city implies giving priority to investments in technology while technology-poor affordable housing or sewage systems are arguably more urgent in many of the world`s cities. Priority-making is of course not an apolitical matter, but the very core of municipal politics."

15 No original: […] what all these initiatives have in common is that smartness is understood as data collection, facilitated by ever more capable sensor technologies. Many of those initiatives also have a strong focus on security."

16 Vale destacar também o interessante trabalho de Meijer, 2017.

Cardullo e Kitchin (2018).[17] Entre os principais achados dos autores, que analisaram o enquadramento dos cidadãos dentro de iniciativas de cidades inteligentes em Dublin, uma das principais críticas é a possibilidade de operar apenas dentro do modelo pré-estabelecido:

> Apesar da participação cidadã ser potencialmente diversa, na maioria das vezes ela é formulada de modo pós-político, fornecendo feedback, negociação, participação e criação, mas dentro de um enquadramento instrumental, ao invés de político ou normativo. Em outras palavras, os cidadãos são encorajados a ajudar na apresentação de soluções para questões práticas – tais como produzindo um aplicativo, comentando sobre um plano de desenvolvimento ou assumindo certos papéis/responsabilidades – mas não para questionar ou substituir as racionalidades políticas fundamentais que moldam uma questão ou plano. Ao invés disso, a maioria dos cidadãos são 'empoderados' nas cidades inteligentes por tecnologias que os tratam como consumidores ou testadores, ou como pessoas que serão direcionadas, controladas ou provocadas a agir de certa maneira, ou como fontes de dados que poderão ser transformados em produtos. Em outras palavras, cidadãos inteligentes atuam dentro dos limites de comportamento aceitáveis ou esperados, ao invés de transgredir ou resistir às normas sociais e políticas. Seu envolvimento expressão uma forma de cidadania neoliberal que não está baseada em direitos civis, políticos e sociais, ou na promoção do bem público e comum, mas sim na autonomia individual. Assim, as demandas voltadas à criação de cidades inteligentes 'centradas no cidadão' parecem ser muito superficiais ou meramente simbólicas, nas quais a administração da cidade ou as corporações continuam controlando a governança urbana e seus serviços, e as iniciativas de cidades inteligentes acabam sendo usadas para exercer uma forma de urbanismo empreendedor liderado pela tecnologia. (CARDULLO; KITCHIN, 2018, n.p., tradução livre) [18]

17 Ver também Datta (2017).

18 No original: "While citizen participation is potentially diverse, it is most often framed in a post-political way that provides feedback, negotiation, participation and creation, but within an instrumental rather than normative or political frame. In other words, citizens are encouraged to help provide solutions to practical issues – such as producing an app, or feeding back on a development plan, or to perform certain roles/responsibilities – but not to challenge or replace the fundamental political rationalities shaping an issue or plan. Instead, most citizens are "empowered" in the smart city by technologies that treat them as consumers or testers, or people to be steered, controlled, and nudged to act in certain ways, or as sources of data which can be turned into products. In other words, smart citizens perform within the bounds of expected and acceptable behaviour, rather than transgressing or resisting social and political norms. Their involvement expresses a form of neoliberal citizenship not grounded in civil, social and political rights, or in the promotion of public or common good, but rather in individual autonomy. As such, claims concerning the

Muitas dessas questões ainda não são abordadas de maneira adequada – e com a urgência necessária – nos espaços institucionalizados de debate e tomada de decisão: as cidades inteligentes ainda precisam ser melhor integradas à agenda de pesquisa e *advocacy* das conferências da ONU de políticas urbanas – como a Habitat – e de governança da internet – especialmente o Internet Governance Forum. Essa integração tem surgido, assim como estudos que se dedicam a obter uma perspectiva crítica, multidisciplinar das cidades inteligentes. Mudanças estão à caminho e é preciso levar em consideração o impacto de regulações como a General Data Protection Regulation (GDPR) 2016/679 da União Europeia, implementada em 2018, e a Lei Geral de Proteção de Dados (13.709/2018) brasileira, sancionada em agosto de 2018.[19]

A seguir será discutida a estruturação da Nova Agenda Urbana, um dos principais documentos que orientará a urbanização sustentável nos próximos anos, com destaque tanto para a incorporação do direito à cidade na agenda, quanto para o papel da discussão de cidades inteligentes na Habitat III e em seus documentos. Busca-se enfatizar questões que foram (ou não) levadas em conta no processo multissetorial que convergiu na NAU.

NOVA AGENDA URBANA: O DIREITO À CIDADE GANHA DESTAQUE

Em outubro de 2016 foi realizada a III Conferência das Nações Unidas sobre Habitação e Desenvolvimento Urbano Sustentável (Habitat III), em Quito, no Equador, cuja finalidade era debater os processos de urbanização e o desenvolvimento sustentável nos últimos vinte anos, bem como construir e adotar uma Nova Agenda Urbana (NAU), que consiste em um documento que orientará a urbanização sustentável nas próximas duas

production of "citizen-centric" smart cities appear to be largely tokenistic, with city administrations and corporations still owning and controlling urban governance and services, and smart city initiatives being used to enact a form of technologically-led entrepreneurial urbanism."

19 Outra questão que vale a pena seguir de perto nos próximos anos diz respeito ao arcabouço regulatório que impacta diretamente as inciativas de cidades inteligentes no Brasil, como as normas referentes às Parcerias Público-Privadas (ver ROLNIK *et al*, 2018), o Marco Regulatório para cidades inteligentes e os esforços em torno de Plano Diretor de tecnologias e cidades inteligentes (aprovado foi em Juazeiro do Norte-CE).

décadas.[20] Ela foi precedida pela Habitat II, que aconteceu em Istambul (1996) e a Habitat I, em Vancouver (1976). A NAU foi endossada pela Assembleia Geral da ONU em 23 de dezembro de 2016.

Os países-membros da Organização das Nações Unidas (ONU) produziram relatórios nacionais, que ajudaram a compor os relatórios regionais e o relatório global, a fim de guiar as discussões da Nova Agenda Urbana. Também vale ressaltar as muitas reuniões preparatórias e negociações em diversos níveis para se chegar a um acordo sobre o documento que guiará os esforços multissetoriais e de variados atores em relação às transformações urbanas nos vinte anos vindouros. Quito acolheu cerca de 30.000 pessoas, de muitos países e trajetórias, para refletir sobre o futuro urbano, tamanho o interesse no tema.

A estrutura das áreas e temas discutidos foram organizados conforme mostra o Quadro 2. Segundo Galindo e Monteiro (2016), dialogando com as seis áreas existem os documentos temáticos elaborados por especialistas, chamados de *issue papers*, cuja finalidade é "aprofundar a análise de questões importantes sobre temas urbanos para discussões na conferência que, após um processo de consulta, resultaram em documentos de *policy units*" (GALINDO e MONTEIRO, 2016, p. 27). Já as *policy units* são "documentos que apontam estudos, dados, práticas e desafios acerca de desenvolvimento urbano, assim como apontam recomendações técnicas, correlacionando temáticas vivenciadas em diversas cidades" (GALINDO; MONTEIRO, 2016, p. 28).

20 Ver: UNITED NATIONS. New Urban Agenda. 2017. Disponível em: <http://habitat3.org/the-new-urban-agenda/documents/issue-papers/>. Acesso em: 2 abr. 2018.

Quadro 2 – Enquadramento de áreas e temas dos *Issue Papers* e *Policy Units*, HABITAT III, 2016

Área	***Issue Papers***	***Policy Units***
1. COESÃO SOCIAL E EQUIDADE – CIDADES HABITÁVEIS	1.Cidades inclusivas	1. Direito à cidade e cidades para todos 2. Estruturas urbanas socioculturais
	2. Migração e refugiados em áreas urbanas	
	3.Cidades mais seguras	
	4.Cultura e patrimônio urbano	
2. ESTRUTURA URBANA	5. Normas e legislação urbana	3. Políticas urbanas nacionais 4. Governança, capacidade e desenvolvimento institucional urbanos 5. Finanças e sistema fiscal municipais
	6. Governança urbana	
	7. Finanças municipais	
3. DESENVOLVIMENTO ESPACIAL	8. Desenho e planejamento urbano e espacial	6. Estratégias territoriais urbanas: mercado imobiliário e segregação
	9. Terras urbanas	
	10. Conexões urbano-rurais	
	11. Espaço público	
4. ECONOMIA URBANA	12. Desenvolvimento econômico local	7. Estratégias de desenvolvimento econômico urbano
	13. Emprego e subsistência	
	14. Setor informal	
5. ECOLOGIA URBANA E MEIO AMBIENTE	15. Resiliência urbana	8. Ecologia urbana e resiliência
	16. Ecossistemas urbanos e gestão de recursos	
	17. Cidades, mudanças climáticas e a gestão de riscos de desastres	
6. HABITAÇÃO URBANA E SERVIÇOS BÁSICOS	18. Infraestrutura urbana e serviços básicos, incluindo energia	9. Serviços urbanos e tecnologia 10. Políticas habitacionais
	19. Transporte e mobilidade	
	20. Habitação	
	21. Cidades inteligentes	
	22. Assentamentos informais	

Fonte: UNITED NATIONS, 2016. Tradução e adaptação minha, baseadas nos documentos em inglês e português.[21]

21 Disponível em: THE NEW URBAN AGENDA. Disponível em: <http://habitat3.org/the-new-urban-agenda/>. Acesso em: 02 abr. 2018.

Pela primeira vez, o direito à cidade assumiu um papel central na composição da NAU. De acordo com Alfonsin *et al*. (2017), as conferências HABITAT envolvem intensa mobilização da sociedade civil ao redor do mundo, com participação ao longo do evento e em agendas de debate paralelas que pautam a construção da agenda urbana:

> Na Conferência de 2016 uma das articulações mais importantes, ao longo do processo preparatório, foi aquela conduzida pela 'Plataforma Global pelo direito à cidade', que congregou, internacionalmente, as diversas entidades e agremiações sociais que participaram do processo de construção internacional do direito à cidade, no qual a elaboração da 'carta Mundial pelo direito à cidade' foi um momento chave. O objetivo de tal articulação era incluir, na nova agenda urbana, o direito à cidade, reconhecido como um novo direito humano dos habitantes das cidades. (ALFONSIN, 2017, p. 1216)

Ao retratar os momentos e documentos da construção da categoria jurídica do direito à cidade, Alfonsin *et al*. (2017) refazem a trajetória desse conceito desde a publicação da emblemática obra de Henri Lefebvre, *Le droit à la ville* nos anos 1960 (ver LEFEBVRE, 2001), passando pelo Estatuto da Cidade (Lei 10.257/2001),[22] a Carta Mundial pelo Direito à Cidade[23] e a NAU/HABITAT III – salientando a centralidade do direito à cidade nos documentos. Os autores também chamam a atenção ao "valor legal atribuível" à NAU, considerada uma *Soft Law*, ou seja, sem valor vinculante, mas que exerce pressão política sobre os estados que assumem compromissos ao assiná-la (ALFONSIN *et al*, 2017, p. 1223-1224).

Como pode ser visto no Quadro 2, a primeira *policy unit* se dedica à questão do direito à cidade – *HABITAT III Policy Paper 1: Right to the City and Cities for All* –, colocando-o como um novo paradigma para o desenvolvimento urbano:[24]

> O Direito à Cidade deve ser considerado como um novo paradigma para o desenvolvimento urbano que busca resolver os principais desafios das cidades e assentamentos urbanos, como a rápida urbanização, redução da pobreza, exclusão social e riscos ambientais, que clamam por ações decisivas

22 Ver: BRASIL. LEI No 10.257, DE 10 DE JULHO DE 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10257.htm>. Acesso em: 02 abr. 2018.

23 Ver: INSTITUTO PÓLIS. Carta Mundial pelo Direito à Cidade. Disponível em: <http://www.polis.org.br/uploads/709/709.pdf>. Acesso em: 02 abr. 2018.

24 Ver: UNITED NATIONS. HABITAT III Policy Paper 1 – Right to the City and Cities for All. 2016. Disponível em: <http://habitat3.org/wp-content/uploads/Policy-Paper-1-English.pdf>. Acesso em: 02 abr. 2018.

> e prioridades políticas dos governos nacionais, regionais e locais. (UNITED NATIONS, 2016, p. 2, tradução livre).[25]

Um dos principais argumentos para que o direito à cidade tenha grande importância na atual agenda urbana baseia-se no fato de que o modelo de desenvolvimento urbano vigente não foi capaz de sanar problemas de desigualdade, pobreza e exclusão nas cidades. Com o rápido crescimento do número de pessoas vivendo em áreas urbanizadas, a urgência de garantir o cumprimento de diversos âmbitos dos direitos humanos se acentua:

> O direito à cidade […] fornece um enquadramento alternativo para repensar as cidades e a urbanização. Ele busca a efetiva realização de todos os direitos humanos internacionalmente acordados, dos objetivos de desenvolvimento sustentável, tal como estão expressos nos Marcos de Desenvolvimento Sustentável e dos compromissos da Agenda Habitat. Não obstante, em face dessa estrutura, ele traz uma nova dimensão que serve de fundação para a Nova Agenda Urbana, baseada na compreensão da cidade como lugar que se esforça para garantir uma vida decente e plena para todos os seus habitantes. (UNITED NATIONS, 2016, p. 3, tradução livre)[26]

Os princípios adotados se alinham às convenções, acordos e tratados internacionais de direitos humanos – como a Declaração e Programa de Ação de Viena de 1993. Partindo de 50 anos de experiência e debate, o conceito de direito à cidade adotado também se baseia em legislações nacionais, declarações municipais, entre outros documentos. Uma das referências citadas no *Policy Unit* é a Lei 10.257 de 10 de julho de 2001, conhecida como "Estatuto da Cidade", que estabelece diretrizes gerais para a política urbana no Brasil.[27]

---

25 No original: "The Right to the City should be considered as a new paradigm for urban development that seeks to address the major challenges in cities and human settlements of rapid urbanization, poverty reduction, social exclusion, and environmental risk that call for decisive actions and policy priorities by national, regional, and local governments."

26 No original: "The right to the city […] provides an alternative framework to rethink cities and urbanization. It envisions the effective fulfilment of all internationally agreed human rights, sustainable development objectives as expressed through the Sustainable Development Goals, and the commitments of the Habitat Agenda. Against this framework, it nevertheless brings a new dimension to serve as foundation for the New Urban Agenda based on an understanding of the city as a place that strives to guarantee a decent and full life for all inhabitants."

27 Ver: BRASIL. LEI No 10.257, DE 10 DE JULHO DE 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10257.htm>. Acesso em 02 abr. 2018.

O direito à cidade é um direito difuso e coletivo que pertence a todos os habitantes, no presente e no futuro, similar ao direito ao meio ambiente e outros instrumentos legais e leis nacionais, como de equidade de gênero, diversidade de expressões culturais e Patrimônio Mundial (UNITED NATIONS, 2016, p. 4), como pode ser visto na figura 2. Nesse enquadramento, o direito à cidade prevê:

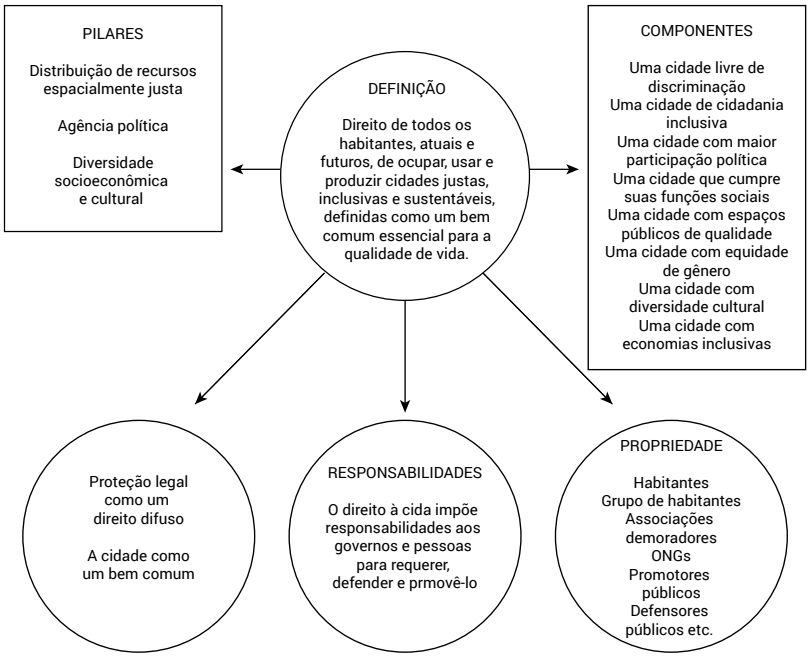
> […] garantir que todos os habitantes tenham capacidade de acessar os recursos urbanos, serviços, bens e oportunidades da vida na cidade; permitir a participação efetiva dos cidadãos nas políticas locais, com responsabilidade; permitir que governos garantam uma distribuição justa de recursos e reconhecer a diversidade sociocultural como fonte de aprimoramento social. (UNITED NATIONS, 2016, p. 5, tradução livre) [28]

A cidade como bem comum que engaja diversos atores e grupos de interesse para ação e implementação da Nova Agenda Urbana, dos cidadãos e organizações da sociedade civil ao governo – federal, estadual e municipal –, setor privado e academia. O acompanhamento desse processo se dá através, principalmente, da formulação, implementação e monitoramento de políticas. Segundo Nelson Saule Júnior:

> O direito à cidade deve ser adotado e compreendido na nova agenda urbana como o direito de todos os habitantes, da presente e das futuras gerações, de ocupar, usar e produzir cidades justas, inclusivas e sustentáveis, definido como um bem essencial comum para a qualidade de vida. O direito à cidade implica ainda responsabilidades sobre os governos e as pessoas a reclamar, defender e promover este direito. (SAULE JÚNIOR, 2016, p. 75)

28 No original: "[…] ensuring that all inhabitants have the capacity to access the urban resources, services, goods, and opportunities of city life; enabling effective citizen participation in local policies with responsibility; enabling governments to ensure just distribution of resources, and acknowledging sociocultural diversity as a source of social enhancement."

Figura 2 – Matriz do direito à cidade



Fonte: UNITED NATIONS, 2016. Tradução e adaptação minha.

Na visão compartilhada da Nova Agenda Urbana, em seu item 11, há um panorama sobre a inclusão do direito à cidade no documento e o lugar que ele ocupa na discussão geral:

> Partilhamos a visão de cidades para todos, no que se refere à igualdade de utilização e fruição de cidades e aglomerados urbanos, procurando promover a inclusão e assegurar que todos os habitantes, das gerações presentes e futuras, sem discriminações de qualquer ordem, possam habitar e construir cidades e aglomerados urbanos justos, seguros, saudáveis, acessíveis, resilientes e sustentáveis e fomentar a prosperidade e a qualidade de vida para todos. Salientamos os esforços envidados por governos nacionais e locais no sentido de consagrar esta visão, referida como direito à cidade, nas suas legislações, declarações políticas e diplomas. (UNITED NATIONS, 2017, p. 5)

Menções ao uso de tecnologias são transversais nos documentos, mas há casos específicos que valem ser citados para o propósito do debate aqui proposto. O *HABITAT III Policy Paper 9 – Urban Services and Technology*[29]

29 Ver: UNITED NATIONS. HABITAT III Policy Paper 9 – Urban Services and Technology. 2016a. Disponível em: <http://habitat3.org/wp-content/uploads/Policy-Paper-9-English.pdf>. Acesso em: 02 abr. 2018.

já indica, no sumário executivo, que as soluções tecnológicas devem ter como propósito contribuir para a equidade e o acesso aos serviços urbanos para todos os cidadãos, incluindo grupos vulneráveis. Adiante, no item 15, salienta que os serviços urbanos devem levar em consideração a crescente digitalização de modo a otimizar os usos de conhecimentos disponíveis, dados e tecnologias "inteligentes", desde que estas contribuam para melhorias para população a fim de manter ou conquistar uma distribuição equitativa e justa de recursos (UNITED NATIONS, 2016a, p. 6). Além disso, o papel do acesso à informação e dados é essencial nesse processo, assim como a questão de gênero:

> […] acesso aberto à informação e aos dados é crucial para democratizar conteúdos técnicos de decisões políticas. Investimentos urbanos sensíveis às questões de gênero são planejados e implementados com a devida consideração às dimensões de gênero e abordando adequadamente as necessidades, prioridades e preferências de infraestrutura das mulheres. (UNITED NATIONS, 2016a, p. 6, tradução livre).[30]

Ao falar das relações entre o avanço de conceitos de cidades inteligentes e o espaço urbano, o documento sugere precaução na integração dessas tecnologias com serviços e infraestrutura:

> O avanço dos conceitos de cidades inteligentes e o ritmo acelerado das tecnologias de informação e comunicação (TIC) tornando-se aninhados dentro da esfera urbana clamam por uma maior integração, ainda que cuidadosa, nas políticas de infraestrutura e serviços, sob condições de inclusão, segurança, resiliência e sustentabilidade, ao mesmo tempo em que devem levar em consideração as dinâmicas distintas de governança e inovação dos serviços e da infraestrutura urbana. A resiliência pode ser aprimorada pelo desenvolvimento de sistemas e redes adaptáveis, incluindo aqueles descentralizados que facilitam a autossuficiência dos municípios e comunidades. (UNITED NATIONS, 2016a, p. 2, tradução livre).[31]

---

30 No original: "[…] open access to information and data is crucial to democratizing technical contents of political decisions. Gender-responsive urban investments are planned and implemented with due consideration to gender dimensions and adequately addressing women's infrastructure needs, priorities and preferences."

31 No original: "The advancement of smart city concepts and the high pace of information and communications technology (ICT) becoming nested within the urban sphere both call for further yet careful integration into infrastructure and service polices under the conditions of inclusiveness, safety, resilience and sustainability, while taking into account the distinctive governance and innovation dynamics of urban services and infrastructure. Resilience may be improved by developing adaptive systems and networks, including decentralized ones facilitating the self-sufficiency of municipalities and communities."

Há também a identificação de categorias e tendências das áreas temáticas que são discutidas no *Policy Paper 9*, divididas em duas: "água, energia e recursos" e "transporte, mobilidade e acesso à oportunidades urbanas", e que podem ser amplamente beneficiadas por uma adoção crítica de tecnologias.

O *Issue Paper 21 – Smart Cities*[32] trata especificamente dos conceitos e aplicações de cidades inteligentes no enquadramento da HABITAT III, começando pelo reconhecimento da pluralidade conceitual em torno da cidade inteligente:

> Existem muitas definições do que é uma 'cidade inteligente' e abordagens 'inteligentes' vêm sendo compreendidas de modo distinto por diferentes pessoas e setores. Algumas definições apontam que cidade inteligentes são aquelas com 'infraestrutura física, social, institucional e econômica inteligente, que ao mesmo tempo garanta a centralidade do cidadão em um ambiente sustentável'; se referem a características chave definidas por fatores distintos (ex.: economia inteligente, mobilidade inteligente, pessoas inteligentes, ambiente inteligente, habitação inteligente, governança inteligente); e focam no uso estratégico de novas tecnologias e abordagens inovadoras para aprimorar a eficiência e competitividade das cidades. A definição do Grupo Focal em Cidades Inteligentes sustentáveis (FG-SSC) da União Internacional de Telecomunicações (ITU) apresenta: 'uma cidade inteligente sustentável é uma cidade inovadora que usa as TICs e outros meios para melhorar a qualidade de vida, a eficiência dos serviços e operações urbanas e a competitividade, ao mesmo tempo em que garante os meios para suprir as necessidades de gerações presentes e futuras, com relação aos aspectos econômicos sociais e ambientais'. O Departamento de Negócios, Inovação e Competências do Reino Unido, considera as cidades inteligentes como um processo, ao invés de um resultado estático, pelo qual o engajamento cidadão, a infraestrutura pesada, capital social e tecnologias digitais 'tornam as cidades mais habitáveis e resilientes e, com isso, capazes de responder mais rápido aos novos desafios'. A Accenture define como inteligente a cidade que fornece serviços para cidadãos e empresas de maneira eficiente em recursos e integrada, e permite colaborações inovadoras para melhorar a qualidade de vida e apoio ao crescimento da economia local e nacional. (UNITED NATIONS, 2015, p. 1, tradução livre) [33]

32 Ver: UNITED NATIONS. HABITAT III ISSUE PAPERS: 21 – SMART CITIES. Disponível em: <http://habitat3.org/wp-content/uploads/Habitat-III-Issue-Paper-21_Smart-Cities-2.0.pdf>. Acesso em: 02 abr. 2018.

33 No original: "Many definitions of "smart city" exist, and "smart" approaches have been understood differently by different people and sectors. Some definitions note that smart cities are those cities with "smart (intelligent) physical, social, institutional and economic infrastructure while ensuring centrality of citizens in a sustainable environment;" refer to key characteristics defined by distinct factors (e.g., smart economy, smart mobility, smart people, smart environment, smart living, smart governance); and focus on the strategic use of new technology and innovative approaches to enhance the efficiencies and competitiveness of cities. A definition by the International Telecommunication Union

O documento posiciona as cidades inteligentes como "uma opção viável para o futuro" (UNITED NATIONS, 2015, p. 3), colocando vários atributos, temas e infraestruturas que devem estar ligadas ao conceito de inteligência urbana (ver Quadro 3):

Quadro 3 – Aspectos de uma cidade inteligente sustentável

Atributos	Sustentabilidade: Relacionada à infraestrutura e governança da cidade, energia e mudanças climáticas, poluição, resíduos, sociedade, economia e saúde;
	Qualidade de vida (QdV): Melhoria da QdV em termos de bem-estar emocional e financeiro;
	Aspectos urbanos: Inclui tecnologia e infraestrutura, sustentabilidade, governança e economia;
	Inteligência ou *smartness*: Aspectos de inteligência comumente citados incluem economia inteligente, pessoas inteligentes, governança inteligente, mobilidade inteligente, vida inteligente, meio ambiente inteligente.
Temas	Sociedade: A cidade é para seus habitantes;
	Economia: A cidade deve ser capaz de prosperar – empregos, crescimento econômico e financeiro, etc.;
	Meio ambiente: A cidade deve ser sustentável em seu funcionamento para as gerações presente e futuras;
	Governança: A cidade deve ser robusta em sua habilidade para administrar políticas públicas.
Infraestrutura	Infraestrutura física inclui edifícios, ferrovias, estradas, linhas elétricas, gasodutos, água, indústrias, etc.;
	A infraestrutura de TIC age como a "cola" que integra todos os outros elementos de inteligência da cidade, atuando como uma plataforma fundamental. A infraestrutura de TIC funciona como o centro nervoso, orquestrando todas as diferentes interações entre vários elementos importantes.

Fonte: UNITED NATIONS, 2015. Tradução e adaptação minha, baseadas nos documentos em inglês e português.

(ITU)'s Focus Group on Smart Sustainable Cities (FG-SSC) reads: "A smart sustainable city is an innovative city that uses ICTs and other means to improve the quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects." The UK Department of Business, Innovation and Skills considers smart cities a process rather than as a static outcome, through which citizen engagement, hard infrastructure, social capital and digital technologies "make cities more livable and resilient and, hence, able to respond quicker to new challenges." Accenture defines smart city as a city that delivers services to citizen and businesses in an integrated and resource efficient way and enables innovative collaborations to improve inhabitants' quality of life and support the growth of the local and national economy."

É importante ressaltar que a urgente questão referente à privacidade e proteção de dados pessoais dos cidadãos não entrou nesse mapeamento dos aspectos de uma cidade inteligente sustentável. O documento aponta, ainda, as principais áreas necessárias para um novo modelo de planejamento urbano: ruas e espaços públicos de alta qualidade; densidade adequada e bem desenhada; usos urbanos mistos e limitação da especialização do uso da terra; conectividade; estrutura social mista; resiliência urbana; eficiência de energia e recursos; observância de normas e regras (UNITED NATIONS, 2015, p. 4-5). Também se reconhece que as cidades inteligentes não existem em um vácuo e precisam ser devidamente integradas aos seus territórios, como as áreas rurais, e com o uso estratégico de novas e antigas tecnologias para dar voz às populações marginalizadas e em situação de vulnerabilidade (UNITED NATIONS, 2015, p. 7).

O *Issue Paper 21* indica, por fim, os principais fatores para a ação, que se baseiam em políticas estratégicas, legislação, regras e regulação, tendo em vista que os benefícios não são automáticos; planejamento/desenho urbano responsivo e inovador; planejamento financeiro robusto, baseado no contexto local; e coerência, advinda principalmente de um consenso internacional do que é uma cidade inteligente e sustentável (UNITED NATIONS, 2015, p. 7-8). O uso e a adoção crítica da tecnologia no âmbito municipal perpassa o documento em questão e as discussões preparatórias para a HABITAT III, e que a NAU incorpora em seu texto.

Já no próprio documento da NAU a única menção direta (item 66) à questão das cidades inteligentes diz respeito, em linhas gerais, à abordagem adotada:

> Comprometemo-nos a adotar uma abordagem de 'cidade inteligente' que faça uso de oportunidades de digitalização, energia e tecnologias limpas, assim como de tecnologias de transporte inovadoras, proporcionando consequentemente alternativas para os habitantes tomarem escolhas mais amigáveis ao ambiente e impulsionarem o crescimento econômico sustentável, permitindo que as cidades melhorem a sua prestação de serviços. (UNITED NATIONS, 2017, p. 19, tradução livre) [34]

Ao incorporar conceitos de cidades inteligentes nos documentos preparatórios e na própria NAU, os atores envolvidos na Habitat III, por um lado, reconhecem a emergência dessa tendência; mas, por outro lado, trazem para as orientações que guiarão as políticas urbanas nas próximas duas décadas um conceito bastante corporativo – e sem algumas reflexões

34 No original: "We commit ourselves to adopting a smart-city approach that makes use of opportunities from digitalization, clean energy and technologies, as well as innovative transport technologies, thus providing options for inhabitants to make more environmentally friendly choices and boost sustainable economic growth and enabling cities to improve their service delivery".

necessárias sobre desafios que as iniciativas de cidades inteligentes impõem aos municípios. Como será visto adiante, a participação do Brasil na preparação dos documentos e na reflexão posterior à conferência apontam lacunas e questões que precisam ser melhor discutidas (BALBIM, 2017).

A PARTICIPAÇÃO DO BRASIL E OS DESAFIOS VINDOUROS

É importante salientar as contribuições e análises do Brasil nas discussões que moldaram a Habitat III e a Nova Agenda Urbana. De acordo com Galindo e Monteiro (2016), em texto publicado anteriormente ao Encontro em Quito, coube ao Ipea a relatoria do documento brasileiro, conforme estipulou a Resolução Administrativa nº 29, de 25 de julho de 2014.[35] Os autores afirmam que:

> No âmbito dos Estados-partes, foram inicialmente solicitados relatórios nacionais com a análise dos últimos vinte anos, apontando também diretrizes para os próximos vinte. No Brasil, coube ao Ipea, a convite do Conselho das Cidades do Ministério das Cidades (ConCidades/MCidades), a relatoria do documento brasileiro, nos termos da Resolução Administrativa nº 29, de 25 de julho de 2014. Administrativamente, a parceria foi estabelecida externamente por um termo de execução descentralizada e internamente por meio de projeto de pesquisa alocado no plano de trabalho da Diretoria de Estudos e Políticas Regionais, Urbanas e Ambientais (Dirur) do Ipea. Além dos produtos já finalizados com o relatório nacional, eventos acompanhados e organizados e publicações diversas, o Ipea dedica-se no momento a elaborar um novo documento em conjunto com o ConCidades para pautar a discussão da nova agenda urbana. (GALINDO; MONTEIRO, 2016, p. 25)

Os comentários da República Federativa do Brasil aos *HABITAT III Policy Papers*, realizados por 14 Ministérios no nível federal, assim como estados e municípios, evidencia os esforços em construir uma agenda urbana que dialogasse com questões de grande relevância para as cidades brasileiras.[36]

O reconhecimento do direito à cidade como um aspecto central da NAU é visto como bastante positivo na análise brasileira do *Policy Paper 1 – Right to the City and Cities for All,*[37] assim como a garantia do direito à

35 Disponível em: <http://www.lex.com.br/legis_25874832_RESOLUCAO_ADMINISTRATIVA_N_29_DE_25_DE_JULHO_DE_2014.aspx>. Acesso em: 02 abr. 2018.

36 O documento pode ser encontrado em: <http://habitat3.org/wp-content/uploads/PU_Comments_Brazil.pdf>. Acesso em 02 abr. 2018.

37 Ver: UNITED NATIONS. HABITAT III POLICY PAPER: 1 – RIGHT TO THE CITY AND CITIES FOR ALL. Disponível em: <http://habitat3.org/wp-content/uploads/PU1-HABITAT-III-POLICY-PAPER.pdf>. Acesso em: 02 abr. 2018.

participação, institucionalizada ou não, com regras e papeis bem delineados, identificando, também, a cidade como espaço de debate e conflito (BRASIL, 2016, p. 1). Além disso, ressalta-se a importância de fomentar planejamento e gestão urbana participativos, de modo a dialogar com princípios de governança como a acessibilidade, transparência e inclusão.

Outros pontos positivos endossados no documento são (BRASIL, 2016, p. 2): a necessidade de se criar mecanismos que fortaleçam a identidade urbana, cultura e patrimônio; a importância de se garantir os espaços públicos como lugares de geração de renda e atividades legalizadas; a abordagem da dicotomia crescimento e bem-estar, que foca na formulação e implementação de estratégias de desenvolvimento que priorizem o bem-estar humano, lutem contra a pobreza e garantam meios de subsistência para todos.

O tratamento sugerido para evitar gentrificação em grandes projetos urbanos e em projetos implementados via parcerias público-privadas com grandes empresas, buscando-se propostas para a descomodificação dos espaços urbanos e a discussão de mecanismos que balanceiem a distribuição de problemas e benefícios que surgem dos processos de urbanização. Ganham destaque outras questões, como o tratamento adequado de questões ambientais; políticas de empregabilidade para populações jovens; equilíbrio do desenvolvimento de regiões metropolitanas, médias e pequenas cidades; entre outras (BRASIL, 2016, p. 2-3).

O documento também aponta omissões de importantes questões, como a não inserção de vários grupos minoritários e sub-representados (BRASIL, 2016, p. 3): jovens, idosos, pessoas com deficiência, crianças e a população LGBT, além de pessoas que sofrem discriminação racial, étnica e religiosa. A falta do caráter interseccional de vulnerabilidades e discriminação – ressaltando-se a juventude negra no Brasil – é tida como um ponto que precisava ser melhorado na discussão do direito à cidade na NAU.

Dentro dos objetivos estabelecidos neste trabalho, vale também abordar alguns comentários e análises do governo brasileiro ao *Habitat III Policy Paper 9 – Urban Services and Technology*.[38] As críticas se voltaram às omissões de questões consideradas relevantes, como a falta de atenção apropriada ao debate sobre cidades inteligentes e tecnologias (BRASIL, 2016, p. 28), que foram abordadas nos *Issue Papers*. Alguns pontos destacados pelo Brasil em relação às cidades inteligentes e que merecem atenção (BRASIL, 2016, p. 29, tradução nossa) são:

38 Ver: UNITED NATIONS HABITAT III POLICY PAPER: 9 – URBAN SERVICES AND TECHNOLOGY <http://habitat3.org/wp-content/uploads/PU9-HABITAT-III-POLICY-PAPER.pdf>. Acesso em: 02 abr. 2018.

I. Criar de cidades inteligentes sustentáveis, com modelos de financiamento de longo prazo e legislações que levem em conta proteção de dados;
II. Estimular a criação e o desenvolvimento de soluções que usem *Internet of Things;*
III. Encorajar o desenvolvimento de startups focadas em gestão de resíduos, saúde, água e esgoto, segurança pública, ecologia urbana e energia, assim como na promoção da capacitação na implementação de tecnologias inteligentes;
IV. Fomentar a participação da sociedade civil em projetos de cidades inteligentes e que o debate sobre "cidades inteligentes" seja baseado na promoção de inclusão social;
V. Garantir que os projetos de cidades inteligentes sejam adequados às aos contextos e particularidades das cidades, levando em consideração a forte assimetria no controle dos dados existentes sobre as pessoas – é preciso explorar melhor os potenciais efeitos do uso de Big Data na gestão das cidades, evidenciando problemas e discutindo os possíveis benefícios para os cidadãos;
VI. Incentivar a adoção de tecnologias abertas, de propriedade independente e colaborativa, assim como o uso de software livre na administração pública, especialmente em sistemas de informação de gestão e planejamento.

O Brasil também forneceu comentários aos *Issue Papers* para ajudar nas discussões da Habitat III. Cabe aqui destacar a breve contribuição ao *Issue Paper 21: Smart Cities*.[39] O documento aponta, em poucas linhas, que diante da crescente urbanização, pesquisas e trabalhos sobre cidades inteligentes devem resultar:

> Na oferta de modelos responsivos às crescentes pressões enfrentadas por países em desenvolvimento para fornecer mais e melhores serviços básicos à uma população urbana crescente. No que diz respeito à aplicação do conceito de 'cidades inteligentes' para países em desenvolvimento, também é importante enfatizar que as discussões devem levar em consideração a possibilidade de salto nas cidades dos países em desenvolvimento, com a incorporação de tecnologia de ponta, assim como o acesso facilitado à tecnologias urbanas básicas já consolidadas. (BRASIL, 2016a, n.p., tradução livre)[40]

39 Ver: HABITAT III. Comments from Brazil to the issue papers that will inform the discussions of the UN Habitat III Conference. Disponível em: <http://habitat3.org/wp-content/uploads/BRASIL-Comments-on-Habitat-III-Issue-Papers.pdf>. Acesso em: 02 abr. 2018.

Renato Balbim (2017) faz uma breve reflexão sobre seu livro *A geopolítica das cidades: velhos desafios, novos problemas*, organizado por ele e lançado pelo Ipea em 2016, antes da Habitat III. Nessa reflexão, ele indica, entre outros pontos, que "a forte presença das empresas de tecnologia no comando dos destinos da NAU" (BALBIM, 2017, p. 43) pode ser percebida após a análise atenta dos documentos da conferência:

> A ideia de smart cities, em certa medida já antiga, foi, pela primeira vez, referendada em uma conferência da ONU. Diversas foram as mesas de debate sobre o tema durante a conferência, com a presença de bancos, companhias e consultores internacionais. A ideia de smart cities faz parte dos documentos finais e é apresentada como uma das soluções para inúmeros problemas nos mais diversos contextos urbanos. A feira de expositores durante o evento, por exemplo, teve forte presença de companhias e bancos internacionais, 37 de 141 expositores, interessados em apresentar temáticas similares. A título de exemplo, os termos 'informação', 'comunicação' e 'tecnologia' aparecem 41 vezes no texto final da NAU, enquanto o termo "direito" aparece 23 vezes. É exemplar também como vários compromissos assumidos são claras intenções de reconhecimento e/ou abertura de mercados, lembrando sempre que, apesar de citado o termo, não há o efetivo reconhecimento do 'direito à cidade' na NAU. (BALBIM, 2017, p. 43)

Essa reflexão de Balbim é fundamental para a discussão aqui apresentada, justamente por oferecer um contraponto bastante crítico do papel do setor privado e da narrativa das cidades inteligentes na NAU. As iniciativas de cidades inteligentes já são uma realidade em diversos municípios brasileiros, com a consolidação de centros de operações e departamentos cuja finalidade é monitorar a cidade em tempo real, coletar grandes volumes de dados e dirigir a tomar decisões. A ocorrência de fóruns variados de cidades inteligentes, a criação de *rankings*[41] e a participação do setor privado na discussão e aprovação de quadros regulatórios para municípios brasileiros chama a atenção para a urgência de se olhar para esse tema a partir de uma perspectiva crítica, multissetorial e transdisciplinar.

---

40 No original: "In the offer of models responsive to the increasing pressures faced by developing countries to deliver more and better basic services to a growing urban population. As far as the application of the concept "smart cities" to developing countries is concerned, it is also important to emphasize that the discussions should take into consideration the possibility of leap-frogging for cities in developing countries, with the incorporation of cutting edge technology, as well as the facilitated access to already consolidated basic urban technologies."

41 Ver, por exemplo: CONNECTED SMART CITIES. Ranking: conceito. Disponível em: <http://www.connectedsmartcities.com.br/ranking-conceito/>. Acesso em: 20 set. 2018.

CONSIDERAÇÕES FINAIS

A Nova Agenda Urbana deu passos importantes na incorporação e consolidação do conceito de direito à cidade, graças à mobilização de diversos atores em torno da problemática nas últimas décadas. A Nova Agenda Urbana tem muitos pontos que mostram a complexidade do pensar, gerir e viver a/na cidade. Como visto, as tecnologias são partes essenciais desse processo e do cotidiano urbano que precisam ser utilizadas e entendidas de acordo com suas potencialidades e limitações.

É necessário não ver a inteligência urbana como algo que diz respeito apenas às iniciativas inteligentes, ou as novas tecnologias como um fim em si mesmo. Também é preciso enxergar para além do *hype* das *smart cities*, uma vez que as tecnologias não são solucionadoras automáticas de problemas, mas sim ferramentas promissoras, repletas de desafios – como a privacidade e a proteção de dados pessoais, por exemplo. A participação social deve ser levada em consideração ao longo da priorização e escolha de tecnologias, assim como durante sua implementação e avaliação, para além do usual enquadramento de *smart citizenship*.

As relações entre a NAU, o direito à cidade e as tecnologias serão questões centrais das políticas urbanas nos próximos anos, já que as iniciativas de cidades inteligentes já estão sendo implementadas nos municípios brasileiros, o enquadramento regulatório deixa a desejar e a participação social nessas tomadas de decisão não se tornou uma realidade difundida. Um alinhamento das agendas de governança da internet e de políticas urbanas, assim como a urgência de se olhar para as cidades inteligentes a partir de uma perspectiva crítica, multissetorial e transdisciplinar são essenciais para garantir o direito à cidade (inteligente).

REFERÊNCIAS

AIELLO, Giorgia; TOSONI, Simone. Going about the city: methods and methodologies for urban communication research. *International Journal of Communication*, v. 10, p. 1252-1262, 2016.

ALFONSIN, Betânia de Moraes *et al*. Das ruas de Paris a Quito: o direito à cidade na nova agenda urbana - Habitat III. *Revista de Direito da Cidade*, v. 9, n. 3, p. 1214-1246, jul. 2017. Disponível em: <http://www.e-publicacoes.uerj.br/index.php/rdc/article/view/29236>. Acesso em: 15 jul. 2018.

BALBIM, Renato. A geopolítica das cidades e a Nova Agenda Urbana. *IPEA - Boletim Regional, Urbano e Ambiental*, 17, jul.-dez. 2017. Disponível em <http://repositorio.ipea.gov.br/bitstream/11058/8139/1/BRU_n17_Geopol%C3%ADtica.pdf>. Acesso em: 15 jul. 2018.

BRASIL. Comments by the Federative Republic of Brazil on the Habitat III Policy Papers. 2016. Disponível em <http://habitat3.org/wp-content/uploads/PU_Comments_Brazil.pdf>. Acesso em: 02 abr. 2018.

BRASIL. Comments from Brazil to the issue papers that will inform the discussions of the UN Habitat III Conference. 2016a. Disponível em: <http://habitat3.org/wp-content/uploads/BRASIL-Comments-on-Habitat-III-Issue-Papers.pdf>. Acesso em: 02 abr. 2018.

BRASIL. LEI No 10.257, DE 10 DE JULHO DE 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10257.htm>. Acesso em: 02 abr. 2018.

BRUNO, Fernanda.; BEZERRA, Julio.; MILANI, Wilson. Tecnopolíticas e Vigilância - Editorial. *Revista Eco-Pós*, v. 18, p. 1-7, 2015.

BURD, Gene. The Mediated Metropolis as Medium and Message. *The International Communication Gazette*, v. 70, n. 3-4, p. 209-222, 2008.

BURD, Gene; DRUCKER, Susan J.; GUMPERT, Gary. *Urban Communication Reader*. Cresskill: Hampton Press, 2007.

CARDOSO, Bruno V. *Todos os Olhos*: videovigilâncias, voyeurismo e (re)produção imagética. Rio de Janeiro: Editora UFRJ; Editora Faperj, 2014.

CARDULLO, Paolo; KITCHIN, Rob. Being a 'citizen' in the smart city: up and down the scaffold of smart citizen participation in Dublin, Ireland. *GeoJournal*, v. 84 n. 1, 2019. https://doi.org/10.1007/s10708-018-9845-8

CASTELLS, Manuel. *The Informational City*. Oxford and Cambridge: Blackwell, 1989.

CONNECTED SMART CITIES. Ranking: conceito. Disponível em: <http://www.connectedsmartcities.com.br/ranking-conceito/>. Acesso em: 20 set. 2018.

DATTA, Ayona. The digital turn in postcolonial urbanism: Smart citizenship in the making of India's 100 smart cities. *Trans Inst Br Geogr*, p. 1-15, 2018. DOI: https://doi.org/10.1111/tran.12225

DICKINSON, Greg; AIELLO, Giorgia. Being through there matters: materiality, bodies, and movement in urban communication research. *International Journal of Communication*, v. 10, p. 1294-1308, 2016.

FERRARA, Lucrécia D'Alessio. Cidade: meio, mídia e mediação. *MATRIZes*, n. 2, p. 39-52, 2008.

GALINDO, Ernesto; MONTEIRO, Roberta A. Nova Agenda Urbana no Brasil à luz da Habitat III. *IPEA - Boletim Regional, Urbano e Ambiental*, 15, jul./dez. 2016. Disponível em: <http://repositorio.ipea.gov.br/bitstream/11058/7085/1/BRU_n15.pdf>. Acesso em: 15 jul. 2018.

GEORGIOU, Myria. Right to the City, or Compulsion to Connect? *Mediapolis Journal*, n. 5, v. 1, nov. 2016. Disponível em: <http://www.mediapolisjournal.com/2016/11/right-city-compulsion-connect/>. Acesso em: 15 jul. 2018

GREENFIELD, Adam. *Against the Smart City.* Londres: Do Projects, 2013.

GUMPERT, Gary; DRUCKER, Susan J. Communicative Cities. *The International Communication Gazette*, v. 70, n. 3-4, p. 195-208, 2008.

HABITAT III. Comments from Brazil to the issue papers that will inform the discussions of the UN Habitat III Conference. Disponível em: <http://habitat3.org/wp-content/uploads/BRASIL-Comments-on-Habitat-III-Issue-Papers.pdf>. Acesso em: 02 abr. 2018.

HARVEY, David. *The condition of postmodernity*: An enquiry into the origins of cultural change. Cambridge: Blackwell Publishers, 1989.

IBGE. Censo demográfico 1940-2010. Disponível em: <https://seriesestatisticas.ibge.gov.br/series.aspx?vcodigo=pop122>. Acesso em: 02 abr. 2018.

INSTITUTO PÓLIS. Carta Mundial pelo Direito à Cidade. Disponível em: <http://www.polis.org.br/uploads/709/709.pdf>. Acesso em: 02 abr. 2018.

JACOBS, Jane. *The Death and Life of Great American Cities*: 50th Anniversary edition. Nova York: Modern Library, 2011.

JASSEM, Harvey; DRUCKER, Susan J; BURD, Gene. *Urban Communication Reader*. Cresskill: Hampton Press, 2010. v. 2.

KITCHIN, Rob. The real-time city? Big data and smart urbanism. **GeoJournal**, 79:1–14. 2014

KITCHIN, Rob. Making sense of smart cities: addressing present shortcomings. *Cambridge Journal of Regions, Economy and Society*, v. 8, n. 1, p. 131–136, mar. 2015. DOI: <https://doi.org/10.1093/cjres/rsu027>.

KITCHIN, Rob; LAURIAULT, Tracey P.; MCARDLE, Gavin (Eds.). *Data and the City.* Nova York and Oxon: Routledge, 2017.

KITTLER, Friederich A; GRIFFIN, Matthew. The City as a Medium. *New Literary History*, v. 27, n. 4, p. 717-729, 1996.

LEFEBVRE, Henri. *The Production of Space*. Oxford: Blackwell Publishers, 1991.

LEFEBVRE, Henri. *O direito à cidade*. São Paulo: Centauro, 2001.

MATSAGANIS, Matthew D; GALLAGHER, Victoria J; DRUCKER, Susan J (Eds.). *Communicative Cities in the 21st Century*: the Urban Communication Reader III. New York: Peter Lang Publishing, 2013.

MATTERN, Shannon. *Deep Mapping the Media City*. Minneapolis, University of Minnesota Press, 2015.

MATTERN, Shannon. *Code and Clay, Data and Dirt*. Minneapolis, University of Minnesota Press, 2017.

MATTERN, Shannon. *A City Is Not a Computer. Places Journal,* fev. 2017a. Accesso em 15 jun. 2018. DOI: https://doi.org/10.22269/170207

MEIJER, Albert. Datapolis: A Public Governance Perspective on "Smart Cities". *Perspectives on Public Management and Governance*, v. 1, n. 3, p. 195-206, ago. 2018. DOI: <https://doi.org/10.1093/ppmgov/gvx017>.

NIAROS, Vasilis. Introducing a Taxonomy of the 'Smart city': Towards a Commons-Oriented Approach". *Triple-C*, n. 1, p. 51-61, 2016. Disponível em: <http://www.triple-c.at/index.php/tripleC/article/view/718>. Acesso em: 10 jul. 2018

PRIVACY INTERNATIONAL. Smart Cities: Utopian Vision, Dystopian Reality, out. 2017. Disponível em: <https://privacyinternational.org/report/638/smart-cities--utopian-vision-dystopian-reality>. Acesso em: 12 jul. 2018.

ROLNIK, Raquel; SANTORO, Paula F.; NASCIMENTO, Denise. M.; FREITAS, Daniel M.; RENA, Natacha.; PEQUENO, Luis. Renato B. (Orgs.). *Cidade Estado Capital*: reestruturação urbana e resistências em Belo Horizonte, Fortaleza e São Paulo. São Paulo: FAUUSP, 2018.

SAULE JÚNIOR, Nelson. O direito à cidade como centro da Nova Agenda Urbana. *IPEA - Boletim Regional, Urbano e Ambiental,* jul./dez. 2016. Disponível em: <http://repositorio.ipea.gov.br/bitstream/11058/7085/1/BRU_n15.pdf >. Acesso em: 15 jul. 2018.

SHELTON, Taylor; ZOOK, Matthew; WIIG, Alan. The 'actually existing smart city'. *Cambridge Journal of Regions, Economy and Society*, v. 8, n. 1, p. 13-25, mar. 2015. DOI: <https://doi.org/10.1093/cjres/rsu026>.

SÖDERSTRÖM, Ola; PAASCHE, Till; KLAUSER, Francisco. Smart cities as corporate storytelling, *City*, v. 18, n. 3, p. 307-320, 2014. DOI: 10.1080/13604813.2014.906716.

THE NEW URBAN AGENDA. Disponível em: <http://habitat3.org/the-new-urban--agenda/>. Acesso em: 02 abr. 2018.

TOWNSEND, Andrew. *Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia*. Nova York: W. W. Norton, 2013.

UNITED NATIONS. HABITAT III Issue Paper 21 – Smart Cities. 2015. Disponível em: <http://habitat3.org/wp-content/uploads/Habitat-III-Issue-Paper-21_Smart-Cities-2.0.pdf>. Acesso em: 2 abr. 2018.

UNITED NATIONS. HABITAT III Policy Paper 1 – Right to the City and Cities for All. 2016. Disponível em: <http://habitat3.org/wp-content/uploads/Policy-Paper-1-English.pdf>. Acesso em: 02 abr. 2018.

UNITED NATIONS. HABITAT III Policy Paper 9 – Urban Services and Technology. 2016a. Disponível em: <http://habitat3.org/wp-content/uploads/Policy-Paper-9-English.pdf>. Acesso em: 02 abr. 2018.

UNITED NATIONS. New Urban Agenda. 2017. Disponível em: <http://habitat3.org/the-new-urban-agenda/documents/issue-papers/>. Acesso em: 2 abr. 2018.

UNITED NATIONS. World Urbanization Prospects: The 2018 Revision, Online Edition, 2018. Disponível em: <https://esa.un.org/unpd/wup/Publications/Files/WUP2018-KeyFacts.pdf>. Acesso em: 10 jul. 2018.

CAMINHABILIDADE NAS CIDADES BRASILEIRAS: MUITO ALÉM DAS CALÇADAS

RICKY RIBEIRO

MARCOS DE SOUSA

> *Caminhar é a primeira coisa que um bebê deseja fazer e a última coisa à qual uma pessoa deseja renunciar. Caminhar é um exercício que não necessita um ginásio. É uma medicação sem remédio, o controle de peso sem dieta e o cosmético que não se pode encontrar nas farmácias. É um tranquilizante sem drágeas, a terapia sem psicanalista e o lazer que não nos custa um centavo. De mais a mais, não contamina, consome poucos recursos naturais e é altamente eficiente. Caminhar é conveniente, não necessita equipamento especial, é autorregulável e intrinsecamente seguro. Caminhar é tão natural como respirar.*
>
> John Butcher, fundador da organização *Walk21*[1]

O QUE É CAMINHABILIDADE

Caminhabilidade – do inglês, *walkability* – é uma qualidade aplicável a espaços públicos, bairros e cidades inteiras e que define o quão convidativo esses lugares podem ser para circular a pé, ou de cadeiras de rodas, no caso de pessoas com deficiência. Ambientes construídos que promovam e facilitem o deslocamento a pé às lojas, trabalho, escola, hospitais, equipamentos e serviços são melhores lugares para viver, têm valores imobiliários mais altos, promovem estilos de vida mais saudáveis e alcançam níveis mais elevados de coesão social.

Por que caminhar? O especialista Roberto Ghidini reúne dez pontos que podem explicar e justificar o investimento público na infraestrutura para pedestres (GHIDINI, 2010):

1. somos todos pedestres em deslocamentos obrigatórios ou à passeio;
2. ruas com a presença de pessoas tornam-se mais seguras;
3. muitos são obrigados a caminhar, outros escolhem fazê-lo;

1 Cf.: WALK21. Disponível em: <http://www.walk21.com>. Acesso em: 18 ago. 2017.

4. é barato;
5. é bom para os negócios (comércio, turismo, etc.);
6. qualquer outro modo de deslocamento exige caminhar;
7. é bom para o meio ambiente;
8. pode reduzir a demanda de infraestruturas de transporte;
9. pode melhorar a saúde das pessoas;
10. melhora a qualidade de vida: independência, sociabilidade, etc.

Em geral, uma área de boa caminhabilidade oferece certas condições e características comuns: calçadas largas e em boas condições, bancos, boa iluminação, rotas fáceis, comércio interessante, prédios e serviços, e um tráfego de veículos de baixa agressividade, que ofereça segurança aos pedestres, especialmente crianças e pessoas com mobilidade reduzida. Também se pode incluir a limpeza urbana, a qualidade do ar que se respira ao caminhar, o nível de ruído da rua e o paisagismo e a arborização que proteja contra o excesso de calor.

Avaliar a caminhabilidade de uma rua, um bairro, ou de uma cidade é o primeiro passo para transformar esse ambiente. A ideia de medir a caminhabilidade de um lugar surgiu na cidade de Otawa, Canadá, em 1992, em função de um problema tributário. Após um forte aumento de impostos sobre os imóveis, os moradores de alguns bairros passaram a questionar a majoração, que consideravam desproporcional ao valor de mercado de suas propriedades. Alguns deles argumentavam que faziam quase todos os seus deslocamentos a pé e que, portanto, não se sentiam responsáveis por manter a infraestrutura das ruas para automóveis.

Nesse contexto, o empresário e ambientalista Chris Bradshaw (1993), que já se interessava pela ideia da mobilidade a pé, tomou a iniciativa de criar uma metodologia para avaliar a condição para caminhar, ou caminhabilidade, que poderia ser um bom argumento de negociação entre a comunidade e as autoridades. A metodologia permitiu a criação de um escore, uma classificação dos bairros e ruas em função do maior ou menor conforto para quem caminha, e considerou que essa pontuação poderia servir como balizador dos impostos municipais.

Mais tarde, depois da Conferência Eco 92, a ideia da mobilidade a pé se mostrou uma excelente alternativa aos veículos motorizados e suas emissões de carbono. Com melhores condições para caminhar as pessoas seriam encorajadas a deixar seus carros em casa para fazer trajetos de um a três quilômetros, com impactos positivos no trânsito, na poluição e no

ruído urbano. Assim, o conceito de caminhabilidade ganhou o mundo, o que explica o surgimento de modelos de avaliação ligeiramente diferentes, adaptados às condições de vários países e continentes.

No Brasil, segundo dados da Associação Nacional de Transportes Públicos (ANTP),[2] as viagens a pé são a modalidade mais praticada nas cidades e representam entre 36% e 50% dos deslocamentos diários. Apesar disso, as cidades brasileiras geralmente oferecem condições precárias e inseguras para as pessoas que caminham. Em função disso, nos últimos dez anos surgiram e multiplicaram-se as organizações que trabalham para difundir o conceito e medir a caminhabilidade dos centros urbanos brasileiros.

FATORES PARA A CAMINHABILIDADE

Uma rápida pesquisa na internet com a palavra *walkability* irá revelar várias iniciativas de medição da caminhabilidade, em vários momentos, países e cidades do mundo. Em sua pesquisa em 1992-93, em Otawa, Chris Bradshaw trabalhou com dez indicadores:

1. densidade de pessoas nas calçadas;
2. estacionamento permitido para veículos;
3. disponibilidade e quantidade de bancos e outros mobiliários para descanso;
4. idade que se pode deixar as crianças caminharem sozinhas pela rua;
5. como são as oportunidades para relações sociais (conhecer, conversar, etc.)
6. como as mulheres veem a segurança no bairro;
7. sensibilidade e facilidade de acesso aos serviços de trânsito local;
8. quantidades de locais importantes mencionados pelos moradores do bairro;
9. distância e capacidade dos locais de estacionamentos de veículos;
10. calçadas, como são e onde estão.

Alguns anos depois, outras organizações ampliaram a abordagem e incluíram mais fatores, como a declividade da via, iluminação, arborização, limpeza pública, nível de ruído, poluição do ar, sinalização dirigida a

2 ANTP. Sistema de Informações da Mobilidade Urbana, Relatório 2014. Disponível em: <http://files.antp.org.br/2016/9/3/sistemasinformacao-mobilidade--geral_2014.pdf>. Acesso em: 18 ago. 2017.

pedestres, tempo de abertura dos semáforos para pedestres, acessibilidade das calçadas – incluindo rampas para cadeirantes – conectividade das rotas caminháveis, atratividade das ruas e calçadas e a facilidade de travessia das ruas, entre outros pontos.

CALÇADAS E PEDRAS NO CAMINHO

Um ponto básico e óbvio é a qualidade das calçadas, que precisam ser niveladas e ter largura adequada para a passagem de pessoas e cadeiras de rodas. Não podem ter degraus, nem rampas de veículos que dificultem o caminhar, assim como outros obstáculos, tal como excesso de postes, árvores mal posicionadas, bancas de jornais, lixeiras etc.

Além disso, precisam ser dotadas de rampas de acessibilidade, em todas as esquinas, não apenas para atender as pessoas com mobilidade reduzida, mas também para facilitar a circulação de carrinhos com crianças, malas com rodinhas, carrinhos de entregas e outros utensílios leves com rodas.

Em 2012/2013 o Mobilize Brasil[3] realizou a campanha Calçadas do Brasil,[4] com uma avaliação dessa infraestrutura em 39 cidades do país. A nota média dos 228 locais avaliados ficou em 3,40, número muito baixo se considerarmos que a nota mínima para uma calçada de qualidade aceitável seria 8, segundo os critérios estabelecidos pela equipe da campanha. Apenas 2,19% dos locais avaliados obtiveram nota acima desse indicador mínimo. E 74,13% das localidades avaliadas obtiveram médias abaixo de 5, numa escala de zero a dez.

SEMÁFOROS, FAIXAS E MAPAS DE ORIENTAÇÃO

Outro aspecto fundamental é a existência – e qualidade – da sinalização voltada a pedestres, incluindo faixas de travessia, semáforos e totens ou painéis com mapas de localização e orientação. Em 2014, o Mobilize rea-

3 Cf.: MOBILIZE BRAZIL. Disponível em: <http://www.mobilize.org.br/>.

4 A Campanha Calçadas do Brasil foi uma iniciativa realizada em 2012 pelo portal Mobilize Brasil para estimular a melhoria das condições de mobilidade para pedestres nas cidades do país. O objetivo era chamar a atenção da opinião pública para o problema da má qualidade, falta de manutenção ou ausência de calçadas nas cidades do país. Uma metodologia de avaliação com oito critérios foi aplicada inicialmente a 13 capitais e, posteriormente, a outras 26 cidades brasileiras. MOBILIZE BRASIL. Relatório final da Campanha Calçadas do Brasil (2013). Disponível em: <http://www.mobilize.org.br/midias/pesquisas/relatorio-calcadas-do-brasil---jan-2013.pdf>. Acesso em: 11 mar. 2017.

lizou a campanha Sinalize!,[5] que procurou observar a sinalização urbana para usuários do transporte público, ciclistas e pedestres. Os resultados revelaram que os sinais de trânsito são, sobretudo (90%), voltados aos motoristas. A nota média da sinalização específica para pedestres nas 14 capitais avaliadas ficou em 3, também numa escala de zero a dez.

POLUIÇÃO E RUÍDO URBANO

Durante os levantamentos de campo realizados para as campanhas Calçadas do Brasil e Sinalize!, foi possível observar a forte interferência de outros dois fatores: ruído e poluição. O excesso de ruído das áreas urbanas do Brasil já foi registrado em vários trabalhos acadêmicos (MOURA, 2002), com medições de 85 dB e até 89 dB em algumas avenidas de cidades como São Paulo, Rio de Janeiro e Curitiba, quando o limite admissível para a saúde humana se situa em 65 dB durante o dia, segundo a Organização Mundial da Saúde.

Ainda em relação às condições ambientais, a poluição do ar é outro fator grave, que afeta a saúde e afasta as pessoas do convívio com a cidade. Dados da Faculdade de Medicina da USP, citados pelo professor Paulo Saldiva em entrevista ao Mobilize,[6] indicam a morte de 4 mil pessoas por ano em função do ar poluído apenas na cidade de São Paulo e de 7 mil pessoas/ano na Região Metropolitana da capital paulista. São condicionantes por vezes intangíveis para as pessoas, mas também interferem, mesmo que de modo inconsciente, na decisão entre deslocar-se a pé ou usar um modo motorizado.

Conectividade e continuidade de rotas caminháveis são também dois fatores citados em alguns estudos sobre o tema, como a metodologia do FitCities, representada no Brasil pela organização Cidade Ativa.[7] O conceito

---

5 A Campanha Sinalize! foi realizada em 2014 pelo portal Mobilize Brasil para avaliar a existência e qualidade da sinalização dirigida a pessoas que caminham, andam de bicicleta ou usam o transporte público. Com base nas boas práticas conhecidas no Brasil e em outros países, fez-se um formulário para avaliar essa sinalização. Cf.: MOBILIZE BRAZIL. Voluntários de todo o Brasil participaram da campanha. Disponível em: <http://www.mobilize.org.br/estudos/190/campanha-sinalize--relatorio-final-referente-a-2014.html>. Acesso em: 18 ago. 2017.

6 Cf.: SALDIVA, P. H. N *et al*. *Avaliação do impacto da poluição atmosférica no estado de São Paulo sob a visão da saúde*. São Paulo: Instituto Clima e Sociedade, 2013. Disponível em: <http://www.saudeesustentabilidade.org.br/site/wp-content/uploads/2013/09/Documentofinaldapesquisapadrao_2409-FINAL-sitev1.pdf> Acesso em: 18 ago. 2017

7 Cf.: CIDADE ATIVA. Disponível em: <https://www.cidadeativa.org.br>.

considera que caminhos desimpedidos, sem travessias difíceis, com rotas claras e facilmente compreensíveis, conectadas a terminais de transportes estimulam as pessoas a empreender seus deslocamentos a pé.

No entanto, como sabemos, é mais interessante caminhar pelas ruas tortuosas e íngremes de cidades históricas, como Ouro Preto ou Salvador, do que seguir a pé as rotas retilíneas, mas com forte tráfego de veículos, de uma cidade planejada, como Brasília. Aqui ingressamos em um aspecto quase subjetivo, que é a atratividade que um local pode exercer sobre as pessoas. Fachadas bonitas e acolhedoras, lojas, bares, bancas de revistas e de vendedores ambulantes – desde que não atrapalhem a passagem –, pequenas praças e jardins podem compor ambientes convidativos ao pedestre, que assim faz sua viagem como um passeio cotidiano. Arborização e paisagismo são também dois componentes sempre citados em pesquisas de conforto para o pedestre, especialmente em cidades de clima solar e quente, como são a maioria delas no Brasil.

FATOR HUMANO, PRESENÇA DE ANIMAIS E SEGURANÇA PÚBLICA

Os tipos de pessoas que frequentam um local também podem influenciar a percepção do pedestre, seja por prazer ou pelo medo. Por exemplo, crianças tendem mais a caminhar por locais onde possam encontrar outras crianças. Também há pessoas que preferem caminhar em lugares da moda, ruas com bares e casas noturnas, ou vias com grande concentração de jovens, de forma que diferentes formas de socialização têm que ser levadas em conta quando se pensa em ambientes caminháveis.

Uma rua pode ser mais ou menos agradável também pela presença de animais: cães bravos e com latido ruidoso, mesmo que dentro dos lotes, podem gerar medo e inibir os pedestres.

Um ponto fundamental para o caminhante é a segurança pública, especialmente para mulheres, crianças e idosos. Esse fator aparece em todos os estudos, mesmo em países com índices de criminalidade bem abaixo dos constatados no Brasil. Qualidade da iluminação, existência de postos policiais, presença de outras pessoas nas ruas e fachadas comerciais abertas, inclusive à noite, são fatores de segurança citados em vários trabalhos.

BREVE HISTÓRICO DE MOBILIDADE URBANA

Até meados do século XIX os deslocamentos nas cidades eram realizados a pé, a cavalo ou sobre veículos de tração animal. No final do século, po-

rém, com o rápido crescimento urbano, o problema da poluição causada pelos cavalos chegou a um nível insuportável em várias cidades do mundo – como Nova York, por exemplo –, que estavam repletas de estrume, moscas, carcaças de animais, congestionamentos e acidentes de tráfego, além da crueldade generalizada contra os cavalos.

O problema, de fato, não era novo. Muito antes, na Roma antiga, o imperador Júlio César proibira as carroças puxadas por cavalos de circular pela cidade durante o dia. Tudo para reduzir engarrafamentos, barulho, acidentes e outros subprodutos desagradáveis do equino urbano. No mesmo período, nos séculos VI e VII AC, surgiram em Pompéia as primeiras calçadas de que se tem conhecimento, justamente para proteger os pedestres dos acidentes com carros de carga. Não há registros sobre o número de acidentes na Antiguidade, mas os dados de Nova York de 1900 indicavam exatas 200 pessoas mortas em atropelamentos e outros acidentes (MORRIS, 2007).

BONDES, BIKES, CARROS E A FAIXA DE PEDESTRES

No final do século XIX, a invenção dos bondes elétricos atraiu cada vez mais passageiros, iniciando um processo de eliminação gradativa da tração animal nas cidades. Contudo, nesse momento o veículo mais ágil e veloz, a novidade da época, ainda era a bicicleta, que conquistou as ruas do mundo.

Nesse período, o nova-iorquino William Phelps Eno criou as primeiras regras de trânsito para reduzir o número de acidentes entre automóveis e veículos de tração animal: nascia o sinal de *stop* – avô do semáforo –, a rua de mão única, e o código de condução dos veículos pelo lado direito das pistas. Surgem também a ilha central nas ruas mais largas, e a faixa de passagem de pedestres. Por volta de 1890 o mundo foi invadido pelos novíssimos carros motorizados, que seduziam pela velocidade e possibilidade de viagens ponto a ponto. Em 1912 os Estados Unidos já tinham mais de 356 mil automóveis e, pela primeira vez, as contagens de tráfego de Nova York, Londres e Paris registraram mais carros do que cavalos. As coisas realmente complicaram em 1908, quando Henry Ford lançou o famoso Modelo T, um carro robusto, confiável, fácil de consertar e, acima de tudo, barato. Resultado: mais de 15 milhões de unidades vendidas até 1927, quando o T saiu de linha.

Com a produção massiva dos carros, as cidades passaram a experimentar grandes congestionamentos, que pediam mais espaço para a circulação dos novos veículos motorizados. Grandes obras viárias são realizadas, praças e calçadas são reduzidas ou desaparecem, e qualquer espaço se torna local para circulação ou estacionamento de automóveis. No entanto, mesmo

com as novas pistas, viadutos, túneis e pontes, os congestionamentos retornavam após algum tempo. O livro *Suburban Nation: The Rise of Sprawl and the Decline of the American Dream*, localiza essa constatação em 1942, quando "o engenheiro e urbanista Robert Moses percebeu que as vias que ele construíra em Nova York, em 1939, estavam de alguma forma gerando maiores problemas de trânsito do que os que existiam anteriormente" (DUANY; PLATER-ZYBERK; SPECK, 2010).

MOSES × JACOBS

Moses, porém, não se rendeu e continuou a desenvolver uma série de obras que transformaram o tecido urbano da metrópole americana. Nos anos 1960, quando trabalhava para a construção de uma via elevada no Greenwich Village, o engenheiro enfrentou a oposição feroz de moradores liderados pela ativista Jane Jacobs, que desenvolveu uma campanha contra a obra e conseguiu barrá-la no final daquela década. Jane defendia um modo de vida baseado na convivência, em passeios a pé e de bicicleta, que ela compartilhava com seus vizinhos no Village, entre eles nomes como Bob Dylan, Norman Mailer e Elizabeth Roosevelt, viúva do ex-presidente Franklin Roosevelt. Jane Jacobs se tornou uma referência mundial na defesa de cidades caminháveis, para a convivência humana, especialmente após o lançamento de seu livro *Morte e Vida das Grandes Cidades* (1961). Quando ela faleceu, em 2006, ativistas de vários países passaram a organizar as ações Jane's Walk,[8] que são caminhadas urbanas em defesa dos direitos de pedestres.

O RESGATE DO ANDAR A PÉ

No final do século XX, com o agravamento dos problemas urbanos e ambientais gerados pelo uso intensivo do automóvel, a caminhada voltou a ser vista como uma forma simples, econômica, natural e eficiente de deslocamento urbano. Organizações que trabalham pela mobilidade a pé espalham-se por todos os continentes e defendem a restauração e melhoramento da infraestrutura urbana para que as pessoas possam voltar a caminhar, sejam elas crianças, jovens, adultos, idosos ou pessoas com deficiência.

Em 2016, as organizações Cidade Ativa e Corrida Amiga desenvolveram a pesquisa Como Anda,[9] com o objetivo de identificar os grupos brasileiros

8 Cf.: JANE'S WALK. Disponível em: <http://janeswalk.org/>. Acesso em: 6 abr. 2017.

9 Ver: Como anda, quem promove a mobilidade a pé no Brasil. Cf.: COMO ANDA. Disponível em: <http://comoanda.org.br/>. Acesso em: 13 abr. 2017.

que defendem a mobilidade a pé. O resultado mostrou a existência de 137 instituições ativistas em praticamente todo o Brasil.

Hoje a demanda pela melhoria das calçadas, da sinalização e da segurança para pedestres é uma pauta comum em todas as comunidades do Brasil, especialmente após a vigência da Lei 12.587/2012,[10] que define a Política Nacional de Mobilidade Urbana, e da Lei 13.146/2015,[11] a Lei Brasileira de Inclusão. Ambos os textos legais obrigam os gestores públicos a desenvolverem políticas que priorizem a acessibilidade e a caminhabilidade nas cidades do país. No entanto, há ainda um longo caminho para que as duas legislações saiam do papel e cheguem às ruas.

BENEFÍCIOS DO CAMINHAR

Caminhar aglutina mobilidade, exercício e lazer em uma única atividade. De acordo com o Dr. Beny Schmidt,[12] patologista neuromuscular, "Caminhar é a opção mais certeira para todos aqueles que procuram uma vida saudável e plena", já que contribui para a prevenção de doenças cardíacas, derrames, osteoporose e diabetes. Melhora a circulação sanguínea, os ossos, o funcionamento do cérebro e dos pulmões. Ainda provoca uma maior sensação de bem-estar, combatendo o estresse e a depressão. Caminhar melhora o condicionamento físico, tonifica os músculos das pernas e do abdome, ajuda no controle do peso e retarda o envelhecimento. Além disso, é barato, não necessita de equipamento especial ou habilidade específica. Assim como a saúde individual, a saúde pública também ganha quando as condições de caminhabilidade são favoráveis. Maior segurança viária significa menos acidentes, menor ocupação de leitos nos hospitais e redução do gasto de dinheiro público. Da mesma forma, quando a população adota hábitos mais saudáveis para se deslocar, a prevenção de doenças se fortalece, gerando uma economia aos cofres públicos.

Além da redução nos gastos com saúde, a administração pública local se beneficia pela menor necessidade de infraestrutura para veículos motorizados e para o transporte coletivo. Com a diminuição do espaço reservado a

10 Cf.: MOBILIZE BRASIL. Lei nº 12.587, de 3 de janeiro de 2012. Disponível em: <http://www.mobilize.org.br/estudos/22/politica-nacional-de-mobilidade-urbana.html>.

11 Cf.: BRASIL. Lei nº 13.146, de 6 de julho de 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13146.htm>. Acesso em: 10 dez. 2018.

12 Ver: <http://www.tribunadabahia.com.br/2015/08/19/especialista-fala-quais-sao-os-beneficios-da-caminhada>.

ruas e estacionamentos, o uso do solo se torna mais eficiente, uma vez que o espaço[13] necessário para circular, estacionar, vender e manter veículos nas grandes cidades gira em torno de 50% do espaço urbano. Governos que investem em melhores condições para os pedestres promovem a equidade e uma alocação mais justa de recursos públicos para os habitantes não motorizados. Lugares com boa estrutura para caminhar e com grande fluxo de pedestres, em diferentes horários, também são mais seguros.

O meio ambiente se beneficia com o aumento na proporção de pedestres, uma vez que há diminuição na poluição atmosférica, no nível de ruído e no consumo de recursos naturais. A presença de árvores também ainda contribui para evitar as "ilhas de calor" e proporcionar maior conforto climático.

Estudos de diferentes países mostram que ambientes propícios aos pedestres são bons para os negócios. Resultados de um levantamento realizado em Washington, nos EUA, indicam que lugares urbanos com elevada caminhabilidade possuem economias mais ativas, maior renda e valorização dos imóveis (BROOKINGS INSTITUTION, 2012). Além disso, são atrativos para o turismo e tornam bairros e cidades mais competitivos (CENTRAL LONDON PARTNERSHIP, 2003). Como exemplo, uma ação voltada para os pedestres em uma rua do Brooklyn, Nova York, provocou um aumento de 172% nas vendas do varejo (NYCDOT, 2012). Em São Paulo, ciente da importância da caminhabilidade para o comércio local, a Associação de Lojistas da Oscar Freire teve a iniciativa de levar adiante um projeto de requalificação da rua em parceria com a prefeitura. Assim, em 2006, as calçadas foram reformadas e alargadas, guias foram rebaixadas para melhorar a acessibilidade, e o local recebeu novo mobiliário urbano, aterramento da fiação elétrica e plantio de árvores, entre outras ações (Soluções para Cidades, 2013).[14]

Ao caminhar, o pedestre se apropria dos espaços públicos, observa com mais atenção os problemas do bairro e desenvolve maior senso de comunidade, o que contribui para a conservação dos espaços urbanos e para o exercício pleno da cidadania. Segundo Appleyard (1981), moradores de vias com maiores volumes de tráfego e velocidade tendem a conhecer menos seus vizinhos e demonstrar menor preocupação com o ambiente local do que as pessoas que vivem em ruas tranquilas, onde a convivência é mais intensa.

13 Comissão de Circulação e Urbanismo da Associação Nacional de Transportes Públicos (ANTP).

14 SOLUÇÕES PARA CIDADES (2013). Requalificação de ruas comerciais: a parceria entre a Associação de Lojistas e a Prefeitura Municipal no projeto da Rua Oscar Freire. São Paulo. Disponível em: <http://www.solucoesparacidades.com.br/wp-content/uploads/2013/08/AF_07_SP_REURBANIZACAO%20OSCAR%20FREIRE_Web.pdf>. Acesso em: 18 ago. 2017

COMO MEDIR

Há inúmeras possibilidades e formas de se medir o nível de caminhabilidade de determinada rua ou região, dependendo de diferentes aspectos e também de qual a abordagem desejada pela pessoa ou grupo que elabora a avaliação. Existem índices desenvolvidos por governos, universidades, escolas, instituições relacionadas à saúde e meio ambiente, associações comunitárias, grupos imobiliários, empresas e uma grande variedade de organizações. Cada um define a quantidade de indicadores, se eles serão agrupados por temas, e também o sistema de pontuação. Diferentes pesos podem ser atribuídos aos vários indicadores para valorizar mais algumas questões em detrimento de outras.

A avaliação pode ser realizada por meio de pesquisas em campo, mapas, fotos de satélites, e de informações obtidas com órgãos públicos ou com concessionárias de serviços. Para isso, é fundamental que haja disponibilidade de dados com qualidade e confiabilidade por parte dos governos. Também é possível usar instrumentos específicos para medir nível de ruído, qualidade do ar, luminosidade e outros fatores ambientais. Nos últimos cinco anos essas metodologias foram gradativamente incorporadas a plataformas digitais colaborativas, integradas a aplicativos para smartphones. Assim, ao menos nas cidades-alvo dessas iniciativas, qualquer pessoa pode rapidamente aferir o nível de caminhabilidade de um bairro, de uma rua, e também registrar as suas próprias avaliações sobre os locais percorridos.

Uma das ferramentas de caminhabilidade mais conhecidas do mundo é o Walk Score.[15] Voltado para o mercado imobiliário, o índice pontua endereços, em escala de 0 a 100, de acordo com a oferta de serviços – mercados, bancos, escolas, restaurantes, parques, empresas, teatros etc. – a uma distância possível de ser percorrida a pé. Embora calcule notas para localidades no mundo inteiro, a ferramenta informa que só há suporte em alguns países, como Estados Unidos, Canadá e Austrália, onde eles garantem a precisão das informações. A maior crítica em relação ao Walk Score se dá pelo fato de que ele desconsidera alguns fatores, como a existência de calçadas, arborização, limpeza e segurança.

Ainda nos países de língua inglesa, destaca-se o Walkonomics,[16] aplicativo colaborativo que promete uma ajuda ao pedestre para encontrar caminhos

15 Cf.: WALK SCORE. Disponível em: <http://www.walkscore.com>. Acesso em: 3 abr. 2017.

16 WALKONOMICS. Disponível em: <www.walkonomics.com>. Acesso em: 10 dez. 2018.

mais agradáveis e menos estressantes. A limitação é que a ferramenta funciona em poucas cidades, nenhuma delas no Brasil.

Uma alternativa é o Walkability Asia,[17] ferramenta que trabalha com dados de 23 cidades asiáticas, incluindo a região da Índia. Trata-se de um app simples, intuitivo, que pede ao usuário opiniões sobre as condições dos passeios, velocidade do tráfego, acessibilidade, relações entre pedestres e motoristas, e segurança pessoal para o caminhante. Ao final, gera uma nota. Outros exemplos interessantes são os *apps* Walk & the City, Walkability Mobile App e a plataforma Rate my Street.

As características do local avaliado e a abrangência almejada também influenciam na avaliação. Alguns índices pretendem ser globais e necessitam de indicadores universais, passíveis de medição em qualquer localidade. Outros são desenvolvidos de forma customizada, considerando as peculiaridades da região analisada. Esses últimos não podem ser aplicados em outro local sem uma prévia adaptação.

O Banco Mundial também desenvolveu sua própria avaliação, o Global Walkability Index.[18] Baseado em diferentes indicadores, separados em três grupos, o índice ainda avalia políticas públicas e iniciativas governamentais voltadas para a infraestrutura voltada ao pedestre.

No Brasil, foi desenvolvida uma ferramenta para avaliar a caminhabilidade das vias do Rio de Janeiro. Contando com 21 indicadores, agrupados em seis categorias – Calçada, Mobilidade, Atração, Segurança pública, Segurança viária e Ambiente –, o índice é fruto de uma parceria entre o Instituto de Políticas de Transporte e Desenvolvimento (ITDP Brasil) e o Instituto Rio Patrimônio da Humanidade (IRPH), órgão da Prefeitura do Rio de Janeiro.

BOAS PRÁTICAS

CIDADES CAMINHÁVEIS

Nova York é o exemplo mundial mais conhecido de transformações urbanas para estimular a mobilidade ativa e a ocupação de ruas e calçadas pelas pessoas. As alterações mais profundas ocorreram na gestão do

17 WALKABILITY. Disponível em: <https://walkabilityasia.org>. Acesso em: 10 dez. 2018.

18 Ver: THE WORLD BANK GROUP. <https://openknowledge.worldbank.org/bitstream/handle/10986/17421/449040NWPBox321IC10tp1181walk1urban.pdf?sequence=1&isAllowed=y>. Disponível em: 10 dez. 2018.

prefeito Michael Bloomberg, entre 2002 e 2013, principalmente a partir de 2007, com a advogada Janette Sadik-Khan à frente do Departamento de Transportes (NYCDOT). Nesse período, ela desenvolveu uma política extensiva de redução dos espaços para automóveis na área mais central da cidade, com o fechamento de algumas áreas aos veículos, a transformação de antigos locais de estacionamentos em praças, ampliação das faixas de travessias de ruas, redução da velocidade do tráfego em algumas vias e a criação de ciclofaixas, e corredores de ônibus. Nos dois últimos anos de sua gestão, Bloomberg deu início à política Vision Zero,[19] ação que teve continuidade no governo De Blasio e que busca zerar as mortes no trânsito nova-iorquino. Bem antes, ainda nos anos 1970, um funcionário do NYCDOT, Sam Schwartz, já havia tentado reduzir as velocidades da cidade, implantar ciclovias e faixas de ônibus, mas foi barrado por uma forte oposição da sociedade. O momento ainda não havia chegado, porém já se sentia a necessidade de mudanças.

REDUÇÃO DO TRÁFEGO E ZONAS 30 KM/H

Em nível mundial, uma das primeiras cidades a desenvolver uma ação permanente de redução do tráfego e estímulo à mobilidade ativa foi a pequena Buxtehude, na Alemanha, em 1983. Por volta de 1997, Copenhague destacou-se na Europa como a primeira capital a reservar suas áreas centrais apenas para pedestres e criar o primeiro sistema funcional de bicicletas públicas, o Gobike. Depois vieram Paris, Londres, Antuérpia, Bruxelas, Barcelona, Madri, Berlim, Viena, Praga, Módena, Milão e várias outras cidades europeias, algumas das quais criaram a "Iniciativa de Cidadania Europeia 30 km/h, dando vida às ruas", uma ação para ampliar as áreas de tráfego calmo, que permitam a circulação segura das pessoas a pé.

O modelo expandiu-se pelo mundo em cidades como Guangzhou – China –, Melbourne – Austrália –, Seul – Coreia –, e também em cidades de toda a América Latina, como Buenos Aires, Lima, Cidade do México, Medellín, Bogotá e cidades de menor porte. Hoje já existem mais de três mil ações de "pedestreanização" de cidades em todo o mundo, segundo dados da organização Urbi-i.[20] O mesmo levantamento computou 152 intervenções em cidades brasileiras, entre elas várias capitais, mas quase sempre iniciativas pontuais, com caráter experimental. Assim, apesar da

19 VISION ZERO. Disponível em: <http://www1.nyc.gov/site/visionzero/index.page>. Acesso em: 18 abr. 2017.

20 Ver: URBI-I, Before-After Gallery. Disponível em: <http://www.urb-i.com/before-after-gallery>. Acesso em: 12 abr. 2017.

Lei de Mobilidade Urbana e da Lei Brasileira de Inclusão, no Brasil não há ainda políticas municipais que realmente consolidem a prioridade total aos pedestres como norma reconhecida por todos.

AÇÕES DE EDUCAÇÃO

Embora a importância do pedestre já estivesse reconhecida por lei e fosse alvo de discussões e campanhas nacionais, como a Campanha Calçadas do Brasil, do Mobilize Brasil, um dos marcos mais importantes das ações pela caminhabilidade urbana foi o Seminário Internacional Cidades a Pé, realizado pela ANTP em 2015 na cidade de São Paulo, com a participação de especialistas da Espanha, México, Estados Unidos, Colômbia e Reino Unido, além de ativistas e pesquisadores de todo o Brasil. O encontro teve também algumas ações concretas, com intervenções urbanas de baixo custo, para mostrar que com poucos investimentos é possível melhorar a condição do pedestre.

Em outra frente, nas escolas, alguns ativistas têm procurado estimular crianças e pais a experimentarem a caminhada como forma de deslocamento para as aulas. Em São Paulo, em um colégio de classe média, surgiu o projeto Carona a Pé,[21] uma ação que organiza os alunos em pequenos grupos para ir e voltar da escola. Objetivo similar tem a ação internacional PediBus, que se autodefine como "um enxame de crianças que vão à escola acompanhados por um adulto"[22] e que já tem seções em vários países da Europa e Américas. Exemplar também é o Walk Day to School, organizado todos os anos em Los Angeles (EUA), para reafirmar o direito das crianças de circular pelas calçadas em segurança para assistir às aulas. Parece óbvio, mas cerca de 50% dos alunos das escolas privadas brasileiras vão à escola de carro, provocando grandes – e deseducativos – congestionamentos diários nos portões das instituições de ensino.

A PÉ PARA O TRABALHO

Segundo o Manual de Mobilidade Corporativa do WRI/Cebeds,[23] cerca de 50% dos deslocamentos urbanos ocorrem para que as pessoas possam simplesmente ir e voltar do trabalho. Junto com outras organizações, o

21 Ver: CARONA A PÉ. Disponível em: <http://caronaape.com.br>. Acesso em: 17 abr. 2017.

22 Cf.: PEDIBUs. PEDIBUS, A pé para a escola, acompanhado. Disponível em: <http://www.pedibus.ch/medias/documents/Traduction-depliants/PEDIBUS-DEPLIANT_PT_WEB.pdf>. Acesso em: 13 abr. 2017.

23 Ver: WRI BRASIL. Passo a passo para a construção de um Plano de Mobilidade Corporativa. Disponível em: <http://www.wrirosscities.org>. Acesso em: 18 ago. 2017.

Cebeds tem realizado um esforço contínuo para estimular as boas práticas de mobilidade, como a carona, o uso do transporte público e da bicicleta. Entretanto, mesmo entre as empresas mais avançadas ainda são raras as que oferecem espaços para banhos ou troca de roupas para os funcionários que caminham – ou pedalam – para ir ao trabalho.

MERCADO IMOBILIÁRIO

Na área imobiliária, a novidade é o lançamento de uma série de empreendimentos residenciais localizados no Centro de São Paulo e que oferecem como principal vantagem a facilidade de acesso, sem carro, a centros comerciais, locais de diversão, hospitais, escolas e outros serviços. Para viabilizá-los os empreendedores começam a discutir estratégias para melhorar as condições de caminhabilidade em seu entorno, incluindo a reforma de calçadas, segurança e iluminação, além do mapeamento das rotas mais adequadas para pedestres. Timidamente o setor imobiliário começa a afastar-se do automóvel como seu principal vetor de expansão.

CONCLUSÃO: A PROMESSA DE UMA NOVA CIDADE

Mais de 60% da população do planeta vivem hoje em aglomerados urbanos. No Brasil, essa concentração é ainda maior e prenuncia o que ocorrerá no mundo nos próximos 30 anos: segundo dados do IBGE (2010), o país tem mais de 170 milhões de pessoas – 85% da população – nas cidades, numa área de 22 mil km^2, o que resulta uma densidade de 7.700 hab/km^2, equivalente a 1/3 da densidade de uma cidade como Paris, ou 1/4 da densidade de Manhattan, a área mais central de Nova York.

O processo de urbanização brasileiro ocorreu em apenas cinco décadas, impulsionado principalmente pela construção de infraestruturas para o automóvel. Acreditava-se que a oferta de automóveis e de linhas de ônibus permitiriam que as pessoas pudessem residir cada vez mais longe de seus locais de trabalho. Essa opção, porém, se mostrou inviável já a partir dos anos 1970, com o aumento progressivo dos engarrafamentos de trânsito. À medida em que a frota de veículos crescia e demandava mais espaço, calçadas e outros espaços destinados a pedestres foram reduzidos ou simplesmente suprimidos. Essa combinação de fatores levou ao progressivo aumento da utilização do automóvel nas cidades, mesmo para deslocamentos menores do que 1 km, gerando um círculo vicioso que afastou os pedestres das ruas.

No entanto, a partir dos anos 2000, ruas e praças das grandes cidades passam a ser ocupadas por organizações de jovens ativistas, entre eles vá-

rios pesquisadores universitários, que buscam a ideia de uma cidade com menos veículos motorizados e mais espaço para a mobilidade ativa, a pé e de bicicleta, cidades para pessoas. Essa articulação da sociedade – hoje respaldada no Brasil por vários instrumentos legais – ainda esbarra em certo conservadorismo de gestores públicos, que resistem em avançar nessas políticas públicas.

Apesar disso, alguns exemplos concretos de sucesso em cidades brasileiras e estrangeiras têm impulsionado a desejada transformação dos espaços públicos, como revela, por exemplo, o projeto de remodelação da área portuária do Rio de Janeiro, em 2016, que devolveu ao pedestre uma extensa área antes ocupada por uma via elevada, a Perimetral, parcialmente demolida e substituída por um túnel.

O exemplo carioca mostra que cabe ao poder público o papel de induzir essa reforma das cidades: assumir a responsabilidade de construção e conservação de sistemas de circulação voltados a pedestres, a começar pela renovação e alargamento de calçadas nos principais eixos de circulação de cada cidade, não necessariamente coincidindo com o sistema viário destinado aos veículos. Esses novos eixos – integrados aos demais modos de transporte – poderão reunir as habitações, escolas, locais de compras, centros culturais e esportivos, enfim os serviços que fazem a vida de qualquer polo urbano.

Para concluir, imaginemos as avenidas marginais dos rios Tietê, Pinheiros e Tamanduateí, em São Paulo, convertidas em grandes passeios públicos, repletos de restaurantes, bares, praças e parques, com deques de acesso às águas – despoluídas –, que por sua vez transportarão barcas de passageiros e cargas. Para a circulação mais rápida nesses eixos, imaginemos uma linha de metrô ou de um veículo leve sobre trilhos, ciclovias e dezenas de estações de bicicletas compartilhadas, e pessoas, milhares delas, de todas as idades, origens e classes sociais, circulando e convivendo nessa nova cidade. Será só um sonho?

REFERÊNCIAS

APPLEYARD, Donald (1981). *Livable Streets*. Berkeley: University of California Press, [s.d].

BRADSHAW, Chris (1993). Creating – and Using – a Rating System for Feighbourhood Walkability: (2) Towards an Agenda for "Local Heroes". Ottawa, Canada. [presented to the 14th International Pedestrian Conference, Boulder CO]

BRASIL. Lei nº 13.146, de 6 de julho de 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13146.htm>. Acesso em: 10 dez. 2018.

CARONA A PÉ. Disponível em: <http://caronaape.com.br>. Acesso em: 17 abr. 2017.

CENTRAL LONDON PARTNERSHIP (2003). Economic Benefits of Good Walking Environments. Consultant: Llewelyn-Davies. Disponível em: <www.livingtransport.com/library/pdf.php?id=185>. Acesso em: 18 abr. 2017.

CIDADE ATIVA. Disponível em: <https://www.cidadeativa.org.br>. Acesso em: 10 dez. 2018.

DUANY, Andres; PLATER-ZYBERK, Elizabeth; SPECK, Jeff. *Suburban Nation*: The Rise of Sprawl and the Decline of the American Dream. Nova York: North Point Press, 2010.

GHIDINI, Roberto (2010). A caminhabilidade, medida urbana mensurável. Disponível em: <http://www.mobilize.org.br/midias/pesquisas/a-caminhabilidade-medida-urbana-sustentavel.pdf>. Acesso em: 3 abr. 2017.

ITDP BRASIL. Índice de Caminhabilidade – Ferramenta. Disponível em: <http://itdpbrasil.org.br/indice-de-caminhabilidade-ferramenta/>. Acesso em: 13 abr. 2017.

JACOBS, Jane. *Morte e vida de grandes cidades*. São Paulo: WMF; Martins Fontes, 2011.

LEINBERGER, Christopher B.; ALFONZO, Mariela. Walk this Way: The Economic Promise of Walkable Places in Metropolitan Washington, D. C. Disponível em: <https://www.brookings.edu/wp-content/uploads/2016/06/25-walkable-places-leinberger.pdf>. Acesso em: 18 abr. 2017.

MOBILIZE BRASIL. Guia de Mobilidade Corporativa EY/MobilizeBrasil. Disponível em: <http://www.mobilize.org.br/midias/pesquisas/guia-de-mobilidade-corporativa-ey---mobilize-brasi.pdf>. Acesso em: 13 abr. 2017.

MOBILIZE BRASIL. Paulo Saldiva: bicicleta, para curar as cidades doentes, 2011. Disponível em: <http://www.mobilize.org.br/noticias/543/bicicleta-para-curar-as-cidades-doentes.html>. Acesso em: 12 abr. 2017.

MOBILIZE BRASIL. Relatório final da Campanha Calçadas do Brasil (2013). Disponível em: <http://www.mobilize.org.br/midias/pesquisas/relatorio-calcadas-do-brasil---jan-2013.pdf>. Acesso em: 11 mar. 2017.

MOBILIZE BRASIL. Relatório final da Campanha Sinalize! (2014). Disponível em: <http://www.mobilize.org.br/estudos/190/campanha-sinalize--relatorio-final-referente-a-2014.html>. Acesso em: 11 mar. 2017.

MOBILIZE BRASIL. Em 1970, Nova York já tentava proibir carros. Sem sucesso. Disponível em: <http://www.mobilize.org.br/noticias/9597/em-1970-nova-york-ja-tentava-proibir-carros-sem-sucesso-.html>. Acesso em: 13 abr. 2017.

MOBILIZE BRASIL. Lei nº 12.587, de 3 de janeiro de 2012. Disponível em: <http://www.mobilize.org.br/estudos/22/politica-nacional-de-mobilidade-urbana.html>. Acesso em: 10 dez. 2018.

MONTGOMERY, Brittany; ROBERTS, Peter. Demand, Constraints and Measurement of the Urban Pedestrian Environment. Washington, 2008. Disponível em: <https://openknowledge.worldbank.org/bitstream/handle/10986/17421/449040NWPBox321IC-10tp1181walk1urban.pdf?sequence=1&isAllowed=y>. Acesso em: 18 ago. 2017.

MORRIS, Eric. From Horse Power to Horsepower, 2007 Disponível em: <http://www.uctc.net/access/30/Access%2030%20-%2002%20-%20Horse%20Power.pdf>. Acesso em: 5 abr. 2017.

MOURA DE SOUZA, Carolina. *Ruído urbano*: níveis de pressão sonora na cidade de São Paulo. São Paulo: Faculdade de Saúde Pública da USP, 2002.

NYCDOT (2012). Measuring the Street: New Metrics for 21st Century Streets. Disponível em: <http://www.nyc.gov/html/dot/downloads/pdf/2012-10-measuring-the-street.pdf>. Acesso em: 18 abr. 2012.

PEDIBUS. PEDIBUS, A pé para a escola, acompanhado. Disponível em: <http://www.pedibus.ch/medias/documents/Traduction-depliants/PEDIBUS-DEPLIANT_PT_WEB.pdf>. Acesso em: 13 abr. 2017.

ORGANIZAÇÃO MUNDIAL DE SAÚDE. Ruído, dados e estatísticas. Disponível em: <http://www.euro.who.int/en/health-topics/environment-and-health/noise/data-and-statistics>. Acesso em: 12 abr. 2017.

SALDIVA, P. H. N *et al*. *Avaliação do impacto da poluição atmosférica no estado de São Paulo sob a visão da saúde*. São Paulo: Instituto Clima e Sociedade, 2013. Disponível em: <http://www.saudeesustentabilidade.org.br/site/wp-content/uploads/2013/09/Documentofinaldapesquisapadrao_2409-FINAL-sitev1.pdf> Acesso em: 18 ago. 2017.

SOLUÇÕES PARA CIDADES (2013). Requalificação de ruas comerciais: a parceria entre a Associação de Lojistas e a Prefeitura Municipal no projeto da Rua Oscar Freire. São Paulo. Disponível em: <http://www.solucoesparacidades.com.br/wp-content/uploads/2013/08/AF_07_SP_REURBANIZACAO%20OSCAR%20FREIRE_Web.pdf>. Acesso em: 18 ago. 2017.

SOUSA, Denise da Silva de. Instrumentos de gestão de poluição sonora para a sustentabilidade, 2004. Disponível em: <http://www.ppe.ufrj.br/ppe/production/tesis/dssouza.pdf>. Acesso em: 18 ago. 2017.

THE WORLD BANK GROUP. WALKABILITY. Disponível em: <https://walkabilityasia.org>. Acesso em: 10 dez. 2018.

URBI-I, Before-After Gallery. Disponível em: <http://www.urb-i.com/before-after-gallery>. Acesso em: 12 abr. 2017.

VISION ZERO. Disponível em: <http://www1.nyc.gov/site/visionzero/index.page>. Acesso em: 18 abr. 2017.

WALK21. Disponível em: <http://www.walk21.com>. Acesso em: 3 abr. 2017.

WALK SCORE. Disponível em: <http://www.walkscore.com>. Acesso em: 3 abr. 2017.

WRI BRASIL. Passo a passo para a construção de um Plano de Mobilidade Corporativa. Disponível em: <http://www.wrirosscities.org>. Acesso em: 18 ago. 2017.

DIREITO À CIDADE, CAPITALISMO E RACISMO EM PROTESTOS NO RIO DE JANEIRO DE 2013-2014

MARIO CAMPAGNANI
NATÁLIA DAMAZIO

INTRODUÇÃO

O direito a cidade, principalmente com o advento dos megaeventos, tornou-se ponto central de debates, tanto no campo acadêmico, quanto na política. Apesar de tal tema ser uma reivindicação de longa data de movimentos sociais, principalmente os que se relacionam à moradia, a proximidade da Copa e Olimpíadas e o início dos grandes protestos de 2013 aqueceram o debate, aprofundando a questão "cidade para quem?". Nesse sentido nos cabe traçar algumas definições para esse breve artigo.

Em primeiro plano, não buscamos exaurir o debate, mas sim lançar questões críticas sobre o tema, tendo como recorte temático processos de repressão e criminalização de protestos na cidade do Rio de Janeiro entre 2013 e 2014. Nesse sentido, apontamos que o processo de acesso e direito à cidade na visão dos autores não se limita somente ao que é possível analisar nesse artigo, tendo em vista que a exclusão e restrições se dão de forma muito mais ampla na cidade, por meio de metodologias diversas da repressão policial em sentido estrito, mas também através da construção de muros nas periferias, falta mobilidade urbana, criminalização da pobreza e da negritude, remoções forçadas, dentre outras (JUSTIÇA GLOBAL, 2013).

Ainda elaborando o recorte aqui determinado, analisaremos apenas o quesito protestos quando esses são contra-hegemônicos, ou seja, protestos que buscavam romper com as opressões em curso impostas pelo capitalismo, sendo essas analisadas pelos impactos e intensidades diversas frente aos diferentes sujeitos que acessam a metodologia de ocupação das ruas, apontando assim descompassos entre a criminalização e repressão dos espaços do centro da cidade e da periferia e suas dimensões raciais na cidade do Rio de Janeiro entre 2013 e 2014.

Ressaltamos ainda que por direito à cidade entendemos, como definido por Harvey (2013), não apenas a visita ou retorno à cidade, mas sim como uma liberdade de transformação da vida urbana. De forma breve e conforme o autor: "A liberdade da cidade é, portanto, muito mais que um direito ao acesso àquilo que já existe: é o direito de mudar a cidade mais de acordo com o desejo de nosso coração. […]" (HARVEY, 2013, p. 28). No que se refere a megaventos, a visão defendida nesse artigo é que não seriam esses à fonte original do problema de exclusão e violência na cidade contra grupos subalternizados, porém funcionam como catalizadores e aprofundadores das estruturas de dominação e opressão já existentes no país.

Nesse sentido analisaremos alguns componentes específicos do processo de repressão e criminalização de protestos:

a. seletividade na definição de um protesto como tal e suas consequências;
b. uso de armas letais e menos letais em protestos de favela e em protestos na região central e sul da cidade;
c. criminalização dos manifestantes em 15 de outubro de 2013 e processo de criminalização de Rafael Braga Vieira em 20 de junho de 2013.

Assim nos propomos, através da exposição de práticas e casos emblemáticos que foram denunciados[1] por vítimas, organizações não-governamentais, articulações políticas e movimentos sociais, analisar as diferenças acima mencionadas, apontando questionamentos de como os impactos do Estado na repressão à pobreza e à negritude se dá de forma também desigual em relação a protestos no espaço da cidade, já que:

> A cidade não é apenas a organização funcional do espaço, suas ruas e edificações, seus bairros, pessoas carregando sonhos, isoladas na multidão, em um deserto de prédios, que aboliu o horizonte e apagou as estrelas. A cidade é a expressão das relações sociais de produção capitalista, sua materialização política e espacial que está na base da produção e reprodução do capital. (IASI, 2013, p. 41)

1 Grande parte dessas denúncias foram recolhidas pela organização Justiça Global e outras organizações parceiras, tanto no Rio de Janeiro quanto no resto do país, para documentar violações de direitos humanos em protesto, buscando realizar denúncias no âmbito internacional para sistemas de proteção de direitos humanos, seja no âmbito da Comissão Interamericana de Direitos Humanos seja nas Relatorias Especiais da Organização das Nações Unidas, cuja temática era afeita aos temas e violações ocorridas nos protestos.

O QUE É TIDO COMO PROTESTO E O QUE NÃO? DISCURSOS HEGEMÔNICOS E SELETIVIDADE

Um dos pontos-chave da legitimação de repressões violentas e criminalização massiva dos protestos entre 2013-2014 era a definição a ele dada, principalmente se observada pela chave "pacifismo" e "não pacifismo". Nesse sentido, atos acabavam perdendo sua legitimidade ao serem descaracterizados enquanto protestos por meios de comunicação e pelos agentes de Estado, passando a ser definidos como "baderna", "vandalismo" ou nos casos de favelas e periferias "ações do tráfico". Nesse sentido, colar a imagem de protesto com paradigmas criminalizantes como vandalismo,[2] tornava-se uma metodologia essencial tanto para o punitivismo, quanto para justificar quaisquer dispositivos repressivos adotados pelo Estado com intuito de desmobilização da respectiva forma de exercer o direito à cidade.

A imprensa, até o início de junho de 2013, apoiava e incentivava as manifestações que vinham ocorrendo em menor escala nos meses anteriores a junho,[3] no entanto com a ampliação do número de participantes teve início uma campanha de desqualificação do movimento, utilizando os termos "vandalismo" e "baderneiros" para se referir aos manifestantes.

Em grande parte das manchetes de jornais, emissoras de TV ou rádios pertencentes aos grupos que possuem a detenção dos meios de informação no país, era comum o uso de frases como "o ato começou pacífico, mas terminou em vandalismo". A aposta não era só de afastar as pessoas das ruas, mas de estigmatizar ativistas identificados mais à esquerda, fossem eles anarquistas, socialistas, ou de outras vertentes políticas. O que parecia estar em jogo era disputa ideológica entre o capital e os privilégios da elite – onde se inclui a imprensa – contra os que questionavam esse

2 É interessante perceber que nos Projetos de Lei em nível federal que buscam criminalizar protesto à ideia de vandalismo, terrorismo e tipos semelhantes tendem a reforçar essa divisão entre manifestações pacíficas e "baderna", legitimando a repressão e a criação de novos tipos penais para tal. Caminhando nesse sentido, apontamos alguns Projetos de Lei em curso hoje, como: (a) desordem em local público: PL 7121/2014; (b) terrorismo: PL 5773/2013, PL 5571/2013, PL 1549/2015, PL 2583/2015, PL 1790/2015, PL 1378/2015, PL 5065/2016, PLS 588/2011; (c) uso de máscaras: PL 5964/2013, PL 7157/2014, PL 6198/2013, PL6461/2013; (d) vandalismo: PLS 508/2013; entre outros.

3 É fundamental apontar que tanto no campo da reforma agrária, quanto nas regiões de favela e periferias, o ato de protestar já não era lido como tal, ficando represados pelo discurso da mídia hegemônica como "atos ligados ao crime organizado" ou "invasão".

estado de coisas.[4] Duas foram as principais consequências da massificação desse discurso: a ampliação de projetos de lei que tramitavam no Congresso Nacional buscando a intensificação dos tipos penais e uma aplicação mais autoritária por parte do judiciário da legislação já existente. Em nível federal, no início de 2014, o então presidente da Câmara dos Deputados, Henrique Eduardo Alves, anunciou que daria andamento a dez projetos de lei (PL) sobre protestos que tramitavam na casa desde 2013, para que fossem apensados em um só projeto, a tramitar em regime de urgência. Tratava-se de textos que em sua maioria proibiam o uso de máscaras, aumentavam penas ou que atribuíam tratamento diferenciado para crimes e "atos de vandalismo" ocorridos em manifestações. Somente um projeto, dentre os dez, poderia ser analisado como potencialmente benéfico ao direito de protestos, pois se destinava à proibição do uso de armas letais em manifestações e estabelecia a aplicação do princípio da não violência e garantia dos direitos humanos no contexto de manifestações e eventos públicos (PL 6500/13).

O caso mais emblemático é a proposta de tipificação do crime de terrorismo. No Congresso Nacional existiam ao menos seis propostas em andamento, como o Projeto de Lei do Senado (PLS) 499/2013; PLS 762/2011; PLS 728/2011 – que cria diversos novos tipos penais especificamente para o período de Copa do Mundo –; PL 5.773/2013; PL 236/2012 – uma proposta de reforma global do Código Penal –; e PLS 44/2014. De forma geral, todas as propostas eram marcadas por uma excessiva indefinição dos elementos do delito, definindo-o como conduta que causa "pânico" ou "medo" na população. São definições subjetivas e a sua constatação varia conforme lugar, o contexto e as pessoas envolvidas, apresentando um risco agravado de criminalização dos movimentos sociais.

---

4 Elencamos a seguir algumas manchetes que realizam exatamente esta divisão entre manifestantes pacíficos e não pacíficos. Em 2013: "Sexto protesto termina em vandalismo em SP", *Jornal da Band*, São Paulo, 19 jun. 2013;"Ato em Brasília começa pacífico, mas termina em vandalismo", **TV UOL**, 21 de junho de 2013;"Protesto que começou pacífico novamente termina em vandalismo, saques e prisões em Porto Alegre", *ZH Notícias*, 25 de junho de 2013; "Protesto pacífico em São Paulo termina com vandalismo", *Público*, 31 de julho de 2013; "Protestos terminam com confronto e atos de vandalismo no Rio e SP", *Folha de S.Paulo*, 16 de outubro de 2013; "Dono de loja depredada em protesto no Rio chora e desabafa: maldade", **G1**; "Protestos contra Sérgio Cabral termina em vandalismo e nem Rede Globo escapa", Rádio Itaperuna FM, 18 de julho de 2013. Em 2014: "Manifestação contra a Copa termina em violência em São Paulo", *O Globo*, 25 de janeiro de 2014; " Manifestação em SP contra os gastos da Copa termina em vandalismo e com feridos", *G1*, 16 de maio de 2016; LISBOA, V., "Quem protestar na Copa pode ser terrorista", *Papo de Homem*; "Manifestação anti-Copa termina em vandalismo em Curitiba", *Bonde News,* 16 de junho 2014.

No ano de 2015, novamente a tipificação do terrorismo ganha força, por intermédio do PL 2016/2015, que cria alteração na Lei de Organizações Criminosas (Lei 12.850/2013). O projeto, desde seu texto inicial, igualmente era possuidor de definições abertas e passíveis de aplicação autoritária. Previa que terrorismo podia ter motivação política e ideológica. Diz o texto:

> É previsto como terrorismo "I- intimidar o Estado, organização internacional ou pessoa jurídica, nacional ou estrangeira ou representações internacionais ou coagi-los a ação ou omissão; II- provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública".

O autor da proposta segue definindo como atos de terrorismo uso ou ameaça de uso, transporte, armazenamento, porte ou transporte de substâncias que possam causar danos ou promover destruição em massa; incêndio, depredação, saque, destruição ou explosão de meio de transporte ou qualquer bem público ou privado, dentre outras condutas.

O projeto tramitava em regime de urgência, tendo sido aprovado no dia 13 de agosto de 2015 na Câmara dos Deputados, incluindo a vedação de aplicação da legislação a manifestantes (Parágrafo 2º) e com a supressão dos motivos ideológicos e políticos de seu texto base. Após a aprovação o PL 2016/2015, foi votado no Senado, sofrendo grave alteração que incluía novamente os termos ideológicos e políticos, trazendo ainda um agravante que é a ideia de um dos motivadores ser "extremismo político", definido como "ato que atentar gravemente contra as instituições democráticas", sendo igualmente suprimidas as excludentes de ilicitude a movimentos sociais. Terminou por ser aprovado nos termos do projeto da Câmara e sancionado em março de 2016, no entanto ainda existem projetos de lei que buscam ampliar o escopo punitivo do tipo "terrorismo".

Do mesmo modo, o uso de máscaras foi um mote para o discurso que pretendia diferenciar manifestantes pacíficos de não pacíficos. Após reiteradas reportagens associando a ideia de manifestantes não pacíficos[5] comumente denominados de vândalos ou *black blocs* pela mídia hegemônica – à utilização de mascaras, inclusive as de proteção contra os efeitos do gás lacrimogênio, o Rio de Janeiro passou a proibir ser uso em protestos. Para tal era autorizado a identificação civil e criminal – prisão para averiguação – daqueles que as utilizassem. A Lei 6.528/13 (Lei das Máscaras), aprovada pela Assembleia Legislativa do Rio de Janeiro em 10

5 Cf. "Os manifestos pacíficos e estragos dos baderneiros mascarados", *Folha da Região*, 29 de outubro 2013; "Mascarados bloqueiam um dos sentidos da Avenida Paulista em SP", *UOL Notícias*, 5 de novembro de 2013; "Manifestantes iniciam quebra-quebra em ruas do centro de Curitiba", *CGN*, 16 de junho de 2014.

de setembro, foi um dos pontos cruciais no processo de criminalização das manifestações populares. A aprovação da lei seguiu a tendência inaugurada pela decisão da 27ª Vara Criminal da Comarca do Rio de Janeiro, que permitiu que manifestantes mascarados pudessem ser identificados criminalmente, mesmo inexistindo a suspeita fundada de prática de infração penal. Isto significa que os policiais passaram a ter a autorização de conduzir coercitivamente para delegacia – com a justificativa de consulta de antecedentes criminais, identificação datiloscópica e fotográfica – os manifestantes que tivessem o rosto coberto por máscara, lenço ou afins, mesmo com identificação civil.

No segundo eixo dessa análise, qual seja a utilização desta dicotomia pelo judiciário, podemos exemplificar o caso da prisão dos 23 manifestantes na véspera da final da Copa do Mundo FIFA em 2014. O processo criminal é marcado pela tentativa de divisão entre manifestantes pacíficos e não pacíficos, intuindo criminalizar aqueles que fossem atribuídas metodologias tidas como não pacificas, independentemente da existência ou não de provas nesse sentido. O referente caso inicia-se no dia 12 de junho de 2014, na cidade do Rio de Janeiro, quando foram cumpridos 26 mandados de prisão temporária. Durante a busca e apreensão feitas nas casas dos 26 manifestantes, quando do cumprimento do mandado, foram apreendidos principalmente celulares, panfletos que continham críticas ao Estado, bandeiras anarquistas, cadernos com anotações sobre reuniões de sindicatos ou movimentos sociais, máscaras contra gás e tornozeleiras, todos tratados como material que comprovaria que tais manifestantes, por exercerem uma crítica ao Estado e por possuírem ideologia diferente da hegemônica, estariam incorrendo no tipo de associação criminosa. A decisão que defere tais mandados não possui nenhuma justificativa amparada em lei, já que seu fundamento é a existência de indícios que levariam a crer que em momento futuro poderia ser cometido pelos manifestantes atos de violência. Na íntegra a decisão afirmava: "Que há sérios indícios de que está sendo planejada a realização de atos de extrema violência para os próximos dias, a fim de aproveitar a visibilidade decorrente da Copa do Mundo de futebol, sendo necessária a atuação policial para impedir a consumação deste objetivo e também para identificar os demais integrantes da associação" (TJRJ, processo n. 0229018-26.2013.8.19.0001, 2014). Isso demonstra que o procedimento implicava na reprodução desta mesma lógica que cinde as manifestações com intuito de legitimar o autoritarismo estatal. No pedido de interceptação telefônica e telemática impetrado no juízo de plantão do Tribunal de Justiça do Estado do Rio de Janeiro, contido no inquérito policial que originou o processo, afirma-se que: "Nas convocações pelas redes sociais, os líderes dos movimentos pregam

uma inversão de valores colocando a sociedade contra os agentes de segurança pública, considerados truculentos e responsáveis pela violência contra inocentes [...]" (TJRJ, Processo 0229018-26.2013.8.19.0001, fls. 479-524). Tal afirmação evidencia que o intuito da investigação é tratar como contrário à lei o ato de crítica ao uso excessivo da força por parte dos agentes do Estado. Esta lógica permanece durante todo o processo.

É importante fazer um aprofundamento nesse ponto sobre o arcabouço probatório acostado na investigação que gerou tal processo. Fundamentalmente o procedimento apuratório foca-se em duas formas de colher informação: notícias de jornais sobre atos e monitoramento de páginas ligadas a movimentos sociais e perfis de determinados manifestantes na rede social Facebook. Criou-se uma lista mapeando mais de 70 movimentos sociais e páginas de coletivos nas redes sociais como alvos do que é denominado "rondas virtuais", no qual geram na realidade *prints* de *posts* e fotos como tentativa de criminalizar posicionamentos políticos virtuais como se fossem indícios de participação em organizações criminosas "responsáveis pelos atos de violência" nos protestos. O papel da vigilância *on-line* e do cerceamento à liberdade de expressão é perceptível também nas propostas legislativas a nível federal, em especial ao se tratar de tipificação de condutas de incitação. Nessa última linha apontamos o PL1790/2015, PL 2294/2015 e, principalmente o PLS 762/2011 que preveem a criminalização de incitação ao terrorismo, sendo que o último define a conduta como "Incitar o terrorismo por meio da divulgação de material gráfico, sonoro ou de vídeo", prevendo aumento de pena específico caso o material seja divulgado na internet.

A reafirmação de dicotomias é eixo estruturante para a possibilidade de se buscar construir uma aparência de legitimidade às vedações arbitrárias exercidas pelo Estado. No entanto, apesar de o grande motor de tais movimentos terem sido os grandes protestos ocorridos nas capitais e regiões centrais do país, é no caso concreto que é possível perceber as nuances do tratamento diferenciado de acesso ao direito à cidade de determinados sujeitos e territórios.

DA BOMBA AO FUZIL: METODOLOGIA REPRESSIVA NO "ASFALTO" E NA FAVELA

Durante as manifestações, a repressão por intermédio do uso de armas menos letais e até mesmo uso de armas letais para dispersar as manifestações e impedir o exercício da liberdade de expressão eram, e seguem sendo, frequentes. No que diz respeito às metodologias utilizadas pela polícia em busca de reprimir os protestos com o uso de armamento menos letal, era

relatado a realização de revistas em diversos manifestantes, fechamento de áreas de escoamento, manutenção de uma situação de estresse até o momento em que se apagavam as luzes do local do protesto, começando a disparar diversas bombas de gás lacrimogêneo e de efeito moral e balas de borracha nos manifestantes. Após a dispersão, a polícia começava a realizar as varreduras, nas quais perseguiam os manifestantes dispersos em diversas áreas, reutilizando os armamentos menos letais e realizando detenções em massa.

O início dos megaeventos, com a Copa das Confederações, marcou uma expansão da repressão de protestos com auxílio do aparato já disponível ao Estado dentro do campo da segurança pública:

> A Copa das Confederações realizada em 2013 foi um marco na atuação conjunta das polícias e das Forças Armadas em megaeventos. Foram empregados cerca de 3.700 militares, além de mais de 500 viaturas de diversos tipos, dentre elas: blindadas, mecanizadas, antiaéreas, de defesa cibernética, comando e controle, transporte de tropa e de defesa química, biológica, radiológica e nuclear. Foram utilizados, também, oito helicópteros das Forças Armadas - um deles equipado com o 'Olho da Águia', dois esquadrões de Cavalaria de Choque e uma seção de Cães de Guerra. (MARINHO, 2014, p. 27)

Os protestos ocorridos neste período sofreram repressão violenta por parte das forças de segurança, incluindo cerco de manifestantes, além de uso desproporcional e em regiões vitais de balas de borracha e bombas de gás lacrimogênio.[6]

Apesar da óbvia arbitrariedade presente nas repressões às manifestações que ocorrem nos centros das cidades, faz-se necessário apontar que essas se tornam ainda mais duras no caso dos protestos em áreas de favela e periferias, marcados pelo uso do armamento letal e de execuções. Aponta-se com isso o racismo enquanto chave para que o Estado se valha de metodologias mais violentas na hora de restringir o acesso ao direito à cidade. Como casos emblemáticos, apresentamos o de José Joaquin Santana e Aliélson Nogueira.

Durante manifestação de moradores em Manguinhos, José Joaquim Santana, de 81 anos, foi atingido na cabeça por disparos de arma de fogo no dia 18 de dezembro de 2013. Policiais da UPP local foram acusados por testemunhas de terem efetuado os disparos.[7] Do mesmo modo, no caso

---

6 Cf. A NOVA DEMOCRACIA. Final da Copa das Confederações é marcada por violentos protestos, ano XII, nº 113, 2ª quinzena de julho de 2013. Disponível em: <http://www.anovademocracia.com.br/no-113/4818-final-da-copa-das-confederacoes-e-marcada-por-violentos-protestos>. Acesso em: 23 ago. 2017.

7 "Idoso é morto em confusão entre moradores e PMs da UPP de Manguinhos", Estadão, 19 de dezembro de 2013.

de Aliélson Nogueira, durante um protesto à noite do dia 04 de abril de 2013, após uma moradora de 10 anos de idade ter sido atingida por uma bomba de efeito moral no rosto,[8] a repressão foi marcada por agressão física e utilização de arma de fogo, deixando três moradores baleados. Um deles foi Aliélson Nogueira, que comia um cachorro quente na região conhecida como Pontilhão, sendo atingido na cabeça e morrendo no local. Os moradores cercaram o corpo do rapaz para impedir que a polícia o retirasse dali, argumentando ter prestado socorro à vítima e no intuito de garantir que a perícia fosse realizada de forma adequada.[9] Após a morte de Aliélson, a manifestação que havia começado mais cedo se ampliou e foi reprimida através da utilização de bombas de efeito moral.

Apesar de poucos estudos abordando o tema racismo e direito à cidade, algumas metodologias de controle podem ser observadas nesse sentido, dentre elas as remoções durante o período dos megaeventos em favelas, os recolhimentos compulsórios de jovens negros durante a operação verão e o perfil dado às abordagens policiais. Enfatizamos que isso são apenas exemplos e não estamos os abordando de forma exaustiva nesse artigo, tendo em vista que cada um desses requer um estudo a parte, mas apenas o trataremos de forma breve para demonstrar o perfil segregador do direito à cidade no Rio de Janeiro.

No que se refere às remoções, tema amplamente denunciado pelos movimentos sociais, pela Defensoria Pública do Estado do Rio de Janeiro por meio do Nucleo de Terras e Habitação e por organizações não governamentais, ocorreram nos últimos anos, principalmente, de duas formas:

a. expulsão por consequência de especulação mobiliária;

b. deslocamento forçado.

Devemos ressaltar que os espaços de favela são compostos por um grande contingente de afrodescendentes do município do Rio de Janeiro (BRAZIL, H., 2011).

As regiões impactadas pelos megaeventos, quais sejam, região portuária, zona sul e zona oeste, sofreram um duro impacto de subida de valores imobiliários durante o período de preparação. A Barra da Tijuca em especial, desde

8 JORNAL EXTRA. Um morador morre e outros dois ficam feridos após confronto com a polícia na UPP do Jacarezinho. Publicado em 5 de abril de 2013. Disponível em: <http://extra.globo.com/casos-de-policia/um-morador-morre-outros-dois-ficam-feridos-apos-confronto-com-policia-na-upp-do-jacarezinho-8033173.html>. Acesso em: 23 ago. 2017.

9 A NOVA DEMOCRACIA. Policiais da UPP atiram para matar no Jacarezinho. Publicado em 5 de abril de 2014. Disponível em: <https://www.youtube.com/watch?feature=player_embedded&v=PAAvYFG7Hjc>. Acesso em: 23 ago. 2017.

os jogos Pan Americanos, sofre grande impacto em termos de expansão, sendo o Rio de Janeiro a cidade que teve, durante esse período, a maior valorização dos imóveis no país. Somados a esse processo que impactou a cidade como um todo, as Unidades de Polícia Pacificadoras também terminam por gerar uma supervalorização do custo de vida e especulação, tornando inviável a manutenção dos antigos moradores, que terminam por se deslocar da região, caracterizando a expulsão por impossibilidade de sustento nesses espaços que se encontravam em zonas não-periféricas da cidade, gerando a segregação da população mais pauperizada para zonas mais distantes (CAMPOS, C., 2014). Simultaneamente, processos mais expressos e violentos de expulsão tomaram lugar nessas mesmas regiões. Segundo Brazil:

> […] os interesses da 'cidade moderna' ficam atrelados à necessidade de valorização do capital e para tanto se faz a higienização social local […]. A exclusão da população pobre ao direito à cidade resulta na procura do seu imóvel em lugares aonde o poder público não alcança. (BRAZIL, 2011)

O efeito segregacionista e higienista de cunho racial do acesso à cidade em sua plenitude torna-se ainda mais explicito quando lidamos com as internações compulsórias que ocorreram com muita intensidade durante o período preparatório dos megaeventos, assim como pelo recorte dado a abordagens policiais. No último caso citado, uma pesquisa feita por Silvia Ramos e Leonarda Musimeci (2005) já delimitou que as abordagens policiais para revista com base em "elementos suspeitos" era galgada, fundamentalmente, em preconceitos de raça e classe. No mesmo sentido, o recolhimento compulsório reforça a perspectiva racista de perseguição e segregação de negros: desde 2011, com intensificação em 2015, o recolhimento compulsório de meninos e meninas em situação de rua vem sendo uma constante atuação do Estado. Nesse sentido, um evento emblemático em 22 e 23 de agosto torna-se fundamental para percepção da agudização dessa violação por parte do Estado. Após determinação de parada e revista de diversos ônibus que vinham da zona norte e oeste em direção à zona sul, aproximadamente 150 jovens negros foram retirados dos transportes coletivos sendo levados ao Centro Integrado de Atendimento à Criança e ao Adolescente (JUSTIÇA GLOBAL *et. al.*, 2016). Quando tal operação foi proibida, "justiceiros" de áreas mais ricas da cidade começaram a perseguir e espancar crianças e adolescentes negros, como ocorrido no dia 20 de setembro do mesmo ano em Copacabana (JUSTIÇA GLOBAL *et. al.*, 2016).

Apesar da catalisação de violência estatal ocasionada por intermédio dos megaeventos, dirigida a protestos, é notório que a acessibilidade entre brancos e negros ao direito à cidade é profundamente cindida e desigual, baseada em uma negativa não apenas da potencialidade de realização de um discurso contra-hegemônico, mas uma negação de sua própria vida.

ORGANIZAÇÃO CRIMINOSA E PORTE DE PINHO SOL: DUAS PRISÕES ILEGAIS E DOIS PESOS

As relações racistas no país igualmente impactam quando o mote para impedimento do exercício do direito a cidade se dá por meio da criminalização. A justiça criminal é seletiva e racista, conforme posto por Wacquant (2011), e tal regra não é alterada quando se trata de criminalização de protestos. Para observar tal proposta, será feita a análise de duas prisões de grande repercussão: a de 84 manifestantes na Cinelândia em 15 de outubro de 2013 e a prisão de Rafael Braga Vieira em 20 de junho de 2013.

Nos protestos comumente era utilizada a tipificação de associação criminosa, derivada da Lei de Organizações Criminosas (Lei 12.850/2013), para ser possível realizar a criminalização de forma genérica com intuito de desmobilizar os protestos. Nesse sentido o dia 15 de outubro de 2013, quando um novo grande ato teve lugar no centro da cidade do Rio de Janeiro, é emblemático. O ato foi marcado pela intensificação da repressão policial, especialmente no que diz respeito às detenções arbitrárias. Segundo informações da Polícia Civil, cerca de 190 pessoas foram detidas,[10] tendo ocorrido 84 casos de prisão provisória em decorrência de suposto flagrante.

Além do grande volume de detenções arbitrárias, o que qualifica especialmente esse dia é o uso do tipo penal de associação criminosa contra os manifestantes. Importante notar que antes mesmo das detenções já havia sido anunciado pelos órgãos públicos a utilização da referida tipificação como forma de repressão aos manifestantes,[11] mostrando uma intenção de criminalizar independentemente da conduta individual do detido.

Os manifestantes foram distribuídos em diversas delegacias, e em grande parte delas, com exceção de uma, todos foram enquadrados no mesmo tipo penal. Isso foi especialmente representativo nas 25ª e 37ª Delegacias, para as quais a maior parte dos manifestantes foi encaminhada, mostrando não

10 UOL. Para chefe da polícia civil do Rio endurecimento da lei aumentou o número de presos em protestos. Publicado em 16 de outubro de 2013. Disponível em: <http://noticias.uol.com.br/cotidiano/ultimas-noticias/2013/10/16/para-chefe-da-policia-civil-do-rio-endurecimento-da-lei-aumentou-numero-de-presos-em-protestos.htm>. Acesso em: 23 ago. 2017.

11 TERRA. RJ: Policia usará Lei de Organização Criminosa contra detidos por Vandalismo. Publicado em 8 de outubro de 2013. Disponível em: <http://noticias.terra.com.br/brasil/policia/rj-policia-usara-lei-de-organizacao-criminosa-contra-detidos-por-vandalismo,8e9b11028b991410VgnCLD2000000ec6eb0aRCRD.html>. Acesso em: 23 ago. 2017.

haver nenhuma correspondência entre a conduta do indivíduo na manifestação e a forma de criminalização. Isso foi posteriormente reconhecido em parte pelo Poder Judiciário, com o arquivamento de um dos casos.

Apesar do relaxamento e arquivamento de dois processos referentes aos manifestantes – dos trinta e três adultos detidos na 25ª Delegacia de Polícia,[12] a dois adultos detidos na 19ª Delegacia de Polícia,[13] e ao relaxamento da prisão de vinte adultos da 37ª Delegacia de Polícia[14] –, o Judiciário também tomou decisões que agravam o processo de repressão política e arbitrariedade do poder público. A participação do judiciário pode ser comprovada, pois grande parte das provas que geraram a prisão em flagrante e conversão em prisão preventiva se deram exclusivamente por depoimentos policiais envolvidos nas prisões.[15] Deve ser ressaltado que em todos estes casos a única prova existente contra os manifestantes são os depoimentos dos próprios policiais militares que efetuaram a prisão, sendo tais depoimentos marcados pela repetição do depoimento de outro policial com as mesmas palavras, como é evidente no Termo de Declaração dos dois policiais que executaram as detenções na 12ª Delegacia de Polícia.[16]

Diversos padrões na conduta criminalizante do Estado nos casos advindos desse protesto podem ser observados, dentre eles:

a. os adolescentes tiveram sua internação provisória[17] decretada, mesmo não existindo nenhum indício de materialidade, autoria ou individualização das condutas que gerassem a internação. Nesse caso, a decisão de prosseguimento da ação com a manutenção da apreensão cautelar foi do Ministério Público, que foi confirmada pela Juíza. Sob o argumento de que os adolescentes, ao participarem de uma manifestação na qual, segundo o entendimento da juíza, "houve abuso de direito", representariam uma ameaça à ordem, ainda que a própria juíza reconheça não ser possível individualizar a conduta dos adolescentes;

12 TJRJ, Processo nº 0361545392013.8.19.0001.

13 *Idem*.

14 *Idem*.

15 Deve ser enfatizado que o risco de arbitrariedade de policiais ser reforçado pelo Judiciário é agravado no estado do Rio de Janeiro, tendo em vista a Súmula 70 do Tribunal de Justiça do Estado do Rio de Janeiro, que prevê que o depoimento de policiais é suficiente para condenação em âmbito criminal, ao contrário do senso de princípios e normas estabelecidos pelo Direito Penal.

16 PCERJ, Registro de Ocorrência nº 012-09784/2013.

17 Modalidade de apreensão cautelar prevista no Estatuto da Criança e do Adolescente como medida de exceção, Art. 174 da Lei 8.069/90.

b. os manifestantes detidos na 19ª Delegacia de Polícia tiveram seus alvarás expedidos em 17 de outubro de 2013 e apenas foram liberados em 22 de outubro, isso é, foram ilegalmente privados de liberdade por cinco dias. De igual maneira, os detidos da 12ª Delegacia de Polícia tiveram seu alvará expedido em 18 do mesmo mês, sendo liberados quatro dias depois. O prazo legal para cumprimento do alvará é de vinte e quatro horas;

c. três manifestantes detidos na 12ª Delegacia de Polícia, no dia 15 de outubro, também foram capitulados por associação criminosa,[18] tendo sua liberdade provisória concedida em 18 de outubro.[19] No entanto, nessas decisões a liberdade foi condicionada à não participação em nenhuma manifestação que tenha qualquer forma de agressão a quaisquer indivíduos, o que claramente é de impossível controle por parte dos indiciados, ainda mais com os constantes relatos de violência policial.

Apesar de gravíssimo caso de tentativa de criminalização de movimentos sociais, mesmo que o poder público tenha sido incapaz de individualizar as condutas dos manifestantes, o caso de Rafael Braga Vieira mostra que a negritude é fator determinante para maior endurecimento no tratamento frente a Justiça Criminal.

Rafael era morador de rua e catador de latinhas na cidade do Rio de Janeiro. Ele foi detido na noite de 20 de junho de 2013, quando ocorreu uma das maiores manifestações das Jornadas de Junho, com cerca de um milhão de pessoas. Rafael carregava duas garrafas no momento da detenção, uma delas contendo desinfetante "Pinho Sol" e a outra contendo água sanitária. Sob a acusação de porte de artefato explosivo (art. 16, III, da Lei nº 10.826/2003), o juiz da 32ª Vara Criminal da Capital condenou Rafael em 2 de dezembro de 2013 a 5 anos de reclusão e 10 dias, além de multa. A defesa apelou da condenação e, em 8 de agosto de 2014, a Terceira Câmara Criminal do Tribunal de Justiça do Rio de Janeiro decidiu manter a condenação, reduzindo, porém, a pena de cinco anos para quatro anos e oito meses de reclusão. Apesar do laudo pericial ter concluído que as garrafas contendo desinfetante e água sanitária teriam pouca potencialidade para serem explosivos, por terem sido confeccionados em garrafas plásticas, ou seja, com mínima possibilidade da quebra possibilitar o espalhamento do seu conteúdo inflamável, para o desembargador relator, Carlos Eduardo Roboredo, isto não inviabilizaria sua capacidade

18 PCERJ, Registro de Ocorrência nº 012-09784/2013.

19 TJRJ, Processo nº 0361545392013.8.19.0001.

incendiária. O desembargador afirmou que não seria necessário ser expert para concluir que uma garrafa, ainda que plástica, contendo substância inflamável e com pavio em seu gargalo, possui aptidão incendiária ao ser acionada por chama. A defesa entrou ainda com Recursos para o Superior Tribunal de Justiça (STJ) e para o Supremo Tribunal Federal (STF), que, entretanto, não foram admitidos. Em 3 de maio de 2015, a defesa ainda apresentou um habeas corpus em favor de Rafael no STJ baseado no resultado do laudo pericial, que teria demonstrado a fragilidade das acusações. Segundo o laudo, uma das garrafas foi desconsiderada por conter água sanitária. Já a segunda garrafa continha quantidade insuficiente de etanol para permanecer dentro se ela fosse arremessada. Além disso, o material da garrafa, por ser de plástico, impediria que ela estourasse de modo a causar explosão e, para completar, o suposto pavio derreteria a garrafa caso fosse aceso, antes mesmo que esta pudesse ser arremessada. O habeas corpus, entretanto, foi indeferido pelo ministro Sebastião Júnior, sob a justificativa de que neste tipo de recurso não é possível reanalisar os fatos já julgados no processo. O caso de Rafael Braga é emblemático pois ele sequer participava da manifestação, e mesmo com uma prova juntada ao processo de que o produto não teria potencial de causar danos, ele foi condenado. Ressalta-se que apenas policiais foram ouvidos como testemunhas no processo. Ele foi a primeira pessoa condenada em decorrência dos protestos que se iniciaram em junho de 2013. Rafael é negro e catador de latinhas, perfil que não se assemelha com a maioria dos manifestantes de 2013. Rafael não foi punido por exercício político do direito à cidade em uma manifestação, ele foi punido dentro da lógica racista por estar próximo a uma manifestação, por ser negro, por ser pobre em uma cidade que o norte político é a desumanização de sua subjetividade e controle de seu corpo.

CONCLUSÃO

Com base na análise de casos emblemáticos esse breve artigo buscou lançar algumas questões sobre o direito à cidade, compreendido também como direito a se valer de metodologias diversas para ocupação e modificação das relações de desigualdade gestadas pelo capitalismo em seu espaço. Apesar de ser comumente trabalhado em categorias genéricas e universalizantes, o tema protesto necessita ser compreendido como parte do fenômeno de exclusão e de gestão dos sujeitos no espaço da cidade, dependendo de que também seja levado em conta as diversas metodologias e intensidades que essa limitação ocorre.

Em uma estrutura política baseada no racismo – que sustenta seu campo de repressão e acesso a direitos em uma seletividade desumanizadora para negras e negros – a reprodução das relações de dominação se refazem no campo de protestos e reivindicações. Ser criminalizado por sua posição contra-hegemônica não é o mesmo que sua existência ser a representatividade de uma subjetividade cuja sobrevivência em si é contra-hegemônica. Negros e negras moradoras de periferias e favelas como Aliélson – cujos direitos não deveriam ser acessíveis dentro da lógica da branquitude que rege as relações de poder no Brasil - o espaço da cidade torna-se hostil, um local de reiteradas tentativas de dominação de sua agência.

No entanto, é nos sujeitos que vivem na fronteira da percepção de sua própria humanidade e das reiteradas tentativas da dominação de seus corpos e desumanização de sua subjetividade que se encontra a maior potência de luta. Romper as amarras que impedem a cidade enquanto local de afetos e de políticas é iniciar um debate e potencializar a luta daqueles que ainda são colocados à margem do capitalismo racista.

REFERÊNCIAS

A NOVA DEMOCRACIA. Final da Copa das Confederações é marcada por violentos protestos, ano XII, nº 113, 2ª quinzena de julho de 2013. Disponível em: <http://www.anovademocracia.com.br/no-113/4818-final-da-copa-das-confederacoes--e-marcada-por-violentos-protestos>. Acesso em: 23 ago. 2017.

BONDE NEWS. Manifestação anti-Copa termina em vandalismo em Curitiba. Disponível em: <http://www.bonde.com.br/?id_bonde=1=3--554-20140616-&tit-manifestacao+anticopa+termina+em+vandalismo+em+curitiba+veja+fotos)>. Acesso em: 23 ago. 2017.

BRAZIL, Hugo Leonardo Salgado. Megaeventos e segregação socioespacial: Olímpiadas 2016 no Rio de Janeiro, 2011. Disponível em: <http://www.itr.ufrrj.br/portal/wp-content/uploads/biblioteca/tcc/T57.pdf1111>. Acesso em: 23 ago. 2017.

CGN. Manifestantes iniciam quebra-quebra em ruas do centro do centro de Curitiba. Disponível em: <http://cgn.uol.com.br/noticia/95049/manifestantes-iniciam-quebra-quebra-em-ruas-do-centro-de-curitiba>. Acesso em: 23 ago. 2017.

FOLHA DA REGIÃO. Os manifestos pacíficos e estragos dos baderneiros mascarados. Disponível em: <http://www.folhadaregiao.com.br/Materia.php?id=320780>. Acesso em: 23 ago. 2017.

FOLHA DE SÃO PAULO. Protestos terminam com confronto e atos de vandalismo no Rio e SP. Publicado em 16 de outubro de 2013. Disponível em: <http://www1.folha.uol.com.br/cotidiano/2013/10/1357278-protestos-terminam-com--confronto-e-atos-de-vandalismo-no-rio-e-sp.shtml>. Acesso em: 23 ago. 2017.

G1. Dono de loja depredada em protesto no Rio chora e desabafa: maldade. Disponível em: <http://g1-globocom.jusbrasil.com.br/noticias/100611388/dono-de-loja-depredada-em-protesto-no-rio-chora-e-desabafa-maldade>. Acesso em: 23 ago. 2017.

HARVEY, David. A liberdade da cidade. In: MARICATO, Erminia et al. (Orgs.) *Cidades Rebeldes*: Passe Livre e as manifestações que tomaram as ruas do Brasil. São Paulo: Boitempo; Carta Maior, 2013. p. 27-34.

IASI, Mauro Luis. A rebelião, a cidade e a consciência. In: MARICATO, Erminia *et al*. (Orgs.) *Cidades Rebeldes:* Passe Livre e as manifestações que tomaram as ruas do Brasil. São Paulo: Boitempo; Carta Maior, 2013. p. 41-46.

JORNAL DA BAND. Sexto protesto termina em vandalismo em SP. Disponível em: <http://noticias.band.uol.com.br/cidades/noticia/?id=100000607452>. Acesso em: 23 ago. 2017.

JORNAL EXTRA. Um morador morre e outros dois ficam feridos após confronto com a polícia na UPP do Jacarezinho. Disponível em: <http://extra.globo.com/casos-de-policia/um-morador-morre-outros-dois-ficam-feridos-apos-confronto-com-policia-na-upp-do-jacarezinho-8033173.html>. Acesso em: 23 ago. 2017.

JORNAL NACIONAL. Manifestação em SP contra os gastos da Copa termina em vandalismo e com feridos. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2014/05/manifestacao-em-sp-contra-os-gastos-da-copa-termina-em-vandalismo-e-com-feridos.html>. Acesso em: 23 ago. 2017.

JUSTIÇA GLOBAL *et al.* Carta ao Comitê sobre os direitos da criança da ONU. Disponível em: <http://www.global.org.br/wp-content/uploads/2016/03/CARTA-AO-COMITE_PORTUGUES.pdf>. Acesso em: 23 ago. 2017.

JUSTIÇA GLOBAL. A invisibilização da pobreza e dos pobres no Rio Olímpico, 2013. Disponível em: <http://www.global.org.br/blog/a-invisibilizacao-da-pobreza-e-dos-pobres-no-rio-olimpico/>. Acesso em: 23 ago. 2017.

LISBOA, Victor. Quem protestar na Copa pode ser terrorista. Disponível em: <http://papodehomem.com.br/quem-protestar-na-copa-pode-ser-terrorista>. Acesso em: 23 ago. 2017.

MARINHO, Glaucia; CAMPAGNANI, Mario; COSENTINO, Renato. Brasil. In: PAULA, Marilene de; BARTEL, Dawid Danilo (Orgs.). *Copa para quem?*: um olhar sobre o legado dos Mundiais no Brasil, África do Sul e Alemanha Rio de Janeiro: Fundação Böll, abril de 2014.

PCERJ. Registro de Ocorrência nº 012-09784/2013.

RÁDIO ITAPERUNA FM. Protestos contra Sérgio Cabral termina em vandalismo e nem RAMOS, Silvia; MUSUMECI, Leonarda. *Elemento suspeito:* abordagem policial e discriminação na cidade do Rio de Janeiro. Rio de Janeiro: Civilização Brasileira; CESeC, 2005.

Rede Globo escapa. Disponível em: <http://radioitaperunafm.com/site/2013/07/18/protestos-contra-sergio-cabral-termina-em-vandalismo-e-nem-rede-globo-escapa/>. Acesso em: 23 ago. 2017.

ROCHA, João Manuel. Protesto pacífico em São Paulo termina com vandalismo. Disponível em: <https://www.publico.pt/mundo/noticia/protesto-pacifico-em-sao-paulo-termina-com-vandalismo-1601813>. Acesso em: 23 ago. 2017.

SANTOS, Carolina Camara Pires dos. A raça do gênero?: As guerreiras da estradinha e a luta pelo direito à moradia adequada, 2014. Disponível em: <https://www.maxwell.vrac.puc-rio.br/Busca_etds.php?strSecao=resultado&nrSeq=22480@1>. Acesso em: 23 ago. 2017.

TERRA. RJ: Policia usará Lei de Organização Criminosa contra detidos por Vandalismo. Publicado em 8 de outubro de 2013. Disponível em: <http://noticias.terra.com.br/brasil/policia/rj-policia-usara-lei-de-organizacao-criminosa-contra-detidos-por-vandalismo,8e9b11028b991410VgnCLD2000000ec6eb0aRCRD.html>. Acesso em: 23 ago. 2017.

TJRJ. Processo nº 0361545392013.8.19.0001.

TV UOL. Ato em Brasília começa pacífico, mas termina em vandalismo. Disponível em: <http://tvuol.uol.com.br/video/ato-em-brasilia-comeca-pacifico-mas-termina-em-vandalismo-04024D1B3468D8A94326/>. Acesso em: 23 ago. 2017.

UOL NOTÍCIAS. Mascarados bloqueiam um dos sentidos da avenida paulista em SP. Disponível em: <http://noticias.uol.com.br/cotidiano/ultimas-noticias/2013/11/05/mascarados-bloqueiam-um-dos-sentidos-da-avenida-paulista-em-sp.htm>. Acesso em: 23 ago. 2017.

UOL. Para chefe da polícia civil do Rio endurecimento da lei aumentou o número de presos em protestos. Disponível em: <http://noticias.uol.com.br/cotidiano/ultimas-noticias/2013/10/16/para-chefe-da-policia-civil-do-rio-endurecimento-da-lei-aumentou-numero-de-presos-em-protestos.htm>. Acesso em: 23 ago. 2017.

URIBE, Gustavo. Manifestação contra a Copa termina em violência em São Paulo. Publicado em 25 de janeiro de 2014. Disponível em: <http://oglobo.globo.com/brasil/manifestacao-contra-copa-termina-em-violencia-em-sao-paulo-11405725>. Acesso em: 23 ago. 2017.

WACQUANT, Loïc. *As prisões da miséria.* Tradução André Telles. 2. ed. Rio de Janeiro: Zahar, 2011.

YOUTUBE. Policiais da UPP atiram para matar no Jacarezinho. Disponível em: <https://www.youtube.com/watch?feature=player_embedded&v=PAAvYFG7Hjc>. Acesso em: 23 ago. 2017.

ZH Notícias. Protesto que começou pacífico novamente termina em vandalismo, saques e prisões em Porto Alegre. Disponível em: <http://zh.clicrbs.com.br/rs/noticias/noticia/2013/06/protesto-que-comecou-pacifico-novamente-termina-em-vandalismo-saques-e-prisoes-em-porto-alegre-4180377.html>. Acesso em: 23 ago. 2017.

A CIDADE INSTANTÂNEA NO FUTURO MAIS QUENTE E INCERTO

NATALIE UNTERSTELL

INTRODUÇÃO

Já há inúmeros centros urbanos que tentam funcionar de "modo conectado" e que recebem a alcunha de "cidades inteligentes" por se mostrarem sensíveis a produzir, consumir e distribuir um grande número de informações em tempo real. Segundo Gaspar, Azevedo e Teixeira, "o modelo de cidade inteligente vem com a proposta de monitorar e integrar as condições de operação das infraestruturas críticas da cidade, atuando de forma preventiva para a continuidade de suas atividades essenciais, melhorando as condições de serviços e a qualidade de vida dos cidadãos".[1]

Em geral, essas cidades agregam três capacidades novas ao seu portfólio tradicional de gestão municipal: a automação, que libera recursos de tarefas repetitivas para outras e pode eliminar a necessidade de envolvimento humano em atividades perigosas; a customização dos serviços e das interações com os cidadãos; e a predição e prevenção, que permite que governos intervenham e previnam problemas antes deles ocorrerem.[2] A governança das cidades inteligentes não é o foco deste artigo – de todo modo, ressalta-se aqui que ela é fundamental ao processo de aprendizado e de regulação das novas funcionalidades da "cidade instantânea". Requer-se que os governos criem e em alguns casos antecipem regras e políticas para lidar com essa "inteligência", como a da vigilância de dados, além de enfrentar gargalos até então não conhecidos.

1 Cf.: CIKI. Análise do ranking connected smart cities. Disponível em <http://via.ufsc.br/wp-content/uploads/2016/12/ANÁLISE-DO-RANKING-CONNECTED-SMART-CITIES.pdf>. Acesso em: 11 ago. 2017.

2 Cf.: WORLD GOVERNMENT SUMMIT. Advanced science and the future of government. Disponível em: <https://worldgovernmentsummit.org/api/publications/document/fae769c4-e97c-6578-b2f8-ff0000a7ddb6>. Acesso em: 11 ago. 2017.

Nessas cidades as informações, os dados e as ideias são compartilhados por diferentes atores da comunidade, do setor público e do setor privado em modo instantâneo. As cidades inteligentes têm o potencial de contribuir para que o poder público reconheça problemas e de oferecer um papel novo ao cidadão quanto a produzir informações, auxiliando a mapear, discutir e enfrentar essas dificuldades, ambos em tempo real.[3] Embora aplicações pontuais apresentem efeitos interessantes, por exemplo, na eficiência de se reduzir o volume de tráfego durante os horários de pico ou na redução do consumo energético através de sensores de iluminação pública, é a composição de dados em tempo real com desempenho de rede e comportamento dos usuários que permite que as cidades inteligentes atuem orquestrando dados e melhorando gradualmente as percepções algorítmicas. Estimativas indicam que em 2020 haverá mais de 24 milhões de "coisas" conectadas em uso nas cidades.[4] Edifícios comerciais e veículos inteligentes serão os principais contribuintes para isso, representando 58 por cento dos todas as "coisas" instaladas e conectadas em rede.[5]

A inteligência das cidades é também incremental: quanto mais dados são tornados públicos e quanto mais "coisas" atuam conectadas em rede, mais aprendizado coletivo fica a serviço da população. A gestão "instantânea" da cidade tem o potencial de aproximar os cidadãos e os serviços, de modo que as expectativas, os comportamentos e os investimentos públicos sejam transformados em uma mesma direção.

Mas a inteligência das cidades precisa ir além da conectividade: os responsáveis pela elaboração de políticas devem considerar os US$ 350 trilhões em gastos globais com construção, operação e manutenção de infraestrutura urbana projetados para os próximos 30 anos como uma oportunidade para que suas cidades se tornem investidoras em soluções transformadoras – e, por extensão, mais resilientes e sustentáveis.

---

3 Cf.: CIKI. Análise do ranking connected smart cities. Disponível em: <http://via.ufsc.br/wp-content/uploads/2016/12/ANÁLISE-DO-RANKING-CONNECTED-SMART-CITIES.pdf>. Acesso em: 11 ago. 2017.

4 Cf.: SPECTRUM. Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. Disponível em: <http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>. Acesso em: 11 ago. 2017.

5 CF.: BUSINESS INSIDER. Here's how the Internet of Things will explode by 2020. Disponível em: <http://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2>. Acesso em: 11 ago. 2017.

Nesse sentido, apresento a seguir três situações em que as cidades buscam expandir sua conectividade e, por conseguinte, sua inteligência, mostrando algumas das limitações e oportunidades presentes nesses casos. A apresentação desses casos está em linha com o conceito de evolução ou maturação das cidades inteligentes ao longo de um "processo" ou "jornada", desenvolvido e aplicado por diferentes organizações.[6] [7]

CADA COISA EM SEU LUGAR

A cidade de Detroit, nos Estados Unidos, perdeu cerca de 70% dos seus habitantes em função da recessão econômica dos anos 2000, que atingiu em cheio sua indústria automotiva. Incapaz de lidar com o desemprego de dois dígitos, com uma das maiores taxas de criminalidade dos Estados Unidos e dado o abandono da cidade já esvaziada, Detroit declarou falência em 2013. Quando assumiu como prefeito em 2014, Mike Dugan tinha de enfrentar esse quadro de falha total. Ele resolveu começar pelo básico: acertar os semáforos das ruas, fazendo com que eles estivessem ligados e sincronizados. Esse gesto deu aos cidadãos um sinal simples, direto e claro: a cidade voltaria a funcionar.

Quase dezesseis meses depois que Detroit declarou a maior falência municipal da história dos Estados Unidos, um juiz federal aprovou um plano para reduzir os US $ 7 bilhões da dívida da cidade e investir mais de US $ 1 bilhão em serviços públicos ao longo de 10 anos. Um dos passos seguintes foi investir em um plano de iluminação inteligente, que não só deu oportunidade para economia de recursos – estima-se quase US $ 3 milhões em contas de energia elétrica do município – como desencorajou a criminalidade – mais iluminação e menos violência – e reduziu a necessidade de manutenção da rede – a fiação deixou de ser feita de cobre e passou a ser de alumínio, de menor valor de mercado.

Detroit ilustra alguns aspectos interessantes para se pensar o direito à cidade: suas "coisas" são "ativas", há planos "coletivos" e as autoridades tomam decisões das mais simples as mais difíceis de modo transparente. Detroit organizou as "coisas" básicas, incrementou ao longo do tempo sua capacidade de servir e guiou-se por uma visão de longo prazo produzida coletivamente e legitimidade por uma eleição.

---

6 Cf.: URBAN TIDE. Overview of the Smart Cities Maturity Model. Disponível em: <https://static1.squarespace.com/static/5527ba84e4b09a3d0e89e14d/t/55aebffce4b0f8960472ef49/1437515772651/UT_Smart_Model_FINAL.pdf>. Acesso em: 11 ago. 2017.

7 Ver: MEETING OF THE MINDS. Evolving Smart City Approaches: Path and Journey. Disponível em: <http://meetingoftheminds.org/evolving-smart-city-approaches-path-and-journey-14087>. Acesso em: 11 ago. 2017.

Organizar as "coisas" básicas da cidade é uma motivação importante ao desenvolvimento e no uso de aplicativos digitais que permitem que cidadãos conectados indiquem problemas na cidade, avaliem serviços públicos e proponham soluções. Do ponto de vista do cidadão, diversos aplicativos servem a esse propósito: de mapeamento de buracos nas ruas à avaliação da gestão. Do ponto de vista de governo, Cingapura, por exemplo, está analisando enormes quantidades de dados anônimos de geolocalização de telefones celulares para ajudar a identificar áreas ocupadas, rotas populares de tráfego e pontos de almoço e usar essas informações para fazer recomendações sobre onde construir novas escolas, hospitais, ciclovias e rotas de ônibus. Para conseguir avançar com esse propósito, Cingapura tinha já um nível de organização municipal bastante alto.

Não está claro se a inteligência de dados serve apenas a cidades já competitivas, como Cingapura. O caso de Detroit ilustra que, a partir de um determinado nível de organização das "coisas" básicas, pode ser viável e de interesse para as cidades considerarem a implementação de tecnologias e análise de dados.

LUGARES EM QUE NÃO HÁ COISAS

Stephen Goldsmith e Susan Crawford no livro *The Responsive City* defendem que o futuro está nas cidades que partilham seus rumos permanentemente com os seus cidadãos. Em 2050, projeta-se que um terço da população mundial viverá em favelas, segundo a Organização das Nações Unidas. Para que as cidades inteligentes deem conta dessa realidade, ferramentas digitais devem ser úteis para todos os cidadãos das cidades. Para tanto, as cidades inteligentes dependem tanto de um espalhamento das "coisas" na sua geografia e no aprimoramento da democracia.

Hoje, há pouca integração entre iniciativas de digitalização nas favelas e sistemas de cidades inteligentes. Esse é o caso do Rio de Janeiro, em que um centro de excelência foi criado para prevenção, monitoramento e resposta que atuou em diversos megaeventos, como a Copa do Mundo e as Olimpíadas; mas o raio de alcance da inteligência urbana é limitado nas fronteiras entre "asfalto e favela".

Único exemplo brasileiro citado no livro *The Responsive City* – este que é considerado como referência maior sobre governança de dados e cidades inteligentes na literatura internacional, a Ágora Digital, na favela do Morro do Vidigal, reunia espaço público, integração urbana e sustentabilidade, em um antigo depósito de lixo que foi transformado em agrofloresta pela comunidade da favela. A Ágora Digital oferecia um espaço digital e físico

para os moradores da comunidade reivindicarem seu lugar na tomada de decisões da cidade e para experimentarem novas abordagens de urbanização. A Ágora Digital tinha como proposta trazer para o tempo da decisão política de hoje os dados históricos e também projeções futuras, para se formularem propostas de arquitetura inteligente na comunidade. Com uso de sensores, projetava-se o mapeamento dos canais de drenagem e saneamento do morro, até então desconhecidos. Independentemente do poder público, a Ágora Digital e outros agentes de interesse público forçaram a favela e a cidade para o campo da inteligência, mesmo que não integrados ainda a um sistema maior.

De acordo com Goldsmith e Crawford (2014), havia na Ágora Digital, feita de baixo para cima, grande contraste com o Centro de Operações do Rio de Janeiro, feito de cima para baixo, segundo eles. "As telas exibem informações de 560 câmeras, um sistema de previsão meteorológica e várias camadas de dados coletados de sensores colocados ao redor da cidade", menciona o livro, enquanto "o Morro do Vidigal ainda não tem um mapa físico da comunidade" (GOLDSMITH; CRAWFORD, 2014).

Se, por um lado, a iniciativa na favela passava à inclusão de áreas além do domínio do Estado no mapa da cidade e na rede virtual, ela pretendia se valer das mesmas ferramentas da cidade inteligente – sensores, etc. – para resolver problemas da comunidade. Seria como uma "favela inteligente", mas por algum tempo desconectada do todo da "cidade inteligente".

Em função do arrefecimento da violência urbana pós-Olimpíadas de 2016, a Ágora Digital foi descontinuada. Houve a expulsão de alguns de seus co-fundadores por operadores do tráfico no Morro do Vidigal, indicando que a governança baseada em dados ainda não dá conta da complexidade política das cidades.

Nessa situação apresentada, a organização tecnológica depende fundamentalmente da organização social e política da cidade. As "coisas" podem ajudar a conectar essas organizações, mas o caso demonstra que o Rio de Janeiro foi uma cidade inteligente para alguns, não para todos, até o momento.

ONDE AS COISAS AJUDAM, MAS NÃO RESOLVEM OS PROBLEMAS PÚBLICOS POR SI SÓ

Há um número crescente de exemplos de aplicação da Internet das Coisas às cidades que otimizam a identificação dos problemas urbanos. Os exemplos aqui citados foram extraídos do relatório Ciência Avançada e o Futuro dos Governos, desenvolvido pela The Economist Inteligence

Unit para o governo dos Emirados Árabes Unidos em 2016, por ocasião da realização da Cúpula Mundial sobre Governos.[8]

Em Hong Kong, algoritmos são usados para agendar os 2.600 trabalhos de reparação do metrô que ocorrem toda semana. O trabalho de reparo ainda é realizado por seres humanos. Os robôs realizam o agendamento identificando oportunidades para combinar diferentes reparos e critérios de avaliação, como os regulamentos locais de ruído. Hoje, o metrô tem um registro de 99,9% de serviços no horário – muito à frente de Londres ou Nova York.

No Reino Unido, está se desenvolvendo um programa para criar cidades "auto-reparadoras", onde pequenos robôs identificam e consertam tudo, desde buracos, calçadas e tubulações. Apesar do nome atraente, os robôs de curto prazo provavelmente serão mais úteis para monitorar e avaliar a infraestrutura em vez de repará-la, dada a destreza que se requer para lidar com a cidade.

Na China, uma ferramenta está sendo testada para avaliar a gravidade da poluição do ar com 72 horas de antecedência e com 30% mais precisão do que as abordagens convencionais. O objetivo é dar às autoridades mais tempo para intervir – por exemplo, restringindo ou desviando o tráfego, ou mesmo fechando temporariamente fábricas alimentadas a carvão. Naquele país, a poluição do ar contribui para 1,6 milhão de mortes a cada ano – um sexto da mortalidade total. Em um determinado dia, a gravidade da poluição depende de vários fatores, incluindo a temperatura, a velocidade do vento, o tráfego e a qualidade do ar do dia anterior.

Nos Estados Unidos, o Estado da Califórnia vem testando a previsão de quais áreas serão as mais afetadas por terremotos. Quando os primeiros sinais de um terremoto são identificados, combinam-se dados sobre a idade e os materiais de construção dos edifícios com dados sísmicos, de modo que os recursos de emergência podem ser direcionados para áreas-chave.

Todos esses casos demonstram o poder de previsão e de prevenção a ser aproveitado pelas cidades com base nas informações advindas de sensores, automação e outros. Porém, "prever" não deve ser confundido com "resolver". Prever o crime, o fogo ou as ondas de tempestade demanda ainda intervenção humana para pará-los ou gerenciá-los. A resolução das causas dos problemas tratados está além da inteligência artificial aplicada às cidades, até o momento.

---

8 Cf.: WORLD GOVERNMENT SUMMIT. Advanced science and the future of government. Disponível em: <https://worldgovernmentsummit.org/api/publications/document/fae769c4-e97c-6578-b2f8-ff0000a7ddb6>. Acesso em: 11 ago. 2017.

AS COISAS ERRADAS NO LUGAR ERRADO

As cidades sofrerão adiante mais e mais "choques" em função da mudança global do clima. Os impactos climáticos poderão ser de progresso lento, como o aumento do nível do mar em cidades costeiras, ou eventos extremos, como inundações e ondas de calor.

Grandes cidades costeiras possuem ativos no valor de bilhões de dólares dentro de zonas que podem sofrer inundações regulares até o final do século, se não antes. Miami e o Rio de Janeiro são algumas dessas cidades e podem aprender com a destruição causada por tempestades recentes, que custaram bilhões em danos à propriedade e perda de produtividade.

Nas próximas décadas, os impactos da mudança climática tornar-se-ão mais evidentes.[9] Para áreas baixas, como a Baixada Fluminense, a probabilidade de inundações substanciais aumentará cada década para o futuro. Planejar o futuro desde uma perspectiva histórica subestima seriamente os riscos.[10]

O Condado de Miami-Dade, na Flórida, Estados Unidos, foi o primeiro município a lançar um Centro de Operações Inteligentes da companhia AT&T em 2017. O programa piloto visa dar ao governo visibilidade das condições de sua comunidade em tempo quase real. A iluminação inteligente e o transporte inteligente são as principais vertentes da iniciativa *smart cities* em Miami-Dade. Por outro lado, esse condado é muito vulnerável à elevação do nível do mar - aproximadamente 60% do seu território está a menos de seis pés – 1.80 metro – acima do nível do mar – e a região é propensa a furacões e chuvas intensas. Já existe um investimento público significativo na proteção das vias públicas com relação a ressacas e ao aumento do nível do mar, que se dá, basicamente, pela elevação das calçadas e prédios. Ainda assim, cidadãos processaram o governo do condado em 2011, quando esse propôs realizar investimentos públicos para renovação de infraestrutura de saneamento em uma área notadamente vulnerável ao aumento do nível do mar. Queriam os cidadãos que os recursos públicos fossem aplicados de modo a tornar o sistema de saneamento resiliente ao aumento do nível do mar ou mesmo que não fizesse o investimento, partindo do pressuposto que o mesmo seria perdido no longo prazo se o mar subir conforme as projeções mais pessimistas indicavam. As grandes

9 Ver: <https://www.ipcc.ch/pdf/assessment-report/ar5/wg1/WG1AR5_Chapter13_FINAL.pdf>. Acesso em: 11 ago. 2017.

10 Ver: <https://www.ipcc.ch/pdf/assessment-report/ar5/wg1/WG1AR5_Chapter13_FINAL.pdf>. Acesso em: 11 ago. 2017.

questões colocadas em juízo aos gestores foram: devemos fazer algo? Agora ou mais tarde? Devemos fazer pouco, muito, tudo que for necessário para gerir os riscos climáticos projetados? O condado optou por nada fazer, deixando para o futuro a resolução dessa questão. Foram comprometidos 12 bilhões de dólares para a melhoria do sistema local de saneamento em um período de dez anos, sem quaisquer mudanças no padrão de construção que tome em conta medidas adaptativas à mudança do clima.

Esse caso indica uma situação interessante: um município que busca trabalhar como cidade inteligente, mas que escolhe áreas de trabalho que podem desaparecer ou perder importância no longo prazo, caso seja afetada pelos riscos contemplados pela mudança no clima em uma região tão vulnerável. Como um contrassenso, a cidade busca se tonar mais inteligente com as coisas erradas. Ou, invertendo a frase, buscando as coisas certas para as áreas erradas.

Se em um primeiro momento as melhorias incrementais produzidas em cidades inteligentes poderão economizar alguns quilômetros por litro de combustível ou quilowatts-hora de uso de eletricidade para os cofres públicos, adiante podem se tornar uma ameaça pois tem o potencial negativo de afundar os centros urbanos em infraestruturas insustentáveis e atrasar mudanças críticas nas cidades já sujeitas aos "choques" derivados das mudanças climáticas. Essa pode ser a tendência no caso de Miami-Dade aqui abordado, em que o investimento como *smart city* passou ao largo dos investimentos à prova de riscos futuros.

Logo, que tipo de inteligência a cidade precisaria para considerar riscos como os mencionados, repletos de tantas incertezas? Como aliar a inteligência de dados disponível para alguns serviços para o planejamento e a visão de longo prazo da cidade como um todo? Poderia a cidade inteligente investir melhor, considerando riscos plausíveis como aqueles associados à mudança do clima? Ou esse não é o seu propósito?

AS COISAS CERTAS NO LUGAR CERTO, MAS DESCONECTADAS ENTRE SI

Em outubro de 2016, a Zona Sul do Rio de Janeiro sofreu com uma forte ressaca em sua orla. Houve a invasão metros a fio das avenidas a beira mar por montes de areia, danos aos equipamentos públicos e privados, além do alagamento que tomou diversos veículos de surpresa.

Ainda que um caso rotineiro, ele ilustra como uma cidade inteligente pode agir aquém do necessário ou do esperado na resolução de casos que devem

ganhar força e ocorrer com maior frequência, dado o aumento do nível do mar. Ainda que não se parametrize a intensidade, é possível monitorar com alguma precisão meteorológica a ocorrência desses fenômenos. Se tal tipo de informação fosse consolidada, um sistema inteligente e integrado, como o Centro de Operações do Rio, poderia recebê-la e processá-las junto com os dados de tráfego que já armazena e utiliza.

Um sistema inteligente, via Internet das Coisas, poderia fazer com os que sinais de trânsito fossem coordenados ou mesmo que as ruas sob risco durante uma ressaca sejam fechadas. Eventualmente, ocorreria um problema associado à restrição de tráfego, mas diminuir-se-ia a exposição das pessoas ao risco de afogamento, enxurradas, etc. e evitar-se-iam mortes nos equipamentos – como nas ciclovias – da orla, evitando prejuízos e riscos de outra ordem – como doenças associadas ao tráfego na área de ressaca. Hoje essa integração de dados não ocorre, mesmo em uma cidade onde foi feito um plano e em que se formou uma visão estratégica de longo prazo. A inteligência, nesse caso, está restrita a um conjunto de dados do momento presente, ignorando projeções futuras, as quais mostram todas uma cidade mais quente e com clima menos previsível.

CONCLUSÃO

A digitalização das informações e dos serviços urbanos é o passo mais aparente de como a revolução de dados está se dando nas cidades. O desafio maior de urbanização em tempos de mudança do clima, de aumento da população e de aumento do volume de informação trocada, é que informação instantânea não parece dar conta das necessidades de aumentar a resiliência da vida urbana vibrante. As situações aqui apresentadas buscaram identificar as aplicações e as limitações das abordagens hoje presentes em algumas cidades, demonstrando que a inteligência é ora setorial, ora focada nos dados mais fáceis, ora desintegrados em tempo e em espaço.

REFERÊNCIAS

ALLWINKLE, S.; CRUICKSHANK, P. Creating smarter cities: an overview. *Journal of Urban Technology*, v. 18, v. 2, p. 1-16, 2011.

BUSINESS INSIDER. Here's how the Internet of Things will explode by 2020. Disponível em: <http://www.businessinsider.com/iot-ecosystem-internet-of--things-forecasts-and-business-opportunities-2016-2>. Acesso em: 11 ago. 2017.

CIKI. Análise do ranking connected smart cities. Disponível em: <http://via.ufsc.br/wp-content/uploads/2016/12/ANÁLISE-DO-RANKING-CONNECTED-SMART-CITIES.pdf>. Acesso em: 11 ago. 2017.

CHURCH, J.A. *et al.*, 2013: Sea Level Change. In: STOCKER, T.F., D. Qin, G.-K. PLATTNER, M. Tignor, S.K. ALLEN, J. BOSCHUNG, A. NAUELS, Y. Xia, V. Bex and P. M. Midgley (Eds.). *Climate Change 2013:* The Physical Science Basis. Contribution of Working Group I to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge, United Kingdom; Nova York, USA: Cambridge University Press, [s.d].

CONLIN, Jennifer. Detroit Pushes Back with Young Muscles. The New York Times, 1 jul. 2011. Disponível em: <http://www.nytimes.com/2011/07/03/fashion/the-young-and- entrepreneurial-move-to-downtown-detroit-pushing-its-economic- recovery.html?pagewanted=all>. Acesso em: 11 ago. 2017.

DAVEY, Monica. Looking Up, Detroit Faces a New Crisis. The New York Times, 23 dez. 2011. Disponível em: <http://www.nytimes.com/2011/12/24/us/detroit-budget-crisis-may-lead-to- outside-manager.html?pagewanted=1&_r=1>. Acesso em: 11 ago. 2017.

DAVEY, Monica Mayor Urges Detroit to Accept Drastic Action to Fix Finances. The New York Times, 16 nov. 2011. Disponível em: <http://www.nytimes.com/2011/11/17/us/mayor-bing-tells-detroit-dire-finances- require-drastic-action.html?scp=1&sq=Detroit&st=cse>. Acesso em: 11 ago. 2017.

DOLAN, Matthew. Revival Bid Pits Detroit vs. Donor. The Wall Street Journal, 2 jul. 2011. Disponível em: <http://online.wsj.com/article/SB10001424052702304887904576397760319014524.html>. Acesso em: 11 ago. 2017.

FLEMING, Leonard; NICHOLS, Darren. Kresge Foundation Pledges $150- Million for Detroit Redevelopment. The Detroit News, 10 jan. 2013. Disponível em: <http://www.detroitnews.com/article/20130110/METRO01/301100384>. Acesso em: 11 ago. 2017.

GOLDSMITH, S.; CRAWFORD, S. (2014) *The Responsive City:* Engaging Communities Through Data-Smart Governance. San Francisco, CA: Jossey-Bass, [s.d].

GUARINO, Mark. Former Detroit Mayor Kwame Kilpatrick Faces Major Corruption Charges. Christian Science Monitor, 18 dez. 2010. Disponível em: <http://www.csmonitor.com/USA/Justice/2010/1218/Former-Detroit-mayor- Kwame-Kilpatrick-faces-major-corruption-charges>. Acesso em: 11 ago. 2017.

KUHNHENN, Jim. Taxpayer Loss on Auto Bailout Narrows: White House Touts Value of Emergency Loans to GM, Chrysler, msnbc.com, 1 jun. 2011. Disponível em: <http://www.msnbc.msn.com/id/43242226/ns/business-autos/t/taxpayer-loss--auto- bailout-narrows/#.TsqdOWD9IbU>. Acesso em: 11 ago. 2017.

LEE, H.; UNTERSTELL, N.; THEEL, S.; NEVE, P. Miami Dade and Sea Level Rise. Case Study. Harvard Kennedy School of Government. 2016. Disponível em: <https://case.hks.harvard.edu/miami-dade-county-and-sea-rise/>. Acesso em: 11 ago. 2017.MEETING OF THE MINDS. Evolving Smart City Approaches: Path and Journey. Disponível em: <http://meetingoftheminds.org/evolving-smart-city-approaches-path-and-journey-14087>. Acesso em: 11 ago. 2017.

OKRENT, Daniel. Detroit: the Death (and Possible Life) of a Great City. Time Magazine, 24 set. 2009. Disponível em: <http://www.time.com/time/magazine/article/0,9171,1926017-1,00.html>. Acesso em: 11 ago. 2017.

OKRENT, Daniel. GRAY, Steven. How To Shrink a City. Time Magazine, 11 nov. 2010. Disponível em: <http://www.time.com/time/magazine/article/0,9171,2030898,00.html>. Acesso em: 11 ago. 2017.

OOSTING, Jonathan. Transformation Detroit: Dan Gilbert's Grand Plan for Downtown Tech Hub, Retail and Residential. mlive.com, 23 jun. 2011. Disponível em: <http://www.mlive.com/news/detroit/index.ssf/2011/06/transform_detroit_dan_gilb erts.html>. Acesso em: 11 ago. 2017.

SENGE, Peter; SMITH, Bryan; KRUSCHWITZ, Nina. The Next Industrial Imperative, *s+b*, Summer 2008: Why facing up to climate change requires a revolution in business thinking. Disponível em: <https://www.strategy.business.com/article/08205>. Acesso em: 11 ago. 2017.

SPECTRUM. Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. Disponível em: <http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>. Acesso em: 11 ago. 2017.

THE ECONOMIST. The Parable of Detroit – So Cheap, There's Hope: Having Lost a Quarter of Its Population in a Decade, America's Most Blighted Big City Could Be Turning the Corner. The Economist, 22 out. 2011. Disponível em: http://www.economist.com/node/21533407 Acesso em: 11 ago. 2017.

URBAN TIDE. Overview of the Smart Cities Maturity Model. Disponível em: <https://static1.squarespace.com/static/5527ba84e4b09a3d0e89e14d/t/55aebffce4b-0f8960472ef49/1437515772651/UT_Smart_Model_FINAL.pdf>. Acesso em: 11 ago. 2017.

WONG, P. P. et al., 2014: Coastal systems and low-lying areas. In: Field, C.B., V.R. Barros, D.J. Dokken, K.J. Mach, M.D. Mastrandrea, T.E. Bilir, M. Chatterjee, K.L. Ebi, Y.O. Estrada, R.C. Genova, B. Girma, E.S. Kissel, A.N. Levy, S. MacCracken, P.R. Mastrandrea, and L.L. White (Eds.) *Climate Change 2014*: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge, United Kingdom; Nova York, USA: Cambridge University Press, [s.d], p. 361-409.

WORLD GOVERNMENT SUMMIT. Advanced science and the future of government. Disponível em: <https://worldgovernmentsummit.org/api/publications/document/fae769c4-e97c-6578-b2f8-ff0000a7ddb6>. Acesso em: 11 ago. 2017.

WORLD WIDE FUND FOR NATURE AND BOOZ & COMPANY. Reinventing the City: Three Prerequisites for Greening Urban Infrastructure. Disponível em: <http://assets.panda.org/downloads/wwf_reinventing_the_city_final_3_low_resolution.pdf>. Acesso em: 11 ago. 2017.

II

PRIVACIDADE E PROTEÇÃO DE DADOS

REVISITANDO A #PRIVACIDADE NA @SOCIEDADEDIGITAL

ANDRIEI GUTIERREZ

Na Era Digital, tudo o que é sólido se digitaliza na rede, ou quase tudo. E, uma vez lá, pode ter consequências muito concretas sobre o mundo real. Fotos e filmes pessoais, informações sobre gostos e preferências, hábitos, locais frequentados e toda uma gama de dados pessoais estão sendo digitalizados e inseridos na rede. E podem – de alguma maneira e em algum momento – ter alguma ação sobre nós. Para o bem e para o mal.

A observar pela realidade a nossa volta, não seria exagero afirmar que é só o começo. Essa tendência está a se acentuar. Isso porque, no balanço geral, a percepção das pessoas, empresas e governos é a de que os benefícios da digitalização são maiores do que os riscos. E esse parece ser um caminho sem volta. Uma tendência que veio para ficar.

Como garantir, então, o direito fundamental à privacidade no contexto da rápida digitalização das esferas sociais que, até recentemente, gozavam de relativo grau de proteção? O rápido desenvolvimento movido a dados em uma sociedade capitalista e a proteção à privacidade seriam elementos antagônicos? Antes de avançar para essas e outras indagações que julgo importantes, cabe uma breve contextualização da profundidade e do alcance do que estou chamando de digitalização e de Era Digital.

A ERA DIGITAL PARECE INDICAR UM PROCESSO DE SUPERAÇÃO DA SOCIEDADE INDUSTRIAL

Vivemos uma nova etapa da Revolução Industrial ou as transformações desencadeadas pela digitalização seriam uma outra revolução tão profunda quanto a primeira? Parece ser importante nos questionarmos sobre a real dimensão desse processo que está em curso. E nessa empreitada, creio que valha uma breve digressão sobre algumas das características da Sociedade Industrial, que teve início no final do século XVIII e, grosso modo, tem predominado desde então.

Com a introdução da produção fabril e dos métodos de gestão baseados no taylorismo-fordismo, assistimos a uma revolução sem precedentes em todas as esferas sociais. As relações de trabalho industriais ganharam importância em detrimento das relações agrícolas e artesanais, com a produção industrial em massa superando – embora não excluindo – a produção artesanal. As relações de consumo se massificaram. As profissões se segmentaram e se especializaram de maneiras sem precedente. As relações culturais da crescente massa urbana passaram a ser pautadas pela indústria da cultura de massas. O rádio e, depois, a televisão tornaram-se as expressões máximas dessa indústria cultural. Na esfera política, a democracia representativa ganhou relevância e se manteve mesmo face às aventuras totalitárias do século XX. As guerras entre Estados também se modernizaram junto com os equipamentos e armamentos militares, frutos do engenho científico-industrial.

Hoje, todavia, há pistas suficientes para pensar na existência de um processo – em curso – de superação dessa Sociedade Industrial. A organização industrial predominante – segmentada nas cadeias produtivas – não estaria passando por uma crise de identidade com o avanço da digitalização de produtos e processos e com a introdução das impressoras 3D? Com a emergência de novos processos produtivos, não seria possível pensar no surgimento de um novo tipo de trabalhador da Era Digital, capaz de superar a relevância social do trabalhador industrial, tal como este o fez com o artesão e o trabalhador agrícola? Na esfera cultural, as plataformas sociais digitais não estariam ganhando relevância face à cultura monopolística de massas, que foi marcada no século XX pelo domínio do rádio e da televisão? E no campo político, a crescente participação popular – impulsionada pelas mídias sociais – não estaria colocando na ordem do dia a reforma do tradicional modelo de democracia representativa baseado no programa eleitoral ratificado de quatro a quatro anos pelo sufrágio popular? Na esfera militar, a guerra cibernética não estaria a preocupar Estados tanto ou até mais que os métodos tradicionais de guerra?

Embora essa comparação seja um exercício instigante, não é o propósito deste ensaio. Vale a reflexão de que se trata de um processo que está em curso e que indica ter profundos impactos que vão muito além do nosso objeto deste ensaio.

A SOCIEDADE DIGITAL NÃO NASCE NO VÁCUO, MAS É CONSTRUÍDA A PARTIR DOS PILARES DA SOCIEDADE INDUSTRIAL

Se a hipótese está correta, a experiência histórica mostra que esse tipo de transição social não se dá sem conflitos. Novos padrões se chocando com os predominantes. Novos modelos de relações sociais – de trabalho, de negócios, de consumo, de gestão, culturais – conflitando antagonicamente com os padrões dominantes.

E são assertivas as pistas que temos para afirmar que passamos por um momento de adaptação e transição social que está sedimentando os pilares que fundamentarão a futura Sociedade Digital. E, acredito, a solidez e longevidade desses pilares dependerão da maneira como esse processo será conduzido.

No momento em que este ensaio é escrito, debate-se na Câmara e no Senado a criação de um arcabouço legal específico para a proteção dos dados pessoais. Essa discussão é pertinente e relevante para que se estabeleça os limites do tratamento[1] de dados pessoais aplicados a empresas, governos, universidades e organizações da sociedade civil em uma sociedade que se digitaliza rapidamente. O desafio, todavia, é o de garantir o direito fundamental à privacidade – até então parcialmente resguardado na sociedade *off-line* – agora na Sociedade Digital. E para tanto, entendo que é preciso olhar com as lentes da nova realidade social que está a se configurar.

E aqui volto ao objeto deste ensaio. Como tratar a privacidade no contexto de transição para a Sociedade Digital? Longe de querer esgotar esse debate, apresento abaixo alguns elementos que considero possam contribuir para essa discussão.

OS DADOS ESTÃO PROGRESSIVAMENTE SE TORNANDO O MOTOR DO DESENVOLVIMENTO ECONÔMICO E SOCIAL

Necessitamos avançar o entendimento de que a sociedade brasileira caminha rapidamente para a sensorização e a digitalização não só de informações pessoais, mas de boa parte do desenvolvimento e da organização da vida social. Do tratamento desses dados, por exemplo, dependerá a melhoria da mobilidade urbana, do sistema educacional, do sistema de saúde e das pesquisas e combate a doenças. É importante entender essa dimensão social dos dados que vai muito além da criação de novos modelos de negócios e novos produtos para consumo.[2]

1 Usamos a expressão tratamento de dados de modo genérico, compreendendo também atividades como a coleta, processamento, armazenamento e transferência de dados.

2 A Campanha pública Brasil, País Digital, iniciativa multissetorial liderada pela Associação Brasileira das Empresas de Software (ABES), surgiu com esse propósito de mostrar como que os dados estão revolucionando a sociedade brasileira e como seus benefícios já se estendem a diferentes setores – educação, saúde, agricultura, mobilidade urbana, democracia, entre outros. Cf.: PAÍS DIGITAL. Disponível em: <www.brasilpaisdigital.com.br>. Acesso em: 14 dez. 2018.

Tal como o petróleo foi o recurso natural mais importante do século XX, os dados estão se tornando rapidamente o recurso natural do novo século. Mas, da mesma maneira que o óleo cru que precisa ser extraído e processado, os dados também necessitam ser coletados e tratados do seu estado bruto para gerarem valor econômico e social.

Por isso, é importante que se tenha uma discussão madura e aprofundada acerca da definição do que são dados pessoais e da possibilidade do tratamento de dados anônimos. Uma visão idílica dos dados pessoais e do controle absoluto do indivíduo sobre seus dados pode atrasar e dificultar o desenvolvimento econômico e social do país.

Olhar o debate sobre proteção de dados pessoais com as lentes da privacidade da Sociedade Industrial seria um ledo engano. E aqui, reside uma vantagem de o Brasil entrar tardiamente nessa discussão. Enquanto mais de 100 países possuem legislações de proteção de dados pessoais voltadas para sociedades industriais, temos a oportunidade de construir um arcabouço jurídico novo, moderno, que permita o desenvolvimento da Sociedade Digital.

É PRECISO REVISITAR O CONCEITO DE PRIVACIDADE DO SÉCULO XXI

Para discutirmos os limites ao tratamento de dados pessoais é necessário que a nossa sociedade faça o exercício de repensar o conceito de privacidade no século XXI à luz das transformações econômico-sociais que estão a ocorrer.

E entendo que esse trabalho vai além do escopo deste ensaio. Uma baliza que talvez possa ajudar nessa reflexão, é a constatação de que não é possível – se é que o foi um dia – trabalhar com o conceito de risco zero. Isso porque uma vez que uma informação – seja ela uma foto ou uma impressão digital de um dedo, por exemplo –, é digitalizada e introduzida na rede sempre correrá certo risco de vazar – seja por razões tecnológicas ou humanas. Tal como um objeto precioso que pode ser roubado de um cofre-forte de um banco, uma informação pode ser retirada ou desviada do seu local de armazenamento, físico ou virtual. A diferença reside no grau do risco e na velocidade e intensidade com que essa nova situação pode impactar o titular dos dados. Isso é um fato novo que, queiramos ou não, precisamos entender e trabalhar para que seus eventuais impactos sejam reduzidos e mitigados.

Bloquear legalmente o tratamento anônimo ou ter uma definição muito ampla de dados pessoais não parece ser o melhor – e mais eficiente – caminho para a proteção da privacidade na Sociedade Digital. Quando aumen-

taram os acidentes e mortes no trânsito, por exemplo, em decorrência do aumento do fluxo de veículos no Século XX, a solução não foi a sua proibição. Ao invés disso, a sociedade criou convenções para o trânsito – como sentidos obrigatórios, faixas de pedestres, limites de velocidades e placas informativas – e adaptamos os veículos para reduzirem o impacto nos seres humanos – cintos de segurança, motores na dianteira, para-choques flexíveis, *airbags,* freios ABS. De modo similar, o debate sobre a proteção de dados pessoais também deveria se focar em como podemos reduzir os riscos e mitigar os efeitos de eventuais vazamentos e usos indevidos dos dados pessoais.

Mesmo tendo sido reduzidos, até hoje ainda existem muitos acidentes e mortes em decorrência do trânsito. Mas nossa sociedade entende que, a despeito do que ainda pode ser feito para reduzir as estatísticas, os seus benefícios ainda são maiores do que os riscos. E parece que a sociedade brasileira já está fazendo sua opção em direção à rápida digitalização. Cabe aos legisladores, tomadores de decisão e formuladores de políticas públicas entenderem esse processo para que possamos garantir a proteção à privacidade de maneira madura, equilibrada e, sobretudo, realista e efetiva.

O MODELO TRADICIONAL DE PROTEÇÃO DE DADOS PESSOAIS BASEADO NO CONSENTIMENTO PRECISA SER REPENSADO

Como mencionei acima, as legislações de proteção de dados pessoais não são um fato novo. Hoje, mais de 100 países já possuem um marco regulatório para tratamento de dados pessoais. As primeiras legislações, a exemplo da diretiva da União Europeia de 1995, se construíram em torno da necessidade de um consentimento prévio e, em certos casos, expresso do titular dos dados autorizando o tratamento. Lá se vão mais de vinte anos e, como vimos acima, muita coisa está mudando. Importar qualquer modelo regulatório, que em sua ampla maioria passam por revisões, parece não ser o melhor caminho face a uma sociedade em rápida transformação.

Na esfera coletiva, estamos reconhecendo a importância dos dados para o progresso da sociedade e a geração de inovação social. Cidades mais inteligentes, sustentáveis e humanas dependem do entendimento de como massas de indivíduos se comportam. A melhoria da mobilidade urbana ou o uso responsável dos recursos hídricos e energéticos são bons exemplos disso, na medida em que se consegue ter uma maior percepção de como os indivíduos estão usando os recursos para propor políticas para sua otimização e uso racional. A coleta e o entendimento desses dados, muitas vezes em tempo real, têm se tornado de suma importância para o interesse coletivo.

Na esfera individual, a emergência dos dispositivos móveis conectados e da chamada Internet das Coisas – IoT na sigla em inglês –, com máquinas e dispositivos que se comunicam autonomamente, colocam muitas questões sobre o mecanismo tradicional de proteção de dados pessoais baseado no consentimento. Pequenos dispositivos podem ser conectados ou implantados no nosso corpo para monitorar sinais vitais e, assim, ajudar na prevenção de doenças e na melhoria da qualidade de vida. Hoje, por exemplo, dados como esses são processados por computadores e algoritmos de alta performance, como a inteligência artificial, que conseguem prever uma hipoglicemia[3] com algumas horas de antecedência sem que ocorra qualquer intervenção humana. A indústria farmacêutica também está se revolucionando. Medicamentos já começam a ter suas doses "calibradas" individualmente a partir das necessidades e do desenvolvimento do paciente, medidos por sensores corporais em tempo real.[4]

Neste sentido, é preciso reconhecer outras modalidades de legitimação do tratamento de dados pessoais além do consentimento. Na era da Internet das Coisas, a aceitação da existência de um *consentimento implícito* ou *tácito* poderia ser uma boa alternativa. Há dispositivos que foram desenvolvidos para uma finalidade explícita e o fato de um usuário comprar e instalar o dispositivo em seu corpo, na sua casa, no seu carro, já pressuporia o seu consentimento individual para a coleta e o tratamento para aquela finalidade.

Outra modalidade de exceção ao consentimento é o tratamento de dado baseado no *legítimo interesse* do responsável pelo tratamento.[5] Permitido pela legislação europeia há alguns anos, o legítimo interesse tem se tornado um dos principais meios para que organizações façam tratamento de dados sem que necessariamente precisem coletar o consentimento. Para que se comprove a existência de um legítimo interesse, é preciso que o responsável pelo tratamento faça uma avaliação de equilíbrio – *balance test,* o termo em inglês –, na qual pondere o equilíbrio entre o seu interesse no tratamento e os direitos e liberdades fundamentais do titular dos dados, tendo em vista as expectativas do titular e as relações entre ambos.

---

3 Para mais informações, ver: ENRIQUEZ, Jof. Medtronic Announces Diabetes Partnerships With IBM Watson, Nutrino, Glooko. Disponível em: <https://www.meddeviceonline.com/doc/medtronic-announce-diabetes-partnerships-with-ibm-watson-nutrino-glooko-0001>. Acesso em: 10 mar. 2017.

4 Para mais informações, ver: IBM. Pfizer Taps IBM for Research Collaboration to Transform Parkinson's Disease Care. Disponível em: <https://www-03.ibm.com/press/us/en/pressrelease/49475.wss>. Acesso em: 10 mar. 2017.

5 Chamo a atenção para o detalhe de que o legítimo interesse se refere ao interesse do responsável pelo tratamento e não do titular dos dados.

Importante mencionar que, nessa modalidade, os interesses e direitos fundamentais do titular dos dados podem vir a se sobrepor aos interesses do responsável – e assim inviabilizar a base legal do tratamento – quando dados pessoais são processados em circunstâncias nas quais o titular não espera razoavelmente por tal processamento.

O legítimo interesse tem sido um importante mecanismo para o tratamento de dados pessoais em países que possuem legislações restritas, como é o caso da União Europeia. Segundo levantamento recente feito por um *think tank* global especializado em privacidade[6] com empresas que usam o legítimo interesse para realizar tratamento de dados, algumas das principais categorias têm sido:

- detecção e prevenção de fraude (prevenção de crimes);
- cumprimento de legislações estrangeiras, aplicações legais, requisições judiciais e de órgãos regulatórios;
- segurança da informação, de sistemas e redes;
- processamento de dados de funcionários para motivações que não estão necessariamente vinculadas à execução contratual, como, por exemplo, programas de retenção, gestão de desastres e emergências, operações de contratação *intracompany*, etc.
- desenvolvimento e melhoria de produtos;
- comunicação, *marketing* e inteligência;
- etc.

Os procedimentos para a execução do teste de equilíbrio devem ser claros e bem delimitados em regulamentação de modo que possam ser, em algum momento, verificados e auditados pela Autoridade de Proteção de Dados Pessoais.[7] Nele devem constar, além do interesse do responsável e suas motivações para o tratamento, ponderações sobre a necessidade do mesmo, a proporcionalidade entre dados coletados/finalidade, avaliação do nível do impacto sobre o titular em caso de vazamento de dados, etc.[8]

---

6 Centre for Information Policy Leadership (CIPL). CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data – Discussion Draft. 16 de março de 2017.

7 A criação de uma Autoridade de Proteção de Dados para o contexto brasileiro é um tema de alta relevância. Retomarei esse ponto abaixo.

8 Nesse sentido, vale a leitura do documento "Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC", produzido pelo Article 29 Working Party, conselho independente da União Europeia para temas de proteção de dados pessoais. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Acesso em: 10 jul. 2017.

A CONFIANÇA CONTINUA A SER UM COMPONENTE ESSENCIAL E DEPENDE DE CONTÍNUO E AMPLO COMPROMISSO COM A TRANSPARÊNCIA

O desenvolvimento da rede mundial de computadores nos ensina diariamente a importância da confiança dos participantes para a sua continuidade e longevidade. Neste sentido, e como já mencionado acima, é preciso garantir que a sociedade continue a acreditar na superioridade dos benefícios da Sociedade Digital. Do mesmo modo, é importante que as pessoas confiem no tratamento que é feito com seus dados, que suas expectativas sejam contempladas. E para isso, transparência é essencial.

Talvez esse seja o princípio mais importante que deve fundamentar as práticas em torno da proteção de dados pessoais. Empresas, Governos e organizações que fazem tratamento de dados devem pensar e introduzir processos que evidenciem aos titulares dos dados tratados informações pertinentes para que estes tomem decisões informadas e que, sobretudo, possam avalizar os benefícios, riscos, as condições do tratamento e se oporem a ele.

É necessário, por exemplo, que estejam claros os termos de troca entre provedor e usuário nas relações de oferta de serviços e produtos – sejam eles gratuitos ou não. É preciso regras para que haja divulgação pública dos incidentes envolvendo dados, notificação imediata dos titulares prejudicados juntamente com recomendações para mitigação de riscos. A sociedade precisa saber como o Estado coleta, trata e cuida dos dados dos cidadãos para avalizar se está condizente com as suas expectativas – sejam elas individuais ou coletivas. Este campo é muito vasto e ainda temos toda uma ampla agenda para construir da qual dependerá os pilares de uma Sociedade Digital democrática.

A EFETIVIDADE E A LONGEVIDADE DO MECANISMO DE PROTEÇÃO À PRIVACIDADE PODEM SER MAIORES SE ADOTARMOS UM SISTEMA DE PROTEÇÃO DE DADOS PESSOAIS BASEADO NO TRIPÉ LEGISLAÇÃO PRINCIPIOLÓGICA – AUTORIDADE DE PROTEÇÃO DE DADOS PESSOAIS – PRIORIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

A despeito de existirem diversos países com legislações em vigor para a proteção de dados pessoais, o debate tem sido colocado em algumas mesas como se se tratasse de uma escolha entre dois modelos regulatórios, um americano – mais liberal – e um europeu – mais protetivo. Em um ponto,

talvez, essa dicotomia esteja certa, mais especificamente na existência de duas tradições jurídicas, um anglo-saxônica e outra latina. A primeira, mais enxuta e focada em princípios. A segunda, mais descritiva e prescritiva. Uma parte do pressuposto de que os indivíduos e organizações irão fazer a coisa certa. A outra se adianta aos eventuais comportamentos desviantes e, a partir deles, detalha as medidas cabíveis.

Nossa sociedade está se transformando. E o faz rapidamente. A noção de tempo da sociedade dos nossos filhos muito provavelmente não será a mesma que a nossa. Qual a melhor maneira de proteger a privacidade nesse contexto de rápida mudança conferindo longeva tranquilidade e garantia jurídica tanto para os titulares dos dados quanto para as organizações que tratam esses dados? O longo processo necessário para a construção de legislações na democracia brasileira dificulta e torna morosa a sua eventual revisão. Desse ponto de vista, a solução principiológica parece levar larga vantagem sobre legislações mais descritivas.

Além disso, a velocidade e a tecnicidade com que o tema exige ser tratado não parecem fazer eco na tradicional estrutura jurídica brasileira de proteção dos direitos fundamentais. Os exemplos internacionais de proteção de dados pessoais têm indicado a pertinência da existência de uma autoridade específica para a proteção de dados pessoais – Data Protection Authority, o termo em inglês – para garantir a normatização e execução da lei com a expertise e a velocidade adequadas. Uma entidade autônoma – política, administrativa, financeiramente[9] – parece ser a melhor maneira de proteger a privacidade seja junto às organizações do setor privado e da sociedade civil como junto ao próprio Estado, maior detentor de informações e dados pessoais de toda natureza. Para tanto, torna-se indispensável não somente uma entidade autônoma, mas sobretudo plural. Não somente setores representativos das empresas e do governo deveriam fazer parte de sua instância consultiva. Representantes da sociedade civil e das universidades também deveriam ser incluídos. Dessa maneira, entendo que estaremos construindo uma autoridade mais longeva e alinhada às expectativas e passível de controle social.

Por fim, o terceiro pilar indispensável à proteção da privacidade diz respeito à priorização da segurança da informação. Num mundo no qual as

9 É preciso, todavia, atentar para eventuais conflitos de interesse. Multas e sanções com impactos financeiros que venham a ser aplicadas por essa eventual Autoridade de Proteção de Dados Pessoais jamais deveriam ingressar nos cofres da entidade. Outros usos seriam mais indicados, como o financiamento de pesquisas (pública ou privada) sobre segurança da informação, de campanhas educativas de conscientização popular, etc.

informações pessoais estão sendo rapidamente digitalizadas, armazenadas e sendo transferidas de dispositivo para dispositivo, a segurança da informação deve ser prioridade primeira. Se queremos proteger a privacidade dos nossos cidadãos, a criação de uma legislação e de uma autoridade regulatória/fiscalizatória ainda são insuficientes.

É preciso ir além. E aqui ainda temos todo um campo no qual avançar. Organizações públicas e privadas precisam ter métodos claros de governança da informação. Pesquisa e desenvolvimento de novas tecnologias de segurança da informação – como a criptografia, por exemplo – devem ser estimulados. É necessário avançarmos mais em investimentos na segurança da informação. E para tanto, também será necessário ter em primeiro plano a formação e capacitação de profissionais na área.

Enfim, somente a legislação não basta para proteger a privacidade. É necessário adotarmos uma abordagem sistêmica, contemplando uma legislação atenta à velocidade da Sociedade Digital e suas transformações, uma efetiva Autoridade de Proteção de Dados Pessoais e o enraizamento social de práticas efetivas de segurança da informação.

OS DADOS SÃO *CROSS-BORDER BY DESIGN* E DO SEU LIVRE FLUXO DEPENDE A INOVAÇÃO GLOBAL

É um equívoco acreditar que medidas unilaterais de localização forçada de dados em um território nacional sejam a maneira mais eficiente para garantir a sua segurança. Os avanços recentes das técnicas de encriptação de dados e da tecnologia *blockchain,*[10] por exemplo, têm de longe evidenciado sua superioridade e eficácia na proteção de informações sensíveis.

Aprendemos com a própria arquitetura da internet, aberta e global, que o desenvolvimento no século XXI está indissoluvelmente ligado ao livre fluxo dos dados. Grande parte dos serviços e do comércio global não seria possível sem essa livre movimentação dos dados.[11]

10 A tecnologia *blockchain* permite que informações de uma determinada rede possam ser compartilhadas de maneira criptografada e de modo descentralizado entre diversos servidores (nós) da rede, garantindo assim a sua segurança e confiabilidade. A IBM tem trabalhado e avançado propostas inovadoras de redes em *blockchain* globalmente, entre governos, empresas e organizações. Para mais informações vale uma visita ao sítio <https://www.ibm.com/blockchain/>.

11 Nesse sentido vale a leitura do estudo *Digital Globalization: the new era of global flows*, do Mackinsey Global Institute, de março de 2016. Disponível em: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>. Acesso em: 10 jul. 2017.

Defender sua manutenção significa seguir no caminho do desenvolvimento sustentável global baseado na economia de serviços, geradora de riqueza e prosperidade para os povos. Nesse contexto, o estímulo de boas práticas para a proteção de dados pessoais deve ser objeto de esforços multilaterais ou pluriregionais.

Um bom exemplo é a iniciativa do fórum da Cooperação Econômica Ásia-Pacífico – APEC, a sigla em inglês – para permitir transferência de dados transfronteiriças. Esse esforço pluriregional criou um conjunto de códigos de conduta tanto para responsáveis por tratamento de dados – *data controlers*, termo em inglês –, quanto para organizações que prestam serviços apenas na camada do tratamento de dados – *data processors*.[12] Também estabeleceu entidades independentes para avaliar e certificar organizações para trafegarem dados entre os 21 países membros da APEC. Esse sistema tem se mostrado o método mais eficiente para buscar boas práticas na transferência internacional sem necessariamente bloquear o fluxo de dados.

PRECISAMOS ACELERAR A CURVA DE FORMAÇÃO DO CIDADÃO DIGITAL

Parece ser sensato pensar que está em curso a formação de um cidadão digital. Um cidadão que se informa rapidamente, que monitora e cobra melhorias na interação com o poder público e com o setor privado. Um cidadão que, no Brasil, desde os massivos protestos de 2013, vem construindo sucessivas e representativas manifestações públicas. E não são poucos os exemplos. Em 2013, foram os protestos contra "Os 20 Centavos" de aumento do transporte público de São Paulo, que se desdobraram em cobranças por melhorias nos sistemas de saúde e educação. Em 2014, foram as fervorosas divergências políticas durante as eleições presidenciais. Em 2015, foram os embates em torno do processo de *impeachment* da Presidente Dilma Rousseff. E, mais recentemente, as manifestações em torno das atividades da Operação Lava-Jato contra a corrupção.

Alguma coisa mudou. Sem dúvidas, a emergência dos *smartphones* e o rápido avanço das mídias sociais entre os brasileiros podem ajudar a explicar esse fenômeno. Fato é que o cidadão não se contenta mais em apenas endossar um programa político de quatro em quatro anos. Ele quer participar.

12 São elas, respectivamente, as Regras de Privacidade entre Fronteiras (Cross-Border Privacy Rules) e o Reconhecimento de Privacidade para Processadores (Privacy Recognition for Processors).

Para que o cidadão digital exerça sua cidadania em plenitude, parece que ainda há outros campos nos quais é preciso avançar sua consciência cidadã, a começar pela ciência da importância do mundo digital, de como ele se integra com o mundo físico, seus benefícios e perigos. Um cidadão que entenda a importância dos serviços públicos oferecidos de forma digital, dos mecanismos digitais de controle e transparência da gestão pública, da conectividade para o exercício da cidadania. Nesse sentido, precisamos de políticas públicas e iniciativas que ajudem a acelerar a curva de formação desse cidadão digital, a começar pela proteção à privacidade e noções de boas práticas de segurança da informação.

...

O momento em que vivemos é um período muito rico de transformações. Passamos por mudanças tão profundas que talvez sejam comparáveis, em termos de amplitude, às da Revolução Industrial, que sedimentaram os pilares da nossa Sociedade Industrial. Mais do que isso, parece que há um processo já em curso de superação dessa sociedade para a construção de uma Sociedade Digital, nas quais os dados e as informações digitalizadas passariam a ser o motor do desenvolvimento econômico e social. Devemos situar o debate sobre proteção de dados pessoais nesse contexto mais amplo.

Precisamos revisitar a maneira como olhamos e entendemos a privacidade nessa nova sociedade. E nessa tarefa, é necessário que façamos o esforço de nos despir das lentes da sociedade industrial. Na medida em que a sociedade está se transformando profundamente, contudo, esse não parece ser um exercício fácil. Importar modelos regulatórios de outros países não é a solução e pode atrasar o nosso desenvolvimento econômico e social.

Neste ensaio procurei pontuar alguns elementos que julgo pertinente para esse debate, entre eles:

- a necessidade de um equilíbrio entre a definição de dados pessoais e a possibilidade de tratamento de dados anônimos;
- a pertinência de repensarmos mecanismos alternativos ao consentimento do titular para legitimação de tratamentos de dados pessoais, tais como o consentimento tácito ou implícito e o *legítimo interesse*;
- a importância da transparência e a centralidade da confiança na construção da sociedade digital;
- a necessidade de um sistema de proteção de dados pessoais baseado em uma legislação principiológica, na criação de uma Autoridade de Proteção de Dados Pessoais e na priorização da segurança da informação;

- a garantia da manutenção do fluxo internacional de dados, motor do desenvolvimento e da inovação global;
- e, por fim, a urgência de acelerarmos a curva de formação do cidadão digital.

Grande parte dos que nasceram antes dos anos 1990, como eu, foi criada, educada e treinada para viver, trabalhar e criar seus filhos em uma sociedade industrial, basicamente analógica. E confrontados por mudanças bruscas e profundas, como as que vivemos hoje, muitas vezes ficamos sem chão, sem saber o que fazer ou como será o futuro. Afinal, estamos tendo de inventar e nos reinventar ao mesmo tempo. Tarefa essa que não é fácil. Se temos dúvidas sobre vários aspectos, em um estou seguro que estamos no caminho certo: o debate aberto, plural e democrático para a construção da sociedade digital. Mãos à obra.

REFERÊNCIAS

ENRIQUEZ, Jof. Medtronic Announces Diabetes Partnerships With IBM Watson, Nutrino, Glooko. Disponível em: <https://www.meddeviceonline.com/doc/medtronic-announce-diabetes-partnerships-with-ibm-watson-nutrino-glooko-0001>. Acesso em: 10 mar. 2017.

IBM. Pfizer Taps IBM for Research Collaboration to Transform Parkinson's Disease Care. Disponível em: <https://www-03.ibm.com/press/us/en/pressrelease/49475.wss>. Acesso em: 10 mar. 2017.

JUSTICE AND CONSUMERS. Article 29 Working Party. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Acesso em: 10 jul. 2017.

MANYIKA James et al. Digital Globalization: the new era of global flows. Disponível em: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>. Acesso em: 10 jul. 2017.

PAÍS DIGITAL. Disponível em: <www.brasilpaisdigital.com.br>. Acesso em: 14 dez. 2018.

PROTEÇÃO DE DADOS PESSOAIS COMO ELEMENTO DE INOVAÇÃO E FOMENTO À ECONOMIA: O IMPACTO ECONÔMICO DE UMA LEI GERAL DE DADOS

BRUNO BIONI

RENATO LEITE MONTEIRO

INTRODUÇÃO: BREVES NOTAS SOBRE A AGENDA "ECONÔMICA" DA PROTEÇÃO DE DADOS PESSOAIS

Uma Lei Geral de Proteção de Dados Pessoais/LGPD tem por objetivo não só garantir a privacidade e outros direitos fundamentais dos cidadãos, mas, também, fomentar a economia. Ao mesmo tempo em que se reduz a assimetria de informação entre entidades privadas, públicas e indivíduos, franqueando aos últimos o controle sobre suas informações pessoais (DONEDA, 2006; SCHERTEL, 2014),[1] estabelece-se alicerces claros para a utilização e monetização dessas informações. Com isso, garante-se, em última análise, segurança jurídica para tais relações.

Ao invés de um custo operacional, os setores regulados, principalmente a iniciativa privada, podem e devem enxergar a proteção dos dados pessoais como um elemento de inovação e fomento à economia. Essa é, aliás, uma perspectiva que tem acompanhado historicamente a criação e a consolidação das normativas a esse respeito.

Nesse sentido, já na década de 80, a Organização para o Desenvolvimento e Cooperação Econômica (OCDE) emitiu diretrizes a respeito do tema (OECD, 2011), as quais foram atualizadas e ampliadas mais de três décadas depois (OECD, 2013). Em ambos os momentos, a narrativa em torno de tal documento se pautou pelo papel estratégico dos dados pessoais para o progresso socioeconômico (OECD, 2013).

1 A proteção de dados pessoais tem sido historicamente associada ao direito dos cidadãos autodeterminar as suas informações pessoais (autodeterminação informacional).

É sintomático, da mesma forma, verificar a recorrência desse movimento em outros organismos internacionais para fins de cooperação econômica, como aconteceu, por exemplo, no âmbito dos países asiáticos e do pacífico. Em 2005, a Cooperação Econômica Ásia-Pacifico (APEC)[2] criou um conjunto de definições e princípios (Privacy Framework) (APEC, [s.d.]) que também tinha como seu fio condutor tal aspecto econômico, notadamente o de expandir o comércio eletrônico (APEC, [s.d.]).

Em vista da recente aprovação da Lei nº 13.709/2018, a LGPD brasileira,[3] mostra-se mais do que pertinente retomar essa narrativa histórica em torna da sua função de fomento à economia, identificar como isso se reverbera dentre alguns dos princípios e direitos desse novo corpo normativo projetado.

SEGURANÇA JURÍDICA: A NECESSIDADE DE UMA REGULAÇÃO GERAL NO CONTEXTO DE UMA SOCIEDADE MOVIDA POR DADOS (*DATA-DRIVEN-SOCIETY*)

Atualmente, o Brasil conta apenas com leis setoriais de proteção de dados pessoais (BIONI, 2014). Apesar da possibilidade de se inferir um diálogo entre os direitos e princípios previstos dispersamente no ordenamento jurídico brasileiro, essa é uma solução precária e provisória (BIONI, 2014), que por vezes determina tratamentos e abordagens distintas a situações similares, caracterizando-se como um terreno pantanoso.

A ideia de uma LGPD é justamente a concepção de um corpo normativo, cujo conjunto de regras e princípios, organizados e projetados de forma unitária, forneça uma regulamentação uniforme. Uma regulação setorial e, portanto, fragmentada é, desde o seu nascedouro, viciada para tal objetivo.

Em uma sociedade cada vez mais movida por dados – *data-driven-society* – (OECD, [s.d.]),[4] essa infraestrutura jurídica se faz ainda mais necessária. Ela é capaz de fornecer respostas a esse fenômeno totalmente multifacetado.

2 Sobre a APEC ver: APEC. About Us. Disponível em: <http://www.apec.org/About-Us/About-APEC>. Acesso em: 04 jul. 2017.

3 Essa é uma das considerações do estudo comparativo da época em que tramitavam diversos projetos de lei acerca da matéria no Congresso Nacional.

4 A terminologia tem se tornando um *buzzword* atualmente. No entanto, já havia sido utilizado em 2013 pela OECD.

A começar, até então não existia nem sequer uma definição clara do conceito de dados pessoais. Diferentes leis[5] e decretos[6] trazem conceitos díspares e de aplicação setorial. Além disso, as poucas normas infraconstitucionais que conceituam dado pessoal não definem, ao mesmo tempo, o que seria um dado anonimizado e, *via-a-vis*, qual o conjunto de direitos e obrigações, mais ou menos rígido, a que tais atividades deveriam seguir.

A LGPD é capaz de trazer um horizonte de segurança jurídica para todos os setores da economia que têm as suas atividades permeadas, de alguma forma, pelo processamento de dados pessoais. Do setor securitário ao da publicidade comportamental, do financeiro ao de serviços de Internet, haveria um "manual de instruções" sobre como processar tais dados, mitigando, em última análise, os riscos de todas essas atividades empresariais.

PRINCÍPIO DA QUALIDADE DOS DADOS: MAIOR EFICIÊNCIA DE UMA CADEIA PRODUTIVA BASEADA EM DADOS E EM PROCESSOS DE DECISÃO AUTOMATIZADOS

Apesar da quantidade de dados em circulação hoje em dia, pessoais ou não, a grande maioria deles pode ser considerado lixo, ou, no termo técnico, ruído – *noise*. Uma consequência direta é que muito tempo e dinheiro são gastos visando transformar esse ruído em dados de qualidade, que sejam "interoperáveis", para que possam ser cruzados para, ao final, ser extraída uma informação útil.

Com a positivação de regras e fundamentos gerais, transversais e multissetoriais de proteção de dados pessoais, todos os agentes estarão obrigados a manter dados que sejam exatos, atualizados e corretos. A tendência será, então, que eles, com o passar o tempo, se tornem mais "limpos", e, por consequência, mais úteis.

Em uma economia cada vez mais orientada pela inteligência de grande base de dados – *big data* – e de automatização de decisões (algoritmos), trata-se de um elemento crítico a alocar maior eficiência em toda a economia.

---

5 Ver, por exemplo, a definição contida no artigo 4º, inciso IV, da Lei de Acesso à Informação (Lei nº 12.527/2011: IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

6 Ver, por exemplo, o artigo 14, inciso I, do Decreto de Regulamentação do Marco Civil da Internet (Decreto nº 8711/2016): "dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa […]".

Da publicidade comportamental à precificação de contratos securitários e financeiros, zelar pela qualidade de dados significa a adoção de estratégias comerciais mais eficazes, lastreadas em informações mais precisas.

Esse é o caso, por exemplo, do setor de crédito. Hoje a análise não se faz mais apenas com base no histórico negativo, isto é, das obrigações não pagas pelo consumidor. Aos postulantes de crédito é atribuída uma nota – *credit score* – que congrega também o seu histórico positivo, isto é, das obrigações por ele adimplidas (BESSA, 2011).[7]

Com isso, forma-se um perfil da capacidade econômico-financeira do potencial consumidor que determina o valor e a taxa de juros de tais contratos. Se essa *personalização do crédito* é precisa e não discriminatória (ZANATTA; DONEDA, 2017), trata-se de uma ferramenta útil para prevenir o fenômeno do superendividamento da população e, última análise, a saúde de uma economia de consumo altamente dependente da "democratização do crédito".

Todavia, se esta contiver, também, dados imprecisos, desatualizados e em excesso, o cálculo do *score* do consumidor poderá estar errado, o que por sua vez pode prejudicar e trazer danos econômicos tanto para o cidadão quanto para a instituição privada.

Ao final, essas e outras transações comerciais, seja da economia *on-line* ou *off-line*, serão otimizadas em razão do cidadão-consumidor estar representado fidedignamente por seus dados. Essa sinergia implica em um mercado mais confiável e que internaliza a proteção dos dados pessoais como um elemento de fomento à economia.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO: A (IN) EVITABILIDADE DO VAZAMENTO DE DADOS PESSOAIS

Após o recente vazamento de dados do sistema SWIFT – responsável por transferências internacionais de valores – na Ásia, as autoridades de vários países se reuniram para rever as regras de proteção de dados da APEC Privacy Framework.[8] A conclusão foi de que seriam necessárias normas mais rígidas por duas razões.

---

7 Para uma análise do conceito de credit score, bem como da Lei do Cadastro Positivo.

8 Cf.: ZHENG, Anjie. Regulators to Tighten Cyberdefenses as Attacks in Asia Increase. The Wall Street Journal, 14 jun. 2016. Disponível em: <http://www.wsj.com/articles/regulators-to-tighten-cyberdefenses-as-attacks-in-asia-increase-1465899792>. Acesso em: 04 jul. 2017.

Primeiro, as fraudes bancárias diminuiriam, uma vez que o acesso indevido aos dados pessoais dos consumidores, o que se convencionou chamar de roubo de identidade (SOLOVE, 2006), propicia transações financeiras por terceiros que não são seus reais beneficiários, causando danos econômicos para o correntista e para a própria instituição financeira.

Segundo, porque a recorrência de tais incidentes gera desconfiança (MARQUES, 2004) entre todos os agentes do ecossistema financeiro, principalmente nos próprios consumidores. Isso os inibiria não só de utilizar o serviço específico em questão, como todo o sistema bancário – tradicional. Em um cenário em que emerge novos rivais nesse mercado, as chamadas *fintechs*, esse risco seria ainda mais significativo.

O mesmo raciocínio seria aplicável a todos os demais setores da economia. Vale mais a pena investir em padrões de segurança da informação para prevenir tais incidentes de segurança do que arcar com os custos de transações fraudulentas e a perda da audiência dos seus consumidores.

Esse é o "cálculo" que orienta as leis gerais de proteção de dados pessoais, especialmente o princípio da segurança lógica e física. A economia gerada com a prevenção de fraudes e o reforço da criação de um ambiente de confiança, associado ao ganho reputacional despertado no consumidor, supera as perdas econômicas causadas por incidentes de segurança da informação.

No Brasil, estima-se que tais incidentes de segurança atingiriam R$ 33,00 (trinta e três reais) dos R$ 225,00 (duzentos e vinte e cinco reais) da renda per capita dos brasileiros (TELESINTESE, [s.d.]). Tais incidentes podem causar não somente danos monetários e reputacionais, mas até mesmo ocasionar incidentes sistêmicos que podem atingir todo o sistema e atividades baseadas nesse fluxo informacional que é transfronteiriço.

Uma lei geral de proteção de dados pessoais, bem como um sistema de fiscalização dessas leis por meio de um agente regulador central com expertise adequada, atuando em conjunto com outros agentes reguladores, pode ter como efeito a diminuição considerável desses riscos locais e sistêmicos, ao não só estabelecer padrões mínimos de segurança da informação, mas, também, fomentar a adoção de códigos de conduta discutidos e pensados pelos próprios players do mercado.

Ademais, a LGPD positiva a obrigação de informar ao regulador, e eventualmente aos titulares atingidos, casos de incidentes de vazamentos de dados, principalmente nas situações em que os responsáveis pelo tratamento não se adequaram aos *standards* definidos pelo mercado em conjunto com a autoridade de proteção de dados pessoais. Esta pode, em moldes

similares a *recall* de carros ou medicamentos, não só aplicar penalidades, mas, também, obrigar que os indivíduos atingidos sejam diretamente informados e de alguma forma os seus riscos de exposição indevida a práticas abusivas mitigados.

O estabelecimento da obrigação de notificar incidentes de vazamentos de dados pessoais deve ser encarado não como um custo operacional maior ou um risco à imagem do responsável pelo tratamento, mas sim como incentivo a mais para que todos as entidades, públicas e privadas, adotem os mais altos níveis de segurança e de procedimentos, o que, por consequência, pode, justamente, melhorar a reputação da entidade perante o mercado e a sociedade.

Desta forma, sob diferentes prismas, os retornos econômicos, reputacionais e de eficiência superam os custos de implementação, adequação e supervisão que tanto assustam parte da iniciativa privada nacional e internacional.

AS HIPÓTESES DE TRATAMENTO DE DADOS COM BASE NO CONSENTIMENTO E NOS LEGÍTIMOS INTERESSES: BASE LEGAIS PARA CONFERIR SEGURANÇA JURÍDICA AOS MAIS DIFERENTES MODELOS DE NEGÓCIO

A pedra angular para o tratamento de dados pessoais é o consentimento do titular, que deve ser, pelo menos, livre, informado e para finalidades determinadas. Todavia, a adjetivação do consentimento varia entre diferentes regulações, o que pode ocasionar um grande impacto nos mais diferentes modelos de negócio.

Por exemplo, o Marco Civil da Internet determina que o consentimento deve ser livre, expresso, informado e para finalidades específicas. Entretanto, a obrigatoriedade de um consentimento tão rígido pode, na verdade, ter efeitos contrários, seja para que o usuário simplesmente aceita tudo que aparece na sua frente (o famoso aceite dos termos de uso sem ter conhecimento do conteúdo, na teoria do *overload* informacional) (MACEDO JÚNIOR, 2010)[9] ou para que haja um engessamento na forma de obtenção deste, o que, na prática, pode levar a um desrespeito das normas, prevendo autorizações genéricas como "compartilhamento com parceiros comerciais",

9 "Estudos sobre o conceito de racionalidade limitada (bounded rationality) e sobrecarga de informação (overloaded information), têm evidenciado que a equação: maior informação = maior capacidade de decisão consciente (e, portanto, livre) frequentemente não corresponde à realidade". Cf.: MACEDO JÚNIOR, 2010, p. 27.

conceito amplo e vago comum em muitas políticas de privacidade aceitas por usuários de serviços de Internet.

Diferentemente do Marco Civil da Internet, a LGPD (BIONI; MONTEIRO, [s.d.]) traz em seu texto dez hipóteses autorizativas para o tratamento de dados pessoais, sendo o consentimento apenas uma delas. Ainda, a adjetivação do consentimento é mais fluída, aceitando que este seja inequívoco e para finalidades determinadas (BIONI, [s.d.]),[10] a exceção caso o tratamento seja de dados pessoais sensíveis ou para fins de transferência internacional. Isso pode evitar com que tratamento de dados sejam realizados fora do escopo legal da norma, ou em afronta direta a esta.

Uma outra importante hipótese autorizativa para o tratamento de dados pessoais é a do legítimo interesse, conceito já presente em diversas legislações, mas ainda até não positivado no brasileiro. O legítimo interesse é a hipótese que deve ser utilizada em situações onde:

I. o consentimento do usuário é desnecessário para as finalidades almejadas;

II. quando se mostrar o embasamento legal mais adequado para a situação concreta, sendo que a sua aplicação depende de um prévio teste de proporcionalidade (BIONI, [s.d.]) [11] entre os interesses em jogo e os direitos e liberdades individuais dos titulares.

Os legítimos interesses devem ser encarados, antes de tudo, como uma base adequada para o tratamento que pode conferir segurança jurídica para diferentes modelos de negócio que hoje provavelmente processam dados pessoais de forma indevida ou se aproveitando de hiatos regulatórios. Este é o caso, por exemplo, de novos modelos baseados em Internet das Coisas e em metodologias de processamento de dados agrupadas no conceito de Big Data (BIONI, 2016), que, devido as características já detalhadas neste artigo, podem encontrar dificuldades em buscar o consentimento dos titulares dos dados pessoais envolvidos. Justamente por estas razões que a iniciativa privada se manifestou fortemente durante a segunda consulta

10 Ver, nesse sentido, a análise comparativa das diferentes adjetivações empregadas ao consentimento pelos projetos de lei que estavam até então em discussão no Congresso Nacional.

11 "Freios e contrapesos entre a hipótese do legítimo interesse e a regra geral do consentimento". Cf.: BIONI, [s.d.], p. 50-51).

pública do então anteprojeto para que esta possibilidade fosse incluída no rol de bases legais para o processamento de dados.[12]

Desta forma, os legítimos interesses podem ser encarados como uma real oportunidade para os modelos de negócios, baseados no uso de dados, oferecerem seus serviços com segurança jurídica. Todavia, os legítimos interesses não podem ser encaradas como uma bala de prata, um cheque em branco para autorizar o tratamento de dados pessoais, ou muito menos ser um substitutivo ao consentimento.

Primeiramente, legítimos interesses não devem ser encarados como qualquer interesse, muito menos interesses amplos, vagos ou hipotéticos, que podem dar margem a mais diferentes práticas de tratamento de dados pessoais. Interesses legítimos devem ser baseados em situações concretas, em interesses reais, mesmo que estes sejam puramente comerciais, baseados em garantir novos usos a um determinado conjunto de dados (EUROPEAN COMISSION, [s.d.]), em benefício ao responsável pelo tratamento, desde que levem em consideração as legítimas expectativas do titular, seus interesses razoáveis, mesmo que os novos usos são sejam em seu benefício. Ou seja, deve tratar-se de uma situação concreta que poderia ser eventualmente aceita por este, assegurados seus direitos fundamentais e liberdades individuais.

Para garantir o cenário acima descrito, o tratamento de dados pessoais com base nos legítimos interesses do responsável pelo processamento dos dados deve sempre estar acompanhado de uma análise contextual (BIONI, 2016)[13]

---

12 "Em 2015, durante o debate público feito na Internet, o Poder Executivo incluiu no projeto de lei uma hipótese adicional que autoriza o tratamento de dados pessoais, o "legítimo interesse" do responsável (art. 7, IX): [o tratamento de dados pessoais poderá ser realizado] quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais, em especial se o titular for menor de idade". "O conceito foi incluído no texto para autorizar determinadas situações nas quais o consentimento não precisaria ser emitido. São situações nas quais não é necessário perguntar ao cidadão ou cidadã se aquele tratamento pode ser realizado, pois, segundo o artigo 10 do projeto, ele deve contemplar as suas "legítimas expectativas". Conceito presente nas regras europeias de proteção de dados, tal hipótese concentrou preocupações de diferentes setores". Cf.: INTERNETLAB. Disponível em: <http://www.internetlab.org.br/pt/conjuntura/reporta-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 04 jul. 2017

13 Ver, nesse sentido, o capítulo intitulado: "Interesses legítimos e o tratamento dos dados pessoais para usos secundários: concreção da privacidade contextual no direito comunitário europeu e o APLPDP e a sua aplicação a casos hipotéticos".

em que um teste específico verificará se os interesses apontados são reais, e não meramente especulativos, e os direitos de transparência, acesso, correção, oposição e liberdades individuais não serão mitigados. Trata-se, portanto, de um teste de proporcionalidade e necessidade em que se corroborará se o uso desta hipótese autorizativa é realmente necessária para se atingir as finalidades almejadas.

O Working Party 29,[14] por meio da sua opinião sobre o uso dos legítimos interesses,[15] lista uma série de questões que ajudariam a balança entre os interesses do responsável pelo tratamento e as legítimas expectativas do titular pender para o lado daquele com base:

I. na natureza dos dados;

II. na impacto do tratamento nos indivíduos; e se

III. há salvaguardas técnicas e jurídicas que possam mitigar eventual impacto.

O outro importante fator que pode favorecer o uso de legítimos interesses como base legal é assegurar ao titular o direito à portabilidade dos seus dados para um outro serviço ou base de dados, caso seja do seu interesse. Esta seria, inclusive, uma forma de fomentar a concorrência entre diferentes modelos de negócio baseados no uso massivo de dados, uma maneira de "compartilhar a riqueza" (UNITED KINGDOM INFORMATION COMMISSIONER'S OFFICE, [s.d.]) quase que natural no uso de dados pessoais como moeda corrente da sociedade da informação.

---

14 O Article 29 Working Party (WP 29) é um órgão consultivo formado por representantes de todas as autoridades de proteção de dados dos membros da União Europeia, por um membro do European Data Protection Supervisor e um membro da Comissão Europeia. Sua principal função é emitir opiniões sobre determinados assuntos envolvendo práticas de tratamento de dados pessoais. Mais informações: EUROPEAN COMMISSION. Article 29 Working Party. Disponível em <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>. Acesso em: 04 jul. 2017.

15 "(i) na natureza dos dados: os dados são necessários para exercício de um direito? Há um interesse público subjacente no tratamento? Quais os benefícios sociais e culturais?

(ii) na impacto do tratamento nos indivíduos: O processamento envolve dados sensíveis?

Os dados são combinados com outros? Quais as expectativas razoáveis do titular? O titular é parte vulnerável na sociedade? Qual o poder econômico do processador?

(iii) há salvaguardas técnicas e jurídicas que possam mitigar eventual impacto: Princípio da minimização foi aplicado? Há medidas técnicas para impedir decisões automatizadas? Há uso de técnicas de anonimização? Há uso de medidas adicionais?". Cf.: EUROPEAN COMMISSION. Article 29 Working Party. Disponível em <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>. Acesso em: 04 jul. 2017.

Um clássico exemplo de tratamento de dados permitido com base em legítimos interesses seria o uso de dados para verificação de situações de fraudes, mesmo que estes não tenham sido originalmente coletados para tal propósito (UNITED KINGDOM INFORMATION COMMISSIONER'S OFFICE, [s.d.]). Nesta situação, não faria muito sentido tentar obter o consentimento de um indivíduo se o responsável pelo tratamento quer justamente verificar se este foi o sujeito ativo de uma fraude. Neste caso, haveria um interesse legítimo do responsável pelo tratamento, pois ser alvo de uma fraude poderia se ocasionar um prejuízo econômico, e também o novo uso estaria dentro da esfera de legítimas expectativas do titular dos dados, pois mesmo que os interesses não lhe beneficiassem, seria razoável esperar que no caso de uma fraude seus dados poderiam ser utilizados para investigá-lo.

Todavia, um exemplo que provavelmente não passaria no teste de proporcionalidade dos legítimos interesses seria a situação em que um grupo de eleitores fornecessem seus dados para um determinado partido na espera que estes sejam utilizados para efetivar a comunicação das plataformas políticas dos seus candidatos, ou até mesmo conclamar para assembleias e encontros. Todavia, se o partido, no afã de angariar fundos, resolve vender sua base de dados para um *data broker* ou agência de *marketing*, que utilizará os dados para fins de oferecimento comercial de produtos e serviços, sem que haja o consentimento dos titulares para tanto, tal prática pode ser considerada desproporcional, fora das expectativas dos titulares do que eventualmente poderia ser feito com seus dados, além destes serem compartilhados sem que direitos como transparência, acesso, retificação, oposição, cancelamento e portabilidade sejam garantidos. Portanto, numa situação como esta, o interesse puramente comercial do partido provavelmente seria considerado ilegítimo, caracterizando-se como um tratamento de dados pessoais ilegal e não autorizado.

Levando em consideração tais premissas, após as sugestões e interesses amplamente discutidos na segunda consulta pública, os legítimos interesses foram incluídos no rol de bases legais para o tratamento de dados pessoais previstos na LGPD:

> Art. 13, IX: "[o tratamento de dados pessoais poderá ser realizado] quando necessário para atender aos interesses legítimos do responsável ou de terceiros, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais, em especial se o titular for menor de idade".

Ainda, o art. 16 implementa um efetivo teste de proporcionalidade, nos moldes não só no já previsto em legislações estrangeiras mas, também,

acatando as sugestões dadas pelo Working Party 29 na opinião retromencionada. Desta feita, os legítimos interesses, na forma como desenhados na legislação projetada, devem:

- a hipótese dos legítimos interesses permite usos secundários dos dados pessoais, mas não pode ser um cheque em branco que autorize qualquer novo tipo de tratamento;
- o legítimo interesse do responsável pelo tratamento deve respeitar os direitos e liberdades fundamentais do titular;
- o tratamento com base nos legítimos interesses deve ser necessário e baseado em uma situação concreta. Não pode ser uma excusa genérica;
- o legítimo interesse deverá contemplar as legítimas expectativas do titular, e não mitigar seus direitos, inclusive os garantidos pela própria lei geral;
- transparência deve ser garantida, visando o possível direito de oposição do titular, que deve obedecer aos preceitos da norma;
- os dados pessoais objeto do tratamento devem ser anonimizados sempre que compatível com a finalidade do tratamento;
- o órgão competente pode requisitar e auditar práticas do mercado, exigindo relatórios de impacto à privacidade (Privacy Impact Assessment).[16]

Todavia, o pesquisador Rafael Zanatta, em apresentação privada feita em março de 2017 para o Ministério das Comunicações e Tecnologia (MCTIC), levantou algumas questões polêmicas que devem ler levadas em consideração:

I. apesar da prevalência dos Direitos Fundamentais no teste de proporcionalidade, como verificar essa posição na prática?

II. como evitar a fuga do consentimento como pedra basilar do tratamento de dados pessoais para os legítimos interesses?

III. seriam as balizas previstas no PL suficientes para garantir um balanceamento adequado no caso concreto?

IV. como garantir que a Autoridade de Proteção de Dados terá expertise e capacidade para verificar os casos baseados em legítimos interesses?

V. como evitar que os argumentos baseados nos usos benéficos do Big Data se sobreponham às medidas para garantir direitos fundamentais?

16 Art. 16, §3º, da LGPD.

Importante enaltecer que a maleabilidade dada ao consentimento e a possibilidade de tratamento com base nos legítimos interesses do responsável não deve retirar o controle por parte do titular, uma vez que o ônus para provar a obtenção deste continuará com o responsável pelo processamento dos dados, mas permitirá uma melhor experiência do usuário – apesar deste ser um argumento clássico para justificar coletas massivas de dados pessoais –, a criação de diferentes modelos de negócio, sem que necessariamente haja uma limitação de direitos, conferindo uma maior segurança jurídica.

FLUXO INTERNACIONAL DE DADOS: COMO ASSEGURAR DIREITOS E SEGURANÇA JURÍDICA EM UM MEIO QUE NÃO RESPEITA LIMITES GEOGRÁFICOS?

É necessário ver o livre fluxo internacional de dados como um diferencial competitivo entre diferentes mercados. Um dos princípios basilares no tratamento de dados pessoais na sociedade em que o fluxo destes não respeita fronteira geográficas é a necessidade dos diferentes países onde os dados serão tratados oferecerem níveis adequados de proteção dos dados pessoais, para que os direitos garantidos aos cidadãos em uma jurisdição não sejam mitigados em outra com um sistema protetivo inferior.

Neste contexto, o Brasil, ainda não oferece um nível de proteção adequado, principalmente quando comparado com o arcabouço legal europeu. Países vizinhos como Argentina e Uruguai,[17] que há anos dispõem de leis gerais, já receberam a chancela da autoridade central europeia, o que na prática autoriza que estes recebem dados pessoais de cidadãos europeus ou originalmente tratados na União Europeia. Os impactos econômicos e comerciais dessas decisões de adequação são enormes. Por exemplo, uma empresa europeia que oferece serviços através da Internet pode escolher utilizar datacenters instalados em Montevideo por estes terem um custo operacional bem inferior aos praticados no velho continente. Todavia, esta mesma empresa não poderia alugar servidores no Brasil para receber dados pessoais de seus clientes, mesmo que o serviço nas terras tupiniquins fosse mais barato, pois ainda não estamos liberados para receber, armazenar e tratar tais dados. Referido cenário poderá ser revertido com a LGPD.

17 Decisão que conferiu o nível de adequação à Argentina e ao Uruguai. Cf.: EUROPEAN COMMISSION. DATA PROTECTION. Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>. Acesso em:04 jul. 2017.

Importante salientar que mesmo com a possibilidade de transferência internacional por meio de consentimento específico, hipótese prevista na LGPD,[18] isso só significa que podemos enviar dados do Brasil para outro país, mas não constitui uma garantia que dados de cidadãos de países terceiros poderão ser enviados para o nosso. Existem outros instrumentos jurídicos, como cláusulas contratuais padrão e Binding Corporate Rules (BCRs), que podem ser utilizados, mas estas são específicas, caso a caso, por muitas vezes burocráticas, o que por sua vez pode não acarretar a mesma eficiência e segurança de uma lei geral, transversal e multisetorial.

Portanto, no contexto do fluxo internacional de dados, o Brasil só tem a ganhar com a recém aprovada LGPD.

PRIVACY BY DESIGN E DATA PROTECTION BY DESIGN: PROTEÇÃO AOS DADOS PESSOAIS DESDE O MOMENTO DA CONCEPÇÃO DOS SERVIÇOS E PRODUTOS

Na esteira de garantir a segurança dos dados como diferencial competitivo, cada vez mais as empresas se voltam para metodologias conhecidas como Privacy by Design e Data Protection by Design, que em suma pregam a necessidade de se ter por norte a proteção à privacidade e aos dados pessoais desde o momento da concepção do serviço/produto, durante o seu desenvolvimento, oferecimento ao mercado e futura supervisão para tentar identificar falhas ou práticas que não puderam ser antevistas no momento adequado. A adoção de tais metodologias se torna de supra importância no cenário da Internet das Coisas, em que até mesmo os equipamentos mais simples e banais presentes no nosso dia contarão com sensores que coletarão dados pessoais de forma quase que ininterrupta, que por ventura serão compartilhadas com outros equipamentos inteligentes, uma vez que a eficiência destes está diretamente ligada a possibilidade de conversarem entre si para permitir maior automação da vida pessoal do indivíduo.

A escolha por não empregar padrões, princípios e regras que visem garantir a proteção dos dados pessoais desde o momento da concepção do produto e do serviço pode ter consequências nefastas, como o incidente que permitiu que quase metade da Internet dos EUA fosse derrubada por horas devido a uma falha de segurança presente em roteadores de webcams conectadas diretamente a Internet, que por sua vez foram capturadas para realizar ataques de DDoS (TIME, [s.d.]). Em um outro cenário possível, o que impedia que estas mesmas webcams não fossem massivamente

18 Art. 33, VIII, da LGPD.

atacadas para permitir o controle sobre as suas capturas de vídeo, desta forma filmando e monitorando milhares de pessoais, em abismal violação ao direito à privacidade destas.

O emprego massivo de diferentes formas de criptografia é um exemplo claro desse movimento de adotar tais métodos. Mas este não é o único. Cada vez mais as empresas se valem dessas orientações para escrever os algoritmos que serão responsáveis por decisões automatizadas, visando evitar que estes, ao se valerem das diferentes variáveis disponíveis no seu ambiente, cheguem a resultados que possam ser considerados discriminatórios ao ponto de mitigar ou violar direitos e garantias fundamentais dos indivíduos atingidos, o que pode ensejar a responsabilização das entidades que processam os dados pessoais. Tal prática é conhecida como Algorithmic Accountability.

Ainda, a prática conhecida como Privacy by Default determina que os serviços já venham com configurações de privacidade mais restritivas de fábrica, cabendo aos usuários flexibilizá-las se assim desejar. As diferentes abordagens do Facebook com relação à privacidade são bons exemplos dessa técnica, uma vez que a rede social começou permitindo que qualquer pessoa tivesse acesso aos perfis e aos conteúdos compartilhados pelos seus usuários, para depois restringir apenas aos amigos ou círculos de pessoas pré-estabelecidos, podendo estes serem estendidos a terceiros, caso fosse do interesse.

As três situações acima descritas (Privacy by Design, Data Protection by Design e Privacy by Default) estão presentes na LGPD, algumas consideradas mandatórias, outras melhores práticas.

DIREITO DE PORTABILIDADE: SERIA ESTE A MAIS EFETIVA FORMA DE GARANTIR A COMPETIÇÃO ENTRE DIFERENTES *PLAYERS* DO MERCADO E CONFERIR EFETIVO CONTROLE AOS TITULARES DOS DADOS PESSOAIS?

Como já tivemos a oportunidade de destacar anteriormente (MONTEIRO; BIONI, [S.D.]), dentre outras inovações previstas na LGPD, há o chamado direito de "portabilidade".[19] Os usuários poderão "levar" consigo seus dados pessoais ao trocar uma aplicação na Internet por outra – ou qualquer outro tipo de serviço que se valha do tratamento de dados pessoais –, devendo, inclusive, a antiga aplicação fornecer os meios adequados para operacionalizar tal transmissão de dados, preferencialmente através de protocolos interoperáveis.

19 Art. 8º, V, da LGPD.

A privacidade poderá se tornar, literalmente, um elemento de competitividade. Afinal, quem trocaria de plataforma caso não pudesse levar consigo todo a sua "vida digital"? Os usuários poderiam, por exemplo, não só migrar para serviços que lhes sejam mais atraentes, inovadores, mas também para àqueles que lhes forneçam maiores garantias à proteção de seus dados pessoais.

Em um cenário pós-Snowden, no qual a confiança nos gigantes da Internet mostra-se fragilizada, não só já existem redes sociais[20] implementando criptografia e servidores descentralizados como ferramentas antiespionagem, mas várias empresas utilizam o incremento na robustez da segurança dos dados dos clientes como bandeiras de marketing, inclusive defendendo judicialmente esse elemento dos seus modelos de negócio. Casos emblemáticos como a batalha entra a Apple e o FBI[21] e os bloqueios do Whatsapp no Brasil[22] por este serviço implementar criptografia ponta-a-ponta são exemplos de até onde estas empresas estão dispostas a ir para defender a privacidade dos dados de seus clientes.

Diversas empresas já consideram a proteção à privacidade um elemento essencial dos seus modelos de negócio, considerando-o um elemento competitivo que os destaca no gigantesco universo de soluções baseadas no uso de dados pessoais. A adoção de serviços como Snapchat no lugar do Instagram; Signal no lugar do Whatsapp, antes desse último ter adotado também criptografia ponta-a-ponta; práticas como dupla autenticação e senhas mais robustas são pequenos exemplos de como as pessoas ainda se preocupam com a sua privacidade e proteção dos seus dados, diferentemente do cenário verbalizado por muitos.

CONCLUSÃO

Nesse sentido, uma Lei Geral de Proteção de Dados Pessoais, visa garantir a autodeterminação informativa, ao mesmo tempo que visa fomentar o desenvolvimento econômico e tecnológico por meio de regras balanceadas para assegurar os interesses de todos os atores de uma economia e sociedade cada vez mais movida por dados. Nesse cenário a iniciativa privada poderá

20 DIASPORA BR. Disponível em: <https://diasporabr.com.br/>. Acesso em: 04 jul. 2017.

21 Carta da empresa Apple explicando o seu ponto de vista do caso: APPLE. Answers to your questions about Apple and security. Disponível em: <http://www.apple.com/customer-letter/answers/>. Acesso em: 04 jul. 2017.

22 Bloqueios.info, iniciativa do Internet Lab que lista e analisa os casos de bloqueio de aplicativos e serviços de Internet no Brasil: BLOQUEIOS.INFO. Disponível em: <www.bloqueios.info>. Acesso em: 04 jul. 2017.

se valer da proteção de dados pessoais como diferencial competitivo e uma vantagem econômico, algo que acompanha historicamente a arquitetura de leis gerais de proteção de dados pessoais.

REFERÊNCIAS

APEC. About Us. Disponível em: <http://www.apec.org/About-Us/About-APEC>. Acesso em: 04 jul. 2017.

APEC. APEC Privacy Framework. Disponível em: <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx>. Acesso em: 04 jul. 2017.

APPLE. Answers to your questions about Apple and security. Disponível em: <http://www.apple.com/customer-letter/answers/>. Acesso em: 04 jul. 2017.

BESSA, Leonardo Roscoe. *Cadastro positivo*: comentários à Lei 12.414, de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

BIONI, Bruno Ricardo. O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo 'Lulu'. *Revista de Direito do Consumidor*, v. 94, p. 283-326, 2014.

BIONI, Bruno Ricardo. *Autodeterminação informacional:* paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado)–Faculdade de Direito da Universidade de São Paulo, São Paulo, 2016.

BIONI, Bruno Ricardo. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Disponível em: <http://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil>. Acesso em: 04 jul. 2017.

BLOQUEIOS.INFO. Disponível em: <www.bloqueios.info>. Acesso em: 04 jul. 2017.

DIASPORA BR. Disponível em: <https://diasporabr.com.br/>. Acesso em: 04 jul. 2017.

DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais.* Rio de Janeiro: Renovar, 2006.

EUROPEAN COMISSION. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Working Party 29. Disponível em:<http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Acesso em: 04 jul. 2017.

EUROPEAN COMMISSION. Article 29 Working Party. Disponível em <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>. Acesso em: 04 jul. 2017.

EUROPEAN COMMISSION. DATA PROTECTION. Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>. Acesso em:04 jul. 2017.

INTERNETLAB REPORTA. Disponível em: <http://www.internetlab.org.br/pt/conjuntura/reporta-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 04 jul. 2017.

INTERNETLAB. Disponível em: <http://www.internetlab.org.br/pt/conjuntura/reporta-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 04 jul. 2017

MACEDO JÚNIOR, Ronaldo Porto. Privacidade, mercado e informação. In: NERY JÚNIOR, Nelson; NERY, Rosa Maria de Andrade (Orgs.). *Direito à informação*. São Paulo: Revista dos Tribunais, 2010. v. 8. (Coleção Doutrinas Essenciais De Responsabilidade Civil)

MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*. São Paulo: Revista dos Tribunais, 2004.

MONTEIRO, Renato; BIONI, Bruno. Que tal uma pizza de tofu com rabanetes? Você vai adorar! Huffington Post. Disponível em: <http://www.huffpostbrasil.com/renato-leite-monteiro/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar_a_21682549/>. Acesso em: 04 jul. 2017.

OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Elaboração de André-Pascal. França: OECD Publications Service, 2011.

OECD. The OECD Privacy Framework 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 04 jul. 2017.

SCHERTEL, Laura. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

SOLOVE, Daniel. *The Digital Person:* Technology and Privacy in the Information Age. Nova York: New York University Press, 2006.

TELESINTESE. Fraude on line cresce quase 200% no ano passado, diz Febraban. Disponível em: <http://www.telesintese.com.br/fraude-on-line-cresce-quase-200-no-ano-passado-diz-febraban/>. Acesso em: 04 jul. 2017.

TIME. How Web Cams Helped Bring Down the Internet, Briefly. Disponível em: <http://time.com/4542600/internet-outage-web-cams-hackers/>. Acesso em: 04 jul. 2017.

UNITED KINGDOM INFORMATION COMMISSIONER'S OFFICE. The conditions for processing. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/>. Acesso em: 04 jul. 2017.

ZANATTA, Rafael; DONEDA, Danilo. O que há de novo no debate "credit score" no Brasil? Portal JOTA, 2017. Disponível em: <https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-que-ha-de-novo-no-debate-credit-score-no-brasil-09022017>. Acesso em: 04 jul. 2017.

ZHENG, Anjie. Regulators to Tighten Cyberdefenses as Attacks in Asia Increase. The Wall Street Journal, 14 jun. 2016. Disponível em: <http://www.wsj.com/articles/regulators-to-tighten-cyberdefenses-as-attacks-in-asia-increase-1465899792>. Acesso em: 04 jul. 2017.

HABILITANDO A LOCALIZAÇÃO DE DADOS PARA CIDADES INTELIGENTES: EXPLORANDO OS REGIMES DE PROTEÇÃO E RETENÇÃO DE METADADOS NO BRASIL[1]

STANLEY SHANAPINDA

INTRODUÇÃO

Dados de telecomunicações são um ingrediente vital para a construção de uma cidade inteligente, uma cidade que responde às necessidades sócioeconômicas de seus cidadãos. Neste capítulo, adotamos uma abordagem exploratória e analisamos os regimes obrigatórios de retenção de metadados de telecomunicações e de proteção de dados no Brasil. O objetivo é aprender como o ordenamento jurídico aborda a proteção de dados. O ordenamento e os metadados são avaliados tendo em vista sua funcionalidade técnica, tendo como base de análise os termos de uso da Telefônica-Vivo, umas das maiores empresas de telecomunicações em operação no Brasil. Os regimes são avaliados com vistas a identificar as possibilidades de compartilhamento de metadados de telecomunicações, de forma que estes sejam úteis na construção de cidades inteligentes.

DADOS ABERTOS PARA O DESENVOLVIMENTO

As iniciativas de abertura de dados para o desenvolvimento pregam que todos os dados públicos sejam compartilhados e usados abertamente. Trata-se de um princípio que encontra respaldo na Lei nº 12.527 de 2011, a Lei de Acesso à Informação. Essa ideia centra-se, principalmente, nos órgãos públicos, em oposição a dados retidos por empresas privadas e, menos ainda, empresas de telecomunicação por celulares móveis, ISPs e conteúdo *over-the-top* (OTT) e prestadores de serviços de comunicações (TelCo's).

1 Tradução feita por Bruna Veríssimo Lima Santos, Helena Ferreira Matos do Carmo e Renan Medeiros de Oliveira. Revisão de Marina Barros.

RETENÇÃO DE METADADOS

De acordo com a Lei nº 12.965 de 2014 – o Marco Civil da Internet – as TelCo's, que na maioria dos casos são empresas privadas, são legalmente obrigadas a coletar, reter, criar e divulgar metadados de telecomunicações para órgãos de segurança pública e agências de segurança nacional (ANTONIALLI; ABREU, 2016). Os tipos de metadados de telecomunicações podem incluir a identificação do dispositivo e informações de localização (DILI) (SHANAPINDA, 2016; SHANAPINDA, 2017).

A lei permite acesso exclusivo aos metadados, por parte desses órgãos públicos. Estes estão habilitado a usar, processar, analisar, compartilhar e reutilizar os metadados, limitados aos seus poderes de investigação. Deste modo, metadados de telecomunicações são legalmente compelidos a serem compartilhados com o setor público pelo setor privado.

Contudo, para além do uso por órgãos de segurança, há uma miríade de outros serviços e funções de interesse público, executados por várias instituições públicas e privadas, para as quais metadados podem ser ressignificados. O marco legal para políticas públicas de compartilhamento de dados por parte das TelCo's, para fins de cidades inteligentes ou qualquer outro propósito, é abordado de forma diversa, conforme será discutido abaixo.

CIDADES INTELIGENTES

As cidades são consideradas inteligentes quando possuem a habilidade de aprender e inovar. Essa habilidade é incorporada na infraestrutura de comunicações digitais e, simultaneamente, em suas instituições de criação de conhecimento (DEAKIN, 2011). Para aprender, inovar e criar conhecimento a partir da infraestrutura de telecomunicações que cobre a comunidade, deve haver a transferência dos dados gerados pelo uso da rede por seus ocupantes para instituições de produção de conhecimento.

A inovação subjacente às cidades inteligentes é possibilitada pelas TIC.[2] Isso coloca as TelCos no cerne do ecossistema das "cidades inteligentes", como controladoras de metadados gerados pela vasta implantação da infraestrutura de telecomunicações. Isso é ainda mais enfatizado pela proximidade com o cidadão da esperada cidade inteligente (KOMNINOS, 2009).

2 N.T.: Tecnologia da Informação e Comunicação.

Os dados em si podem ser considerados infraestrutura, ou seja, bens públicos.[3] A transferência destes é seguida por sua utilização para encontrar soluções aos desafios socioeconômicos, emergenciais e de desenvolvimento, enfrentados pelos habitantes das cidades. A coleta, transferência e o subsequente uso dos dados devem, contudo, ser lícitos, garantindo a privacidade e as comunicações pessoais de seus habitantes.

PROTEÇÃO DE DADOS PESSOAIS

O compartilhamento de metadados está sujeito à proteção da privacidade. O indivíduo tem como direito a determinação sobre seus dados pessoais, como previsto no Marco Civil da Internet (FILHO; SCHWARTZ; ANDRÉ, 2016). Contudo, o fato de que o indivíduo não está ciente dos processos de Big Data prejudica o exercício destes direitos e cria um paradoxo (FILHO; SCHWARTZ; ANDRÉ, 2016). Isso pode resultar na falta de proteção (LIMA; BARRETO, 2016). A privacidade pode, portanto, exigir maior proteção (TORRES JÚNIOR, 2017).

Dahlmann, Venturi, Dickow e Maciel (DAHLMANN; VENTURINI; DICKOW; MACIEL, 2016) argumentam que "[…] o Brasil ainda não possui um quadro legal coerente para lidar com os direitos à privacidade e a proteção de dados". A falta de uma lei geral de proteção de dados faz com que a esta seja invariavelmente obscura (ASOCIACIÓN POR LOS DERECHOS CIVILES AND INTERNET LAB, 2016). Não surpreende que, até 2016, de acordo com uma avaliação independente das políticas de proteção de dados das empresas atuantes no Brasil, poucas eram as TelCo's que mantinham seus usuários informados sobre suas práticas de processamento de dados (EFF; INTERNETLAB, 2017). O que ainda não foi examinado é a fragmentação empírica dos elementos das previsões legais do Marco Civil da Internet, em relação à funcionalidade técnica dos dados, contrastando com a recente abordagem de notificação e consentimento implementada pela Telefônica-Vivo e desenvolvimentos estatutários, para explorar ainda mais o paradoxo acima mencionado.

A abordagem de notificação e consentimento é utilizada apenas como um meio de explorar dados pessoais dos indivíduos e é ineficaz. É necessária uma abordagem mais efetiva (BELLI; SCHWARTZ; LOUZADA, 2017). Intermediários estabelecem e impõem seus termos de uso unilateralmente, apresentando-os como se fossem voluntariamente aceitos através da expressão do consentimento livre e informado (BELLI; VENTURINI,

3 OPEN DATA INSTITUTE. What Is Data Infrastructure? Disponível em: <https://theodi.org/what-is-data-infrastructure>. Acesso em: 12 abr. 2017.

2016). O usuário não é informado da identidade dos terceiros para os quais seus dados podem ser transferidos, sendo deixado fora do ciclo de decisões e não tendo uma ideia clara dos impactos em sua privacidade. Um consentimento expresso, livre e informado é, consequentemente, apenas uma ficção jurídica (BELLI; VENTURINI, 2016, p. 10). A arquitetura das redes é deliberadamente moldada por algoritmos que determinam o fluxo do tráfego em benefício do ecossistema da internet (BELLI; VENTURINI, 2016, p. 2-4). No entanto, esta arquitetura também é o arranjo físico da rede, significada por acordos de interligação que moldam o fluxo de dados e, por isso, deve ser mencionada. Ela determina a coleta e o processamento de dados do usuário. Desta forma, as TelCo's definem os termos de uso contratuais através de acordos privados com terceiros. Estes regulam a medida em que o usuário pode desfrutar da privacidade (BELLI; VENTURINI, 2016, p. 3-4). Os termos de uso podem ser considerados um meio eficiente e bem adaptado para governar o mundo online, cujos limites devem ser determinados pelas leis (BELLI; VENTURINI, 2016, p. 6). Contudo, esses limites legais são analisados criticamente abaixo, em relação à arquitetura técnica. São esses limites que se encontram nos testes de consentimento.

OS TESTES DE CONSENTIMENTO ESPECIFICAMENTE APLICADOS A SERVIÇOS DE ACESSO À INTERNET E SERVIÇOS DE APLICAÇÃO DA INTERNET DILI

De acordo com o Marco Civil da Internet, "qualquer coleta, uso, armazenamento ou tratamento de dados pessoais requer consentimento expresso do titular dos dados" (BAKER; MCKENZIE, 2016, p. 7). Isso dá origem a dois testes primários de consentimento:

1. O teste claro e compreensivo de informação e finalidade sobre a coleta, o uso, o armazenamento ou tratamento;
2. O teste de consentimento para compartilhar dados com terceiros.[4]

O TESTE CLARO E COMPREENSIVO DE INFORMAÇÃO E FINALIDADE

Esse teste exige que nos perguntemos se o usuário recebeu informações claras e compreensivas ou informações claras e completas sobre a coleta (MEDEIROS; BYGRAVE, 2015), uso, armazenamento, tratamento e prote-

4 Ambos deduzidos a partir do art. 7, incisos VII, VIII e IX, da Lei 12.965 de 2014 - Marco Civil da Internet.

ção de seus dados pessoais, que por sua vez só podem ser utilizados para as seguintes finalidades:[5]

a. finalidades que justifiquem a coleta dos dados pessoais;
b. finalidades que não são proibidas pela lei;
c. finalidades que são especificadas nos contratos de prestação de serviços ou em termos de aplicações de internet.

O TESTE DE CONSENTIMENTO PARA COLETAR, USAR, ARMAZENAR E TRATAR OS DADOS

Nesse teste, devemos fazer as seguintes perguntas:[6]

a. Foi obtido consentimento expresso do usuário para coletar, usar, armazenar e tratar os dados pessoais?;
b. isto foi destacado nos termos contratuais?

O TESTE DE CONSENTIMENTO PARA COMPARTILHAR DADOS COM TERCEIROS

A fim de compartilhar dados pessoais, logs de conexão e dados de acesso a aplicações da internet com terceiros, é preciso determinar se:[7]

a. o consentimento foi livre;
b. o consentimento foi expresso e informado; ou
c. se os dados foram compartilhados dentro de casos previstos em lei.

No que diz respeito ao item c, existiria então a possibilidade de fornecimento dos dados de localização, sem necessidade obtenção do consentimento do usuário, para serem compartilhados com terceiros, desde que previsto em lei. Isso permitiria que órgãos de segurança tivessem acesso o à dados de identificação de dispositivos e informações de localização (DILI). A questão é se uma exceção similar poderia ser feita dentro de uma perspectiva de cidades inteligentes.

---

5 Em consonância com o art. 7º, incisos VIII e VII, da Lei 12.965 de 2014 - Marco Civil da Internet.

6 Também de acordo com o Marco Civil da Internet, em seu art. 7º, inciso IX.

7 De acordo com o Marco Civil da Internet, em seu art. 7º, inciso VII.

Se o indivíduo não sabe como identificar as informações que são compartilhadas e com quem, e a funcionalidade LCS – explicada mais adiante – não foi descrita e explicada a ele, pode-se dizer que o indivíduo recebeu informações claras e compreensivas antes dos dados serem coletados, usados, armazenados, processados e protegidos? Ou isso é uma coleta justificável de dados pessoais? Ou se poderíamos, antes de mais nada, considerar esse tipo de dado como dado pessoal?

DILI: OS NÚMEROS DE IDENTIFICAÇÃO, DADOS DE LOCALIZAÇÃO E IDENTIFICADORES ELETRÔNICOS

Números de identificação, dados de localização ou identificadores eletrônicos podem ser considerados informações pessoais, mas somente se e quando vinculados a uma pessoa.[8] Estas são as modalidades de DILI usadas para se obter a localização de um aparelho e, por conseguinte, do seu usuário. As DILI incluem

> Informações do Sistema Global de Navegação por Satélite, tais como latitude, longitude e, possivelmente, altitude; endereço de assinantes; a IMSI (Identidade Internacional do Assinante Móvel); o *Cell Global Identification* (CGI); a Identificação da Célula (CID)- RTT (round-trip time); os padrões de radiofrequência (RF); o Número de Identidade do Assinante Móvel (MSIN); o Número ISDN da Estação Móvel (MSISDN); a Identidade Internacional do Equipamento Móvel (IMEI); o endereço de controle de acesso à mídia (MAC); o Identificador de Conjunto do Serviço (SSID); e o Serviço Básico Independente (BSS); a Identidade Temporária do Assinante Móvel (TMSI); a Identidade Temporária de Pacotes ao Assinante Móvel (P-TMSI); a Identidade Temporária SAE do Assinante Móvel (S-TMSI); a Temporary Logical Link Identity (TLLI); a *Globally Unique Temporary UE Identity* (GUTI); (CGI) imagens geradas por computador; nome da estação base; nome para cobrança; nome da região metropolitana; estado; latitude da antena; rolamento da antena (antena bearing); nome da célula; tipo de Estação Base; data e hora. (SHANAPINDA, 2016; SHANAPINDA, 2017; TELSTRA CORPORATION LIMITED AND PRIVACY COMMISSIONER, 2015; ETSI, 2016a; ETSI, 2016b)

8 Tal como previsto no Decreto nº 8.771 de 2016, que regulamenta o Marco Civil, em seu art. 14, I.

COMO A FUNCIONALIDADE DE SERVIÇOS DE LOCALIZAÇÃO (LCS) USA A DILI

Os identificadores são utilizados para controlar e rastrear constantemente os dispositivos móveis e equipamentos instalados pelas TelCo's, conforme estes se movem entre as estações-base (BTS). Isto é inerente ao funcionamento dos serviços de localização (LCS), para garantir que a comunicação seja entregue ao dispositivo móvel. Os LCS são uma funcionalidade utilizada pelo dispositivo ou pela aplicação nele instalada para controlá-lo e rastreá-lo, usando a DILI (SHANAPINDA, 2016; SHANAPINDA, 2017). Deste modo, as DILI referem-se ao dispositivo e, então, usando dados de registro tais como detalhes biográficos, residenciais, número do RG ou CPF, número do passaporte, endereço de e-mail ou detalhes de contato e qualificação da pessoa natural, o usuário é identificado e cobrado (ANTONIALLI; ABREU, 2016; MANHEZ FILHO, 2015).[9]

Outra função dos LCS é garantir que o dispositivo correto seja cobrado. As BTS estão localizadas próximas às torres de celular. Elas contêm o Registro de Localização de Unidade Móvel Local – Home Location Register (HLR) – e o Registro de Localização de Unidade Móvel Visitante –Visitor Location Register (VLR) – que atribui e aloca os respectivos identificadores aos dispositivos. Estes identificadores estão armazenados no VLR e no HLR e encontram-se ligados uns aos outros para garantir a identificação precisa.

A Figura 1 demonstrará como as funcionalidades de LCS operam. As DILI estão contidas em sinais de rádio e são transferidas pela rede, de um elemento para o seguinte, até que sejam entregues para o cliente destinatário. A própria aplicação de Internet instalada no dispositivo móvel pode ser esse cliente. O cliente pode ser externo, interconectado como parte de uma cobertura de roaming para celular móvel ou um conteúdo OTT e serviço de mapeamento de comunicações (BELLOVIN *et al*, 2016), por exemplo. Os LCS utilizam estes sinais para calcular a posição do dispositivo, reportando-a de volta ao cliente destinatário (CISCO, 2016; SHAPINDA, 2017). A operação pode ser descrita como se segue:

---

9 De acordo com o Decreto nº 8.771 de 2016, que regulamenta o Marco Civil, em seu art. 11, § 2º, III, que trata dos dados cadastrais; ver também o art. 10 da Resolução da ANATEL nº. 477, de 07 de agosto de 2007, que regulamenta o Serviço Móvel Pessoal; e também BRASIL. The Brazilian Civil Framework of the Internet in English. Law nº. 12,965, of April 23, 2014. Article 10, section. Câmara dos Deputados. Brasília: Documentation and Information Center/Edições Câmara Brasília, 2016, p. 29. Disponível em: <http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf?sequence=1>. Acesso em: 5 maio 2017.

O Subsistema Multimídia IP (IMS) é usado para fornecer conteúdo interativo, texto e voz, que está no centro do conteúdo OTT e dos serviços de comunicação. O IMS Public User Identity (SIP-URI) (ETSI, 2016b, p. 143) e o Número Internacional ISDN da Estação Móvel (MSISDN) (ETSI, 2016b, p. 17) são os dispositivos identificadores-chave de interesse para as agências.

O IMS usa o SIP-URI para encaminhar pedidos de LCS acerca de estimativas de localização para a rede doméstica de um dispositivo. O SIP-URI é usado como a identidade pública do dispositivo na Internet pública. (ETSI, 2016b, p. 143). O MSISDN é o número do dispositivo no IMS. O MSISDN é obtido pela rede doméstica do dispositivo a partir do Home Subscriber Server (HSS) (ETSI, 2016b, p. 27). O MISISDN compreende o CC – Código do país – e o número telemóvel nacional – existente. O número móvel nacional – significativo –, por sua vez, compreende o Código Nacional de Destino (NDC) e o número de assinante (SN) (ETSI, 2016A, p. 22).

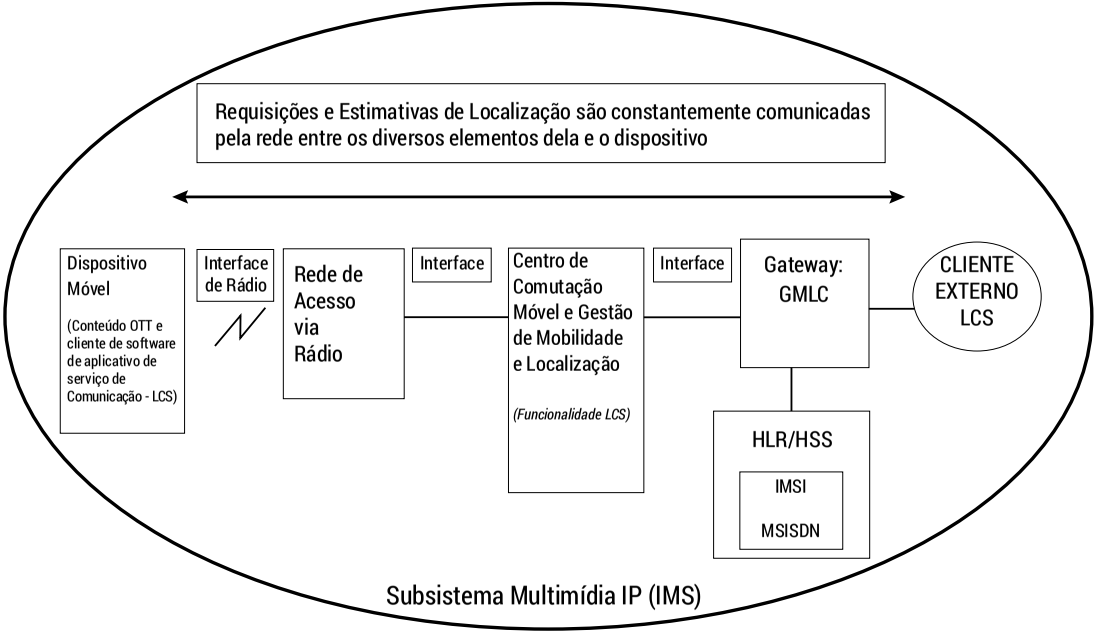
A solicitação de serviços LCS é encaminhada juntamente com o MSISDN pelo SIP-URI das redes domésticas através da interface para o Gateway Mobile Location Center (GMLC) doméstico.

Endereços ou nomes de domínio (DNS) pré-configurados podem ser usados para identificar a rede doméstica do dispositivo a fim de encaminhar as informações. O MSISDN pode ser usado para obter o endereço IP (Internet Protocol) do Registro de Localização de Unidade Móvel Local (HLR).

Pesquisas dos endereços de destino ou Domain Name Server (DNS) pré-configurados podem ser usadas para identificar a rede doméstica do dispositivo, a fim de encaminhar as informações. O MSISDN pode ser usado para obter o endereço IP (Internet Protocol) do Registro de Localização de Unidade Móvel Local (HLR) ou HSS (ETSI, 2016b, p. 143; SHANAPINDA, 2017).

A Figura 1 descreve a arquitetura dos LCS e demonstra a funcionalidade dos LCS na geração e na comunicação de informações de localização e de dispositivos identificadores, conforme discutido acima.

Figura 1. A Funcionalidade e Arquitetura dos LCS



Fonte: Elaborado pelo autor. [10]

10 Uma versão definitiva desta figura, certificada e aprovada após revisão por pares foi publicada no periódico [ISSN 2203-1693, Volume 4, Number 4, December 2016 and http://doi.org/10.18080/ajtde.v4n4.68] e está disponível em: TELSOC. <http://telsoc.org>. Acesso em: 23 ago. 2017.

O cliente externo será o Ponto de Interconexão (POI) com um terceiro (INTVEN, 2000). A interconexão pode ocorrer por componentes físicos, acesso sem fio e software (algoritmos). O ambiente IMS é IP-based. Isto representa um desafio para conhecer ou descobrir o compartilhamento de DILI, seja dentro dos diversos departamentos nacionais e internacionais da Telefônica-Vivo, seja com parceiros externos (BELLOVIN, 2016).

O indivíduo, contudo, desconhece o cálculo da localização e o fato de ele estar sendo comunicado para vários elementos da rede, tal como descrito acima. Os DILI podem ser compartilhados e armazenados para além da rede da TelCo ou com a rede de um terceiro, a fim de, justificadamente, permitir comunicações, tais como o *roaming* de celular. O usuário pode desconhecer o cliente destinatário. Ele também desconhece a arquitetura da rede e de quaisquer redes de interconexão com redes de terceiros. O indivíduo pode não conhecer quem são os diversos atores que podem operar, possuir ou administrar uma determinada parte de equipamento, especialmente dados os acordos de interconexão para intercâmbio de tráfego entre operadores móveis e operadores móveis virtuais e conteúdo OTT e serviços de comunicação.

A questão que se coloca é se seria possível dizer que o indivíduo deu seu consentimento expresso e informado nas circunstâncias acima descritas ao aceitar o *roam* e as notificações nos termos de uso. Por outro lado, se qualquer DILI corresponder ao registro de dados e os identificadores estiverem relacionados a uma pessoa, em qualquer estágio do processo de transferência, entre a rede do operador inicial e do terceiro, isto demonstraria que o consentimento expresso e informado do indivíduo deve ser obtido? Questiona-se quão prático isto seria. Exige-se que certos acordos de interconexão e de *roaming* sejam levados a público. Isto é suficiente? É isto que demonstra o consentimento livre, expresso e informado, para fins práticos? Ou deveria cair na categoria do que é considerado justificável, legal e, portanto, nenhum consentimento deveria ser obtido, na medida em que a interconexão pode ser relevante e parte integrante da entrega do serviço ao indivíduo? Podem os terceiros utilizar as DILI e, se assim o for, o recurso da notificação compreende tal cenário? De forma alternativa, questiona-se qual é o peso do indivíduo sobre as cláusulas de confidencialidade que podem constar desses acordos.

Em nível secundário, se as DILI são então compartilhadas com o propósito de uma cidade inteligente, o consentimento livre e informado do indivíduo requer o respeito de quais DILI? O modelo atual de notificação e privacidade é suficiente ou existe uma alternativa melhor? Com o que este formato alternativo se parece, dadas as descrições técnicas dinâmicas expostas acima?

PROCESSAMENTO DAS DILI E DOS SERVIÇOS DE LOCALIZAÇÃO

O processamento de dados pessoais exige o consentimento prévio e informado do indivíduo. Esse processamento pode ser definido como:

> […] *qualquer* operação realizada com dados pessoais, tais como: coleta, produção, recepção, classificação, uso, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou monitoramento da informação, comunicação, modificação, transferência, difusão ou extração. [11]

A recepção, transmissão, distribuição, processamento, armazenamento, monitoramento de informações, monitoramento de comunicação, a transferência, a difusão e a extração dos DILI entre redes de celular e IP no ambiente IMS; entre as empresas TelCo e de *analytics*; em acordos de interconexão técnica; com aplicações de serviços de mapeamento, podem se qualificar como processamento de dados pessoais. Este processamento relaciona os DILI aos indivíduos, utilizando certos dados de registro. É possível afirmar que as funcionalidades LCS são, portanto, funcionalidades de processamento. Nestas circunstâncias, como pode a TelCo informar o indivíduo de forma compreensível sobre o uso dos DILI e obter o consentimento expresso e informado? A lei é vaga ou ampla demais ou estaria a empresa de TelCo violando disposição legal razoável? As empresas de telefonia afirmam que colaboram com as leis do respectivo país. A lei parece exigir que os indivíduos sejam informados acerca da funcionalidade dos serviços de localização. Os Termos de Uso não parecem fazer referência aos LCS porque se trata de algo total ou parcialmente justificável?

A NÃO-REGULAÇÃO DE DADOS DE LOCALIZAÇÃO DE SERVIÇOS DE TELEFONIA MÓVEL

Os metadados de telefones são "densamente interligados", re-identificáveis e valiosos para fazer inferências de natureza sensível (MAYER; MUTCHLER; MITCHELL, 2016). Diante disso, qual é a posição dos testes de consentimento em relação a DILI geradas a partir de serviços não baseados em IP e que permita o desenvolvimento de uma cidade inteligente?

O Decreto 8771, que regula o Marco Civil da Internet e, por conseguinte, o próprio Marco Civil da Internet, não parece aplicar-se aos serviços de telecomunicações que não se destinem a fornecer acesso à Internet e apli-

11 Tal como disposto no art. 14, II, do Decreto nº 8.771, de 11 de maio de 2016 que regulamenta o Marco Civil da Internet. (grifo nosso)

cações de serviços de Internet (ANTONIALLI; ABREU, 2016). Como tal, não parece haver uma estrutura de compartilhamento de dados para DILI que não seja encaminhada pela Internet para objetivos de conectividade com a Internet e conectividade com aplicações da Internet. Serviços que não são regulados incluem, possivelmente, chamadas de voz no celular e SMSs que não usam endereços IP[12] como seu endereço de rede. Eles podem usar, em vez disso, o número de telefone. Parece que as DILI, no que diz respeito às comunicações celulares, são apenas diretamente reguladas pelas resoluções da ANATEL, que exigem a coleta de dados e seu compartilhamento com órgãos de segurança, com ou sem uma ordem judicial.[13]

Parece ter havido casos em que os dados de localização e registros telefônicos foram partilhados com órgãos de segurança, sem um mandado, com base em interpretações ao abrigo da Lei de Organizações Criminosas (ANTONIALLI; ABREU, 2016). As TelCos são obrigadas a manter os "[…] documentos de faturamento (documentos de natureza fiscal) que contêm dados sobre chamadas recebidas e enviadas, datas, horas, duração e preço, bem como informações de conta de assinantes […]" (ANTONIALLI; ABREU, 2016). Esses documentos incluiriam, muito provavelmente, algumas das DILI descritas acima. DILI tais como: o IMEI; IMSI; ID de celular; a localização; número original chamado; número chamado; data da chamada; duração da chamada; duração da chamada em segundos. Todos esses dados foram legalmente identificados como dados pessoais em outras jurisdições, tal como na Austrália, por exemplo (TELSTRA CORPORATION LIMITED AND PRIVACY COMMISSIONER, 2015; CORTE FEDERAL DA AUSTRÁLIA, 2017).

A questão é, esses mesmos dados de localização podem ser compartilhados para o desenvolvimento de uma cidade inteligente ou outros arranjos comerciais, e em que medida deve ser obtido o consentimento prévio e informado do indivíduo? Um quadro geral que estabeleça a partilha de dados de localização poderá ter que indicar legalmente o seu *status* jurídico e as circunstâncias em que as DILI podem ser partilhadas com a órgãos de segurança e para o desenvolvimento de cidades inteligentes, respectivamente.

---

12 Os registros e detalhes incluem: "[…] a given IP address used at the terminal for incoming and outbound data packets, among other data that permits identification of the access terminal used […]".

13 Resolução nº 426, de 09 de dezembro de 2005. Artigo 22 e Resolução nº 614, de 28 de maio de 2013. Artigo 53.

Alternativamente, isso significa que as TelCo podem compartilhar comunicações celulares DILI sem quaisquer restrições, na ausência de uma lei geral de proteção de dados? (KIRA; TAMBELLI, 2017). Se uma lei desse tipo fosse aprovada, como iria tratar de DILI usadas somente em comunicações celulares, para fins de segurança e iniciativas de cidades inteligentes?

OS TERMOS DE SERVIÇO DA TELEFÔNICA-VIVO

A Telefônica-Vivo Brasil afirma que só utiliza as informações coletadas para oferecer serviços contratados e proporcionar uma melhor experiência e atender às necessidades do cliente (TELEFÓNICA S.A., 2017). Isso é bastante vago e limita o uso apenas aos serviços já contratados, ao contrário da política da empresa-mãe.

Existe uma preferência para que qualquer informação recolhida é seja processada internamente. Ela pode ser compartilhada globalmente e processada dentro do Grupo Telefônica de empresas ou de empresas parceiras, apenas por razões de segurança, aparentemente (TELEFÓNICA GROUP, 2017). Isto implica possíveis interconexões entre as redes do Grupo Telefônica. Dado o regime de interconexão, com outras TelCo, ISPs, servidores web, arranjos via satélite e como o LCS opera, seria interessante ver como o consentimento livre, expresso e informado dos clientes é obtido nessas circunstâncias.

A expressão "consentimento da pessoa envolvida" é definida como "Qualquer manifestação de vontade livre, específica e informada, através da qual o interessado aceita o tratamento de dados pessoais que lhes digam respeito, seja por meio de uma declaração, seja por uma ação clara" (TELEFÓNICA GROUP, 2017). Não há menção aos termos "expressa" ou "consentimento". Em outras palavras, a aceitação é consentimento e ela pode ser implícita. Isto parece contradizer o que os testes de consentimento exigem.

A Telefônica-Vivo não especifica claramente se compartilha as DILI com outros fins comerciais que não estejam relacionados à cobrança, à aplicação da lei e não relacionados à qualidade do serviço. A expressão "outras finalidades", nos seus termos, é vaga e sujeita à má utilização. Dado que a Telefônica-Vivo não especifica explicitamente a partilha de dados para objetivos de cidade inteligente nos seus termos de serviço, que parecem vagas e contraditórias, não se sabe se tal objetivo será legítimo.

ANÁLISE CRÍTICA DOS TERMOS DE USO

A Telefônica-Vivo afirma que respeita a privacidade e a proteção de informações pessoais. A questão é que tipos de DILI considera pessoais e quais não. Desta forma, ela se encontra numa posição única para decidir unilateralmente quais os propósitos de uso dessas informações que requerem consentimento e que tipo de consentimento. A questão mais importante é quais tipos de DILI a lei protege, de modo que a Telefônica-Vivo garanta o seu cumprimento. A empresa sequer menciona um tipo específico de DILI ou explica a funcionalidade LCS. Essa política só parece abranger especificamente usuários acessando sites da Telefônica-Vivo.

Estaria a Telefônica-Vivo autorizada a coletar DILI e compartilhá-la com órgãos de gestão de desastres ou com autoridades municipais de planejamento urbano e gestão de tráfego, dada a imprecisão de suas políticas de privacidade? Essas políticas, por sua vez, parecem basear-se na vagueza da lei em relação às DILI de serviços de telefonia celular móvel.

Estaria também a Telefônica-Vivo está em conformidade com as disposições do Marco Civil da Internet e do Decreto 8771, de 11 de maio de 2016, em relação aos serviços de acesso à Internet? A funcionalidade LoCation Services, no entanto, opera indiscriminadamente em ambos os ambientes. DILI é compartilhado entre serviços e aplicações, independentemente do serviço final consumido, e é principalmente as mesmas DILI compartilhadas, entre celulares e aplicações de serviço de internet. Se você coletar as DILI para um serviço, é provável que as tenha para o outro.

A Telefônica não mencionou os terceiros com os quais está interconectada e com quem compartilha as DILI para seus aplicativos de internet ou para fornecer acesso à web, como partes que administram, possuem e operam servidores web ou a configuração estrutural da funcionalidade LCS. Assim, até que ponto devem os terceiros interligados à rede física e lógica da TelCo serem identificados para o indivíduo? O que seria necessário para o indivíduo tomar uma decisão informada e o que seria excessivo para as TelCo e informação demais para o indivíduo? Até que ponto as empresas de análise de dados devem ser identificadas? Até que ponto o propósito de usar esses dados para iniciativas de cidade inteligente deve ser identificado e ser explicitado? Em que medida as DILI devem ser especificadas e explicadas ao indivíduo, dadas as denúncias de que a Telefônica-Vivo vende dados para terceiros na América Latina? (LISSARDY, 2017). O desafio consiste em elaborar o formato sob o qual se pode dizer que o indivíduo foi informado de forma clara e abrangente a respeito dos metadados recolhidos e dos vários fins para os quais foram utilizados e obter o consentimento

previamente. Além disso, o objetivo é evitar o mau uso dos dados. Como isso pode ser conseguido nas atuais circunstâncias não é claro.

Diante disso, a própria lei pode ser reivindicada como vaga e pouco clara. Ela parece não identificar especificamente quais tipos de DILI são considerados dados de localização, para os quais deve ser obtido o consentimento informado. Também não parece indicar suficientemente o que significa informação abrangente. Dada a complexidade da arquitetura técnica, como demonstrado pela funcionalidade LoCation Services, talvez seja necessário desenhar linhas claras, mas onde e como?

CONCLUSÃO

Registros de informações de chamadas, informações de localização de celular geradas por serviços de comunicações baseados ou não em IP podem ser reorientados para uma miríade de metas de entrega de serviço público, pensando em uma perspectiva de cidades inteligentes. O desafio é como obter o consentimento livre e esclarecido prévio do indivíduo em cada etapa da coleta, uso, compartilhamento, processamento e proteção dos dados pessoais, a fim de garantir a conformidade legal e evitar o uso indevido. No entanto, não reconhecer como dados pessoais os dados de localização relacionados com serviços não relativos a IP, no âmbito do regime de proteção de dados existente, cria uma lacuna de proteção que pode ser suscetível a mau uso se ainda não o tiver feito. Os termos de uso da Telefônica-Vivo não informam o usuário, de modo detalhado, sobre seus direitos legais com relação a qualquer tipo de serviço. Independentemente dessas incertezas legais e das complexidades técnicas, não parece que o indivíduo receba informações suficientemente abrangentes para poder dar o seu consentimento livre, expresso e informado para a utilização, partilha e processamento das DILI.

Qualquer estrutura que vise a incentivar a partilha de dados para iniciativas de cidades inteligentes teria de reconhecer a privacidade e o caráter pessoal das DILI, garantindo a sua proteção contra o uso indevido. Dado o quão interconectadas e convergentes são as comunicações multimídia, de celular e de linha fixa em uma rede IMS digital, as resoluções da ANATEL e os vários estatutos exigem um alinhamento. A ANATEL, nas suas resoluções, e o Poder Legislativo deveriam considerar os tipos de DILI e delimitar claramente quais são podem ser classificados como dados pessoais, cuja cobrança e uso irão requerer um mandado judicial e o consentimento individual livre, expresso e informado. Um vocabulário e um sistema de classificação podem ser desenvolvidos para ajudar com os

esclarecimentos técnicos e legais. As TelCo podem então ter deveres legais claros, aplicando os testes de consentimento em seus acordos técnicos e comerciais que afetam a privacidade do usuário, algo que atualmente parece inexistente, em sua maior parte.

Um *framework* de consentimento informado precisa ser desenvolvido para avaliar como o consentimento expresso e livre deve ser obtido do indivíduo. No cerne está a questão de como o indivíduo permanece informado, bem como em que fase pode ser considerado justificável que ele não o seja, com base no que é prático e no risco de uso indevido.

REFERÊNCIAS

ANTONIALLI, D.; ABREU, J. DE S. State Surveillance of Communications in Brazil and the Protection of Fundamental Rights. [S.l.]: Electronic Frontier Foundation/ InternetLab, 2016. Disponível em: <https://necessaryandproportionate.org/files/brazil-en-march2016.pdf>. Acesso em: 5 maio 2017.

ASOCIACIÓN POR LOS DERECHOS CIVILES AND INTERNET LAB. *Políticas de protección de datos personales en las empresas de telecomunicaciones:* estudio de casos de Argentina, Brasil, Chile y México. [S.l.]: ADC, 2016. v. 2. Disponível em: <https://adcdigital.org.ar/wp-content/uploads/2017/02/Politicas-proteccion-datos-personales-telcos.pdf>. Acesso em: 5 maio 2017.

BAKER; MCKENZIE. 2016 Global Data Protection Enforcement Report – Enforcement by Regulators: Penalties, Powers and Risks. International Association of Privacy Professionals, jan. 2016. Disponível em: <https://iapp.org/media/pdf/resource_center/BM-2016-Global-Enforcement-Report.pdf>. Acesso em: 5 maio 2017.

BELLI, L.; SCHWARTZ, M.; LOUZADA, L. Selling your Soul While Negotiating the Conditions: from Notice and Consent to Data Control by Design. Health Technol., 2017. Disponível em: <https://link.springer.com/article/10.1007/s12553-017-0185-3>. Acesso em: 5 maio 2017.

BELLI, L.; VENTURINI, J. Private Ordering and the Rise of Terms of Service as Cyber-regulation. *Internet Policy Review*, v. 5, n. 4, p. 1-17, maio 2016.

BELLOVIN, S. M.; BLAZE, M.; LANDAU, S.; PELL, S. K. It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law. *Harvard Journal of Law and Technology*, v. 30, n. 1, p. 1-101, 2016.

CISCO, S. I. Location Services. In.: CISCO, S. I. (Ed.). *MME Administration Guide, StarOS Release 21*. California: Cisco Systems, Inc., 2016. p. 297-310. v. 21.

CORTE FEDERAL DA AUSTRÁLIA. Privacy Commissioner v Telstra Corporation Limited. FCAFC 4. VID 38 of 2016. 19 jan. 2017. Disponível em: <http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/full/2017/2017fcafc000>. Acesso em: 5 maio 2017.

DAHLMANN, A.; VENTURINI, J.; DICKOW, M.; MACIEL, M. Privacy and Surveillance in the Digital Age: a Comparative Study of the Brazilian and German Legal Frameworks, mar. 2016. [no prelo]

DEAKIN, M.; AL W. H. From Intelligent to Smart Cities. *Journal of Intelligent Buildings International*, v. 3, n. 3, p. 140-152, jul. 2011.

EFF; INTERNETLAB. Quem defende seus dados? Disponível em: <http://quemdefendeseusdados.org.br/en/>. Acesso em: 5 maio 2017.

ETSI. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification. Sophia Antipolis Cedex - France: ETSI, 2016a.

ETSI. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Functional stage 2 description of Location Services (LCS) (3GPP TS 23.271 version 13.0.0 Release 13). Sophia Antipolis Cedex - France: ETSI, 2016b.

FILHO, A. S.; SCHWARTZ, D.; ANDRÉ. G. Big data – Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. *Conpedi Law Review,* v. 2, n. 3, p. 311-331, jun. 2016. Disponível em: <http://portaltutor.com/index.php/conpedireview/article/view/314>. Acesso em: 5 maio 2017.

INTVEN, H. Telecommunications Regulation Handbook, Module 3. Washington, D.C.: World Bank, 2000.

KIRA, B.; TAMBELLI, C. N. Data Protection In Brazil: Critical Analysis Of The Brazilian Legislation. Internetlab, 2016. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2017/03/Legal-Framework-Analysis-Brazil.pdf>. Acesso em: 5 maio 2017.

KOMNINOS, N. Intelligent Cities: Towards Interactive and Global Innovation Environments'. *International Journal of Innovation and Regional Development*, v. 1, n. 4, p. 337-355, 2009.

KUIAWINSKI, R. Z. Análise crítica sobre a nova lei de organização criminosa no combate ao crime organizado. 13. ed. *Anais da Semana Acadêmica Fadisma Entrementes.* 2016. Disponível em: <http://sites.fadisma.com.br/entrementes/anais/wp-content/uploads/2016/09/analise-critica-sobre-a-nova-lei-de-organizacao-criminosa-no-combate-ao-crime-organizado.pdf>. Acesso em: 5 maio 2017.

LISSARDY, Gerardo. 'Despreparada para a era digital, a democracia está sendo destruída', afirma guru do 'big data'. BBC, Nova York, 9 abr. 2017. Disponível em: <http://www.bbc.com/portuguese/geral-39535650#>. Acesso em: 5 maio 2017.

MANHEZ FILHO, José. Organização Criminosa – Lei 12.850/13 – Ação controlada, infiltração de agentes e acesso a registros. Faculdade EDUVALE, out. 2015. Disponível em: <http://www.eduvaleavare.com.br/wp-content/uploads/2015/10/organizacao.pdf>. Acesso em: 5 maio 2017.

MAYER, Jonathan; MUTCHLER, Patrick; MITCHELL, John C. Evaluating the Privacy Properties of Telephone Metadata. *Proceedings of the National Academy of Sciences*, v. 114, n. 20, p. 5536-5541, 2016.

MEDEIROS, F. A.; BYGRAVE, L. A.. Brazil's Marco Civil da Internet: Does it Live Up to the Hype? *Computer Law & Security Review*, v. 31, n. 1, 2015, p. 120-130.

OPEN DATA INSTITUTE. What Is Data Infrastructure? Disponível em: <https://theodi.org/what-is-data-infrastructure>. Acesso em: 12 abr. 2017.

SHANAPINDA, S. Retention and Disclosure of Location Information and Location Identifiers OTT Content and Communication Services. *Australian Journal of Telecommunications and the Digital Economy*, v. 4, n. 4, p. 251-279, 2017. Disponível em: <https://telsoc.org/ajtde/index.php/ajtde/article/view/68>. Acesso em: 11 jan. 2017.

SHANAPINDA, S.. The Types of Telecommunications Device Identification and Location Approximation Metadata: Under Australia's Warrantless Mandatory Metadata Retention and Disclosure Laws. *Communications Law Bulletin*, v. 35, n. 3, p. 17-19, 2016. Disponível em: <http://www.camla.org.au/communications--law-bulletin/>. Acesso em: 5 maio 2017.

TELEFÓNICA GROUP. *Privacy Policy of the Telefónica Group*. 2. ed. Madrid: Telefónica S.A., dez. 2015. Disponível em: <https://www.telefonica.com/documents/1258915/3538310/privacy_policy_EN.pdf/6c122ed0-88e1-4843-8523-948ffd4ea3f5>. Acesso em: 5 maio 2017.

TELEFÓNICA S. A. Política de privacidade. Disponível em: <http://www.telefonica.com.br/servlet/Satellite?c=Page&cid=1386094985990&pagename=InstitucionalVivo%2FPage%2FTemplateConteudoFull>. Acesso em: 5 maio 2017.

TELSOC. <http://telsoc.org>. Acesso em: 23 ago. 2017.

TELSTRA CORPORATION LIMITED AND PRIVACY COMMISSIONER [2015] AATA 991 (18 December 2015) (Administrative Appeals Tribunal of Australia 2015).

TORRES JÚNIOR, Paulo Fernandes Moreira. O direito à privacidade e à intimidade na Internet. Repositório Institucional Tiradentes, jul. 2016. Disponível em: <http://openrit.grupotiradentes.com/xmlui/handle/set/1172>. Acesso em: 5 maio 2017.

QUEM MEXEU NO MEU "PORN"? BREVES APONTAMENTOS ACERCA DA RELAÇÃO ENTRE O DIREITO, A TECNOLOGIA E A INDÚSTRIA DO SEXO

NATHALIA FODITSCH

INTRODUÇÃO

Sexo e pornografia, um assunto que permeia várias áreas do Direito. Como é possível, portanto, que se trate tão pouco de tais temas, ao menos no que se refere à sua interface com o Direito e o desenvolvimento tecnológico? Há algum papel a ser desempenhado pelo Estado neste debate? Deve tal tema ser discutido de forma ampla ou se trata de algo de foro íntimo, que não deve ser trazido à tona, e muito menos no âmbito de um livro como este? Estes são questionamentos que me faço há alguns anos.

Minha carreira tem sido dedicada ao desenvolvimento das comunicações. Há alguns anos, quando trabalhava com projetos de infraestrutura de banda larga no Banco Interamericano de Desenvolvimento (BID) me deparei com diferentes textos informando que aproximadamente 60% do tráfico da Internet vem de sítios de conteúdo adulto, estatística que já foi declarada falaciosa por alguns especialistas.[1] Me perguntei à época, se por meio do meu trabalho eu estaria dedicando um tempo considerável à indústria do sexo e à pornografia, mesmo que indiretamente. Percebi que se trata de um tema de grande relevância, ainda que pouco discutido em certas esferas,

1 Veja, por exemplo, a apresentação da consultoria *Telegeography* (vídeo), dizendo que se trata de um mito a estimativa de que seria em torno de dois terços o total de tráfego de dados relacionados a conteúdo adulto. Ver: SIMPSON, Thomas. Mythbusters: Revenge of the Cable Myths, Part III. TeleGeography, 14 jul. 2016. <http://blog.telegeography.com/mythbusters-revenge-of-the-cable-myths-part-iii>.

como as da direito, política e regulação[2] (WOSICK, 2015).[3] Mesmo sem adentrar em quaisquer discussões relacionadas ao mérito desta indústria ou seu impacto, é impossível ignorar, por exemplo, que ela movimenta grandes montantes, chegando a arrecadar até US$60 bilhões por ano no mundo (WOSICK, 2015), embora muitas das estimativas a ela relacionadas não sejam confiáveis (DARLING, 2014; ALTAWEEL, 2017; SULLIVAN; MCKEE, 2015). O maior portal *on-line* de conteúdo pornográfico conta com mais de 75 milhões de acessos diariamente, ou seja, é o 39º sítio da Internet mais acessado no mundo e o 24º sítio mais acessado nos Estados Unidos.[4] No Brasil, um outro portal, também com conteúdo pornográfico, aparece em 17º lugar no *ranking* geral do país.[5]

A crescente evolução da indústria do sexo e a adoção e o uso de conteúdos pornográficos traz consigo implicações jurídicas, econômicas, e até mesmo políticas. Assim, entender o funcionamento de tal indústria, o impacto exercido pelo desenvolvimento tecnológico em suas mudanças, e sua relação com a Internet são exemplos de reflexões necessárias e relevantes. Da mesma forma, é importante pensar se o Estado deve ou não interferir na referida indústria. Nos Estados Unidos, debates relacionados aos limites da intervenção do Estado no que concerne à pornografia ocorrem há décadas. Uma frase citada em muitos trabalhos acadêmicos relacionados, data de 1964, quando o Juiz Potter Stewart, da Suprema Corte americana, disse não ser necessário adentrar no que pode ser definido como "obsceno" ou "pornográfico" afirmando apenas "Eu sei quando vejo".[6][7] Edelman (2009) explica que nos Estados Unidos o tema do conteúdo de entretenimento adulto já foi discutido em diversos projetos de lei e também permeou o

2 Não adentrarei no debate acerca das razões pelas quais o tema ainda é pouco debatido. Entre elas, sem dúvidas, estão os tabus relacionados a tudo que envolve a sexualidade humana.

3 Há um crescente interesse no tema por parte de profissionais de humanas e das ciências sociais.

4 Dados coletados por meio do portal Alexa. Acesso em maio de 2017. O sítio em questão é o Pornhub. Mais informações podem ser acessadas em: RANKS, Alexa Traffic. How popular is pornhub.com? Disponível em: <http://www.alexa.com/siteinfo/pornhub.com>. Acesso em: 17 dez. 2018.

5 Dados coletados por meio do portal Alexa. Acesso em maio de 2017. O sítio em questão é o XVideos. Mais informações podem ser acessadas em: ALEXA. Top Sites in Brazil. Disponível em: <http://www.alexa.com/topsites/countries/BR>. Acesso em: 17 dez. 2018.

6 No original: "I know it when I see it"

7 Jacobellis v. Ohio, 378 U.S. 184 (1964).

debate de leis que foram aprovadas. Discutiu-se, por exemplo, até que ponto a pornografia está ou não contemplada pela Primeira Emenda da Constituição, que protege a liberdade de expressão[8].

No Brasil, o debate acerca de questões jurídico-regulatórias envolvendo a indústria do sexo e a pornografia é quase inexistente. De todo modo, o consumo de pornografia online no país apresenta dados curiosos. De acordo com dados referentes ao ano de 2016, o Brasil está entre os países no mundo com a maior quantidade de tráfego.[9] Um grande número dos acessos a tais conteúdos – 43% – é feita por menores de 24 anos de idade, e a porcentagem de acesso por mulheres é superior do que a média mundial –33% Brasil v. 25% média mundial.[10] Além disso, o país está entre os dez países com o maior número de atrizes na indústria pornográfica (MILLWARD, 2013).

Embora a relação entre o Direito, a tecnologia e a pornografia ainda seja pouco explorada no Brasil, a chamada "pornografia de vingança" é discutida há vários anos, inclusive no âmbito do Judiciário e do Legislativo, por meio de Projetos de Lei. Esta prática, que ocorre quando imagens ou vídeos com conteúdos íntimos são compartilhados – geralmente pela Internet – sem prévio consentimento, foi explorada no estudo de Valente *et al.* (2016), dedicado inteiramente ao tema, no qual se destaca que existem instrumentos a serem usados contra esta prática, tanto na esfera penal como na civil (VALENTE *et al*, 2016).[11] Embora a "pornografia de vingança" seja

---

8 Kathleen Ann Ruane (2014) explica que a Suprema Corte americana determinou por meio de sua jurisprudência, tipos de expressão que não são contempladas pela referida Emenda, quais sejam: (i) a pornografia infantil; (ii) o discurso obsceno; e (iii) a expressão que gera "reais ameaças". Veja também a pesquisa de Isabella Frajhof, que analisou decisões americanas relacionadas ao "discurso obsceno", que é uma das formas de expressão que não estão contempladas pela Primeira Emenda nos Estados Unidos.

9 Veja: PORN HUB INSIGHTS. Pornhub's 2016 Year in Review. Disponível em:<https://www.pornhub.com/insights/2016-year-in-review>. Acesso em: 17 dez. 2018. Veja também: PORN HUB INSIGHTS. Redtube & Brazil. Disponível em: <https://www.pornhub.com/insights/redtube-brazil>. Acesso em: 17 dez. 2018.

10 Veja: PORN HUB INSIGHTS. Pornhub's 2016 Year in Review. Disponível em:<https://www.pornhub.com/insights/2016-year-in-review>. Acesso em: 17 dez. 2018. Veja também: PORN HUB INSIGHTS. Redtube & Brazil. Disponível em: <https://www.pornhub.com/insights/redtube-brazil>. Acesso em: 17 dez. 2018.

11 Não obstante, o estudo destacou também uma série de entraves no que se refere à defesa dos direitos das pessoas que têm estes conteúdos expostos.

um tema de grande relevância e complexidade, há muitos outros temas envolvendo a indústria do sexo e a pornografia que devem ser debatidos.

Abordarei abaixo de forma breve:

i. o que são a indústria do sexo e a pornografia;

ii. de que forma elas estão ligadas às variadas áreas do direito e da tecnologia;

iii. a relação entre privacidade, a pornografia e a "Internet das Coisas do Sexo".

Por fim, farei breves considerações a respeito da evolução da tecnologia, de sua influência na indústria do sexo, e das razões pelas quais o debate acerca deste tema deveria ser promovido.

A INDÚSTRIA DO SEXO E A PORNOGRAFIA: O QUE SÃO?

Este artigo se referirá à indústria do sexo em sentido mais amplo, que abarca serviços e produtos assim como a pornografia. Quando comercializada, portanto, a pornografia é parte da indústria do sexo. De acordo com o que explica Tarrant (2016), a expressão pornografia refere-se a conteúdos cujo objetivo é provocar a excitação sexual em uma pessoa, algo que já era visto até mesmo em livros publicados no século XVIII, e logo depois na fotografia e no cinema. Filmes franceses e alemães introduziram conteúdos cinematográficos explícitos já no final da primeira década do século XX (TARRANT, 2016). Desde então, tecnologias mudaram, possibilitando novas formas de produção e distribuição de conteúdo. A convergência de plataformas também transformou a pornografia, possibilitando que conteúdos sejam acessados de diferentes formas. Hoje em dia, quando se fala em pornografia, a correlação com vídeos na Internet é feita quase que imediatamente, uma vez que o consumo tem aumentado de forma galopante ao redor do mundo.

Embora conteúdos pornográficos tenham sido produzidos há séculos, a facilidade de produção e distribuição trazida pela Internet trouxe uma dinâmica sem precedentes para a indústria. A pornografia foi transformada em uma *commodity* e forças de mercado puderam operar mais do que nunca. Um exemplo de tal dinâmica é a existência de um conglomerado dono de várias empresas relacionadas à indústria pornográfica – o *Mindgeek* – que atua na produção de conteúdos e também na distribuição. O conglomerado também lançou, por exemplo, um selo musical em 2014 e um cassino *on-line* em 2016. O aumento do poder do MindGeek ocorreu em poucos anos, e em 2012 a consolidação dos portais de distribuição de conteúdo pornográfico começou a ocorrer (THE ECONOMIST, 2015).

Como é possível notar, há um movimento de integração vertical e horizontal da indústria pornográfica. Muitos dizem que o grupo esta integração é liderada pela MindGeek apenas, mas é difícil afirmar com segurança qual seria o real poder de mercado de tal empresa. No entanto, ao que parece, tal consolidação passou longe dos olhos dos órgãos responsáveis pelo controle de concentração. As consequências relacionadas a esta consolidação devem ir além de questões econômicas e de mercado. Na Inglaterra, por exemplo, o Digital Economy Act, aprovado em 2017 tem uma parte inteira dedicada à pornografia *on-line*, e estabelece regras estritas para evitar que menores de 18 anos acessem tais conteúdos. Muitos dos veículos de mídia, contudo, ressaltaram o poder que a MindGeek terá caso dados cadastrais sejam mandatórios, sendo que a empresa teve ativo papel nas discussões jurídico-regulatórias e tentou impor seu próprio sistema de verificação de identidade (VAAS, 2017). Além disso, também é possível esperar variados e importantes impactos de cunho sociocultural e comportamental decorrentes desta concentração. No entanto, não nos dedicaremos a discuti-los no presente texto.

A INDÚSTRIA DO SEXO E O DIREITO

A indústria do sexo relaciona-se com as mais variadas áreas do direito e com importantes discussões relacionadas às políticas públicas. Um exemplo é sua conexão com a inovação. Um artigo acadêmico publicado há mais de vinte anos já argumentava que a pornografia "encoraja a experimentação de novas mídias" (JOHNSON, 1996, p. 218, tradução nossa). Anos depois, na Conferência Arse Eletronika, realizada na Áustria em 2015, discutiu-se a relação existente entre as novas tecnologias que estão sendo desenvolvidas e a ideia de "código aberto" (*open source*).[12] Foi levantado o argumento, inclusive, de que os "brinquedos" sexuais trazem inovações à toda indústria de eletrônicos.[13]

Até mesmo questões de propriedade intelectual e concorrência têm interfaces com a indústria em questão. Um exemplo é o fato de que o MindGeek, conglomerado citado acima, está envolvido em disputas judiciais relacionadas à propriedade intelectual dos vídeos acessados em seus portais, sendo autora de uma ação e ré em outra (THOMSEN, 2015). Uma

12 Veja: ARSE ELETRONIKA. Arse Elektronika San Francisco 2015 Disponível em: <http://www.monochrom.at/arse-elektronika/talkabstracts.html>. Acesso em: 17 dez. 2018.

13 Veja o argumento da empresa Comingle, apresentado em: ARSE ELETRONIKA. Arse Elektronika San Francisco 2015 Disponível em: <http://www.monochrom.at/arse-elektronika/talkabstracts.html>. Acesso em: 17 dez. 2018.

outra questão de propriedade intelectual refere-se a patentes e "brinquedos" sexuais. Como exemplo, um acordo firmado em 2016 entre a empresa sueca Leloi AB e a empresa canadense rival Standard Innovation Corp. estabeleceu o licenciamento das patentes entre as respectivas empresas (BULTMAN, 2016).

O direito concorrencial também tem uma interface com o MindGeek, que esteve envolvido em um disputa antitruste relacionada aos nomes de domínio XXX, voltados para o entretenimento adulto e oferecidos pela primeira vez em 2011.[14] O MindGeek alegou, entre outras coisas, que o estabelecimento do domínio XXX pela Corporação para Atribuição de Nomes e Números na Internet (ICANN) corresponderia a uma conduta monopolística, e que estava sendo vítima de práticas anticompetitivas que prejudicariam seus negócios e consumidores.[15] Esta relação com a ICANN revela curiosas conexões da indústria pornográfica com instituições basilares para o desenvolvimento da tecnologia e até mesmo com a chamada "governança da Internet". Poucos já pararam para pensar a respeito destas interfaces.

Conforme podemos notar, a indústria em questão se relaciona com os mais variados aspectos jurídicos. Uma das questões fundamentais, no entanto, é a forma pela qual a privacidade e os dados pessoais são afetados. Tais questões serão abordadas a seguir.

PRIVACIDADE E DADOS PESSOAIS

Imagine um mundo no qual informações acerca de suas preferências sexuais podem ser acessadas por diferentes partes, tais como a empresa provedora do acesso à Internet ou empresas que distribuem conteúdos *on-line*. Imagine, ainda, que a *webcam* do seu computador pode ser *hackeada* a qualquer momento, e, portanto, que suas imagens e vídeo podem ser acessadas. Este não é o futuro. Este é o presente. Não obstante, tanto no Brasil como em outros países, a discussão relacionada à privacidade e à proteção dos dados pessoais daqueles que consomem conteúdos adultos *on-line*, ou compram objetos sexuais é quase inexistente.

14 Veja o caso resolvido em 2013 por meio de um acordo extrajudicial. Cf.: ICANN History Project. Manwin Licensing International v. ICM Registry, et al. Disponível em: <https://www.icann.org/resources/pages/manwin-v-icm-2012-02-25-en>. Acesso em: 17 dez. 2018.

15 Veja a petição inicial da Manwin, empresa que foi comprada pela MindGeek. ICANN History Project.Manwin Licensing International v. ICM Registry, et al. Disponível em: <https://www.icann.org/en/system/files/files/complaint-16nov11-en.pdf>. Acesso em: 17 dez. 2018.

Muito embora a discussão acerca de toda a complexidade da indústria do sexo seja incipiente, hoje a "repressão penal em função de posse de pornografia, os vazamentos de informações privadas em larga escala, e as crescentes tentativas de extorsão decorrentes de informações pessoais coletadas online" (ALTAWEEL *et al.*, 2017, p. 11, tradução nossa) são comuns. Assim, talvez tenha chegado a hora de enfrentar o assunto de maneira mais profunda. Tais assuntos devem deixar de serem tratados como tabu para que seus aspectos sociais, econômicos, políticos e regulatórios possam ser debatidos.

Embora o debate pertinente à privacidade e sua relação com os conteúdos adultos ainda seja incipiente, já podemos notar algumas ações. Um exemplo é uma iniciativa do Center for Democracy & Technology (CDT), do Free Speech Coalition (FSC) e demais parceiros, cujo objetivo é aumentar a adoção do "Protocolo Seguro de Transferência de Hipertexto" (HTTPS) em sítios de conteúdo adulto (HALL; NORCIE, 2016). A função do HTTPS é incrementar a proteção dos dados transmitidos entre o computador e o servidor. Com tal protocolo, é mais difícil, por exemplo, que governos acessem as informações transmitidas ou que *hackers* consigam usar páginas da web para executar um ataque distribuído de negação de serviço (DDos) (HALL; NORCIE, 2016). Um estudo apresentado em uma conferência sobre privacidade organizada pela Comissão Federal de Comércio (FTC) dos Estados Unidos analisou onze portais de pornografia mais populares e concluiu que apenas dois usavam HTTPS de forma automática e um deles possibilitava a escolha desta opção (ALTAWEEL *et al.*, 2017). Podemos especular que se existisse ao menos uma boa autorregulação por parte das empresas na indústria em questão, o uso do protocolo HTTPS não seria uma novidade. De todo modo, mudanças começam a ser implementadas. O recente debate nos Estados Unidos relacionado ao histórico de navegação dos usuários de Internet e a possibilidade do uso de tal histórico pelos provedores de acesso à Internet, também está fazendo com que os maiores portais de conteúdo adulto adotem o HTTPS (FUNG, 2017a e FUNG, 2017b).

A organização Eletronic Frontier Foundation (EFF) explica as variadas práticas dos provedores em relação aos dados dos usuários, que incluem: (i) a venda dos dados para empresas de marketing; (ii) a apropriação do conteúdo dos termos buscados pelos usuários; (iii) a interceptação de tráfego e inserção de anúncios publicitários; (iv) a pré instalação de software nos aparelhos de celular de forma que todas as URL são gravadas; (v) a introdução de *cookies* que não são passiveis de detecção, não podem ser deletados e rastreiam todo o seu trafego online (GILLULA, 2017).

Até mesmo as categorias e termos buscados por usuários são facilmente vazados para terceiros, tais como o Google Analytics ou o Yandex – baseado na Rússia – (ALTAWEEL *et al.*, 2017). Assim, não apenas informações sobre as páginas acessadas podem ser descobertas por terceiros, mas também preferências específicas dos usuários. Em 2010, pesquisadores baseados na Áustria, França e Estados Unidos analisaram quase 270 mil páginas de sítios pornográficos *on-line*, tanto pagos como não pagos e descobriram que 3,23% deles têm alguma conduta mal-intencionada (por exemplo, servem de vetor de diferentes tipos de *malware*) e a que segurança destes sítios da web, de acordo com os pesquisadores, é pífia (WONDRACEK *et al.*, 2010). Contudo, estudos também revelam paradoxos: em 98,2% dos casos nos quais um código malicioso foi encontrado, tal código não havia sido originalmente criado pelos próprios sítios analisados (WONDRACEK *et al.*, 2010). Assim, na grande maioria dos casos, tais sítios haviam sido explorados por terceiros, não pelo sítio eletrônico acessado. Além disso, o número de *cookies* gerados pelos sítios pornográficos *on-line* é menor do que a média dos demais sítios (ALTAWEEL *et al.*, 2017), e os mesmos seguem as regras estabelecidos pelo FTC referentes ao compartilhamento de dados, e transparência em relação à coleta e ao tratamento de dados, mais do que fazem sítios em outras indústrias (MAROTTA-WURGLER, 2016).

A "INTERNET DAS COISAS DO SEXO"

A indústria do sexo está mudando e se adequando a diferentes dinâmicas competitivas. Existe uma oferta abundante de conteúdos, uma vez que barreiras à entrada são poucas, que há uma fácil substituição de conteúdos e que os sítios mais populares oferecem conteúdos gratuitamente e em larga escala, uma vez que sua receita vem de anúncios (DARLING, 2014).[16] Além disso, oferta de serviços, experiências e de interatividade tem sido o novo foco da indústria (DARLING, 2014).[17,]

16 O modelo tradicional da indústria audiovisual depende em grande parte da proteção de direitos autorais, mas infrações de direitos autorais são muito comuns na indústria dos conteúdos adultos.

17 Uma conferência chamada de "CamCom" realizada nos Estados Unidos, por exemplo, direciona-se especificamente a modelos que produzem conteúdo adulto online em tempo real. A existência de tal conferência e seu grau de especialização são indícios desta busca pela interatividade. Veja: THANK YOU VERY MUCH FOR MAKING HISTORY WITH US! STAY TUNED FOR UPCOMING DATES. #CAMCON2018. Disponível em: <http://www.cammingcon.com/>. Acesso em: 17 dez. 2018.

A interatividade deverá crescer ainda mais, uma vez que os conceitos de "realidade virtual" (RV) e "realidade aumentada" (RA) deverão se aproximar cada vez mais da pornografia e do sexo. Por exemplo, vídeos 3D e aparelhos sexuais conectados à Internet estão surgindo – o termo "Internet das Coisas" – *Internet of Things* (IoT), em inglês – refere-se a variados tipos de objetos conectados à Internet, que mandam e recebem dados. Seria possível, inclusive, falar em uma "Internet das Coisas do Sexo" uma vez que dispositivos como "brinquedos" sexuais se popularizam. A expectativa é de que surjam não apenas novos tipos de experiências, mas também novos modelos de negócio (TAVES, 2016).

Um dos aspectos mais sensíveis e urgentes relacionados ao desenvolvimento deste "nicho" específico de IoT é – novamente - a privacidade e a proteção de dados pessoais. Exemplo disso é a o acordo firmado em março de 2017 nos Estados Unidos, no qual a empresa We-Vibe concordou em pagar quase USD 4 milhões no âmbito de uma ação coletiva (BOYSEN, 2017). A disputa referiu-se a questões de privacidade e dos dados pessoais dos usuários do produto oferecido pela We-Vibe: um brinquedo sexual que além de estar conectado à Internet também pode ser controlado por meio de um aplicativo instalado no celular dos usuários. Alegou-se que os dados relativos ao uso do aparelho estavam sendo utilizados pela empresa sem a devida anuência do usuário. Além disso, aqueles que fizeram uso do aplicativo no celular, estiveram ainda mais expostos por terem concedido dados adicionais (HAUTALA, 2016). Como podemos notar, são muitos os desafios relativos à proteção da privacidade e dos dados pessoais.

BREVES APONTAMENTOS

A indústria do sexo passa por mudanças sem precedentes. A Internet alterou de forma substancial a maneira pela qual a pornografia é produzida, distribuída e consumida. A convergência de plataformas possibilita que conteúdos sejam acessados de diferentes formas. Ademais, a existência de objetos conectados à Internet também faz parte das inovações que tal indústria promove. Tendências tais como a da interatividade são a nova fronteira a ser explorada, uma vez que se espera que a "Internet das Coisas", a "realidade virtual" e a "realidade aumentada" possibilitarão experiências diferentes do que existia há pouco.

Muito embora este tema desperte a curiosidade de muitos, há pouca discussão no que se refere a seus aspectos jurídicos, regulatórios e políticos. A falta de debate acerca de tais aspectos faz com que usuários estejam expostos a diferentes práticas e/ou omissões. Não obstante, de acordo com o que foi demonstrado neste artigo, várias áreas do Direito estão relacionadas com o desenvolvimento da indústria do sexo.

O presente artigo focou principalmente em questões ligadas à privacidade e aos dados pessoais dos usuários de serviços e produtos de tais industrias. Um exemplo claro de que há pouca proteção de tais dados é a incipiente conscientização por parte dos grandes portais de conteúdo pornográfico de que o protocolo HTTPS deve ser utilizado. Além disso, práticas da indústria em questão incluem até mesmo a venda de dados dos usuários, tais como os tipos de categorias e os termos buscados, ou a guarda de dados sem prévio consentimento, conforme exemplos mencionados acima.

Embora existam potenciais aspectos a serem aprimorados, alguns argumentam que se trata de uma indústria cujo desenvolvimento gera inovações, beneficiando diferentes setores. Assim, tabus de quaisquer natureza não podem impedir esforços no sentido de melhorar o ambiente para a referida indústria, de propiciar um melhor arcabouço jurídico e regulatório, e de proteger diretamente e indiretamente o ecossistema da Internet e da chamada "Internet das Coisas".

Por último, considerando que a produção e a distribuição de conteúdos pornográficos está cada vez mais concentrada em poucas empresas, é possível esperar variadas implicações decorrentes de tal concentração. Podemos prever, por exemplo, grandes mudanças socioculturais e comportamentais, estas sim demasiadamente complexas para serem abordadas em apenas um artigo.

REFERÊNCIAS

ALEXA. Top Sites in Brazil. Disponível em: <http://www.alexa.com/topsites/countries/BR>. Acesso em: 17 dez. 2018.

ALTAWEEL, Ibrahim; HILS, Maximillian; HOOFNAGLE, Chris Jay. Privacy on Adult Websites. Social Science Research Network. Disponível em: <https://papers.ssrn.com/abstract=2851997>. Acesso em: 07 jul. 2017.

ARSE ELETRONIKA. Arse Elektronika San Francisco 2015 Disponível em: <http://www.monochrom.at/arse-elektronika/talkabstracts.html>. Acesso em: 17 dez. 2018.

AUERBACH, David; WEISSMANN, Jordan. Vampire Porn. Slate, 23 out. 2014. Disponível em: <http://www.slate.com/articles/technology/technology/2014/10/mindgeek_porn_monopoly_its_dominance_is_a_cautionary_tale_for_other_industries.html>. Acesso em: 07 jul. 2017.

BOYSEN, Ryan. 2017. Sex Toy Maker Settles Vibrator Privacy Suit For $3.75M". Law360. Disponível em: <https://www.law360.com/articles/900548/sex-toy-maker-settles-vibrator-privacy-suit-for-3-75m>. Acesso em: 07 jul. 2017.

BULTMAN, M. 2016. Sex Toy Rivals Settle Long-Running Patent Dispute. Law360. Disponível em: <https://www.law360.com/articles/755834/sex-toy-rivals-settle--long-running-patent-dispute>. Acesso em: 07 jul. 2017.

CDT. 2017. It's Time to Move to HTTPS. Center for Democracy & Technology. Disponível em: <https://cdt.org/blog/its-time-to-move-to-https/>. 07 jul. 2017.

DARLING, Kate. 2014. IP Without IP? A Study of the Online Adult Entertainment Industry. Stanford Technology Law Review. Disponível em: <https://journals.law.stanford.edu/stanford-technology-law-review/online/ip-without-ip-study--online-adult-entertainment-industry>. Acesso em: 07 jul. 2017.

EDELMAN, Benjamin. 2009. Red Light States: Who Buys Online Adult Entertainment? *Journal of Economic Perspectives,* v. 23, n. 1, p. 209-220, [s.d.]

FLAHERTY, Scott. 2017. Adult Website Operator Manwin Settles. XXX Antitrust Row - Law360. Law360. Disponível em: <https://www.law360.com/articles/438074/adult-website-operator-manwin-settles-xxx-antitrust-row>. Acesso em: 07 jul. 2017.

FRAJHOF, Isabella. 2011. Liberdade de expressão e a pornografia na Suprema Corte Americana. Disponível em: <http://www.pucrio.br/pibic/relatorio_resumo2011/Relatorios/CSS/DIR/DIR_Isabella%20Z.%20Frajhof.pdf.> Acesso em: 07 jul. 2017.

FUNG, B. 2017a. The House just voted to wipe away the FCC's landmark Internet privacy protections. Washington Post. Disponível em: <https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/>. Acesso em: 07 jul. 2017.

FUNG, B. 2017b. Porn websites beef up privacy protections days after Congress voted to let ISPs share your Web history. Washington Post, 30 mar. 2017. Disponível em: <https://www.washingtonpost.com/news/the-switch/wp/2017/03/30/porn-websites-beef-up-privacy-protections-days-after-congress-voted-to-let-isps--share-your-web-history/>. Acesso em: 07 jul. 2017.

GILLULA, Jeremy. 2017. Five Creepy Things Your ISP Could Do If Congress Repeals the FCC's Privacy Protections. Electronic Frontier Foundation, 19 mar. 2017. Disponível em: <https://www.eff.org/deeplinks/2017/03/five-creepy-things-your-isp-could-do-if-congress-repeals-fccs-privacy-protections>. Acesso em: 07 jul. 2017.

HALL, Joseph Lorenzo. 2016. Issue Brief: The Time Has Come to Move to HTTPS! Center for Democracy and Technology (CDT). Disponível em: <https://cdt.org/files/2016/10/Issue-Brief-The-Time-Has-Come-to-Move-to-HTTPS.pdf>. Acesso em: 07 jul. 2017.

HALL, Joseph; NORCIE, Greg. 2016. It's Time to Move to HTTPS Center for Democracy and Technology, 7 out. 2016. Disponível em: <https://cdt.org/blog/its-time-to-move-to-https/>. Acesso em: 07 jul. 2017.

HAUTALA, Laura. Vulnerable Vibrator: Security Researchers find Flaw in Connected Toy. CNET, 10 ago. 2016. Disponível em: <https://www.cnet.com/news/vulnerable-vibrator-security-researchers-find-flaws-in-connected-toy/>. Acesso em: 07 jul. 2017.

ICANN History Project. Manwin Licensing International v. ICM Registry, *et al*. Disponível em: <https://www.icann.org/resources/pages/manwin-v-icm-2012-02-25-en>. Acesso em: 17 dez. 2018.

ICANN History Project. Manwin Licensing International v. ICM Registry, *et al*. Disponível em: <https://www.icann.org/en/system/files/files/complaint-16no-v11-en.pdf>. Acesso em: 17 dez. 2018.

JOHNSON, Peter. Pornography Drives Technology: Why Not to Censor the Internet. *49 Federal Communications Law Journal 217,* v. 49 n. 1, 1996. Disponível em: <http://www.repository.law.indiana.edu/fclj/vol49/iss1/8>. Acesso em: 07 jul. 2017.

MAROTTA-WURGLER, Florencia. 2016. Understanding Privacy Policies: Content, Self-Regulation, and Markets. SSRN Scholarly Paper ID 2736513. Rochester, NY: Social Science Research Network. Disponível em: <https://papers.ssrn.com/abstract=2736513>. Acesso em: 17 dez. 2018.

MILLWARD, Jon. Deep Inside: A Study of 10,000 Porn Stars. *Jon Millward, Data Journalist: Exploring the Curious Corners of Society and Psychology*, 14 fev. 2013. Disponível em: <http://jonmillward.com/blog/studies/deep-inside-a-study-of--10000-porn-stars/>. Acesso em: 17 dez. 2018.

PORN HUB INSIGHTS. Redtube & Brazil. Disponível em: <https://www.pornhub.com/insights/redtube-brazil>. Acesso em: 17 dez. 2018.

PORN HUB INSIGHTS. Pornhub's 2016 Year in Review. Disponível em:<https://www.pornhub.com/insights/2016-year-in-review>. Acesso em: 17 dez. 2018.

PORNHUB INSIGHTS 2017. Pornhub's 2016 Year in Review. 4 jan. 2017. Disponível em: <https://www.pornhub.com/insights/2016-year-in-review>. Acesso em: 07 jul. 2017.

PORNHUB INSIGHTS. Redtube & Brazil. 5 fev. 2016. Disponível em: <https://www.pornhub.com/insights/redtube-brazil>. Acesso em: 07 jul. 2017.

RANKS, Alexa Traffic. How popular is pornhub.com? Disponível em: <http://www.alexa.com/siteinfo/pornhub.com>. Acesso em: 17 dez. 2018.

ROLLING STONE. Pornhub Launches Record Label. Disponível em: <http://www.rollingstone.com/music/news/pornhub-launches-record-label-20140925>. Acesso em: 07 jul. 2017.

RUANE, Kathleen Ann. Freedom of Speech and Press: Exceptions to the First Amendment. Congressional Research Service. Disponível em: <https://fas.org/sgp/crs/misc/95-815.pdf>. Acesso em: 07 jul. 2017.

SIMPSON, Thomas. Mythbusters: Revenge of the Cable Myths, Part III. TeleGeography, 14 jul. 2016.

SULLIVAN, Rebecca; MCKEE, Alan. 2015. *Pornography*: Structures, Agency and Performance. Polity. [S.l: s.n.: s.d.]

TARRANT, Shira. 2016. *The Pornography Industry*: What Everyone Needs to Know. Oxford: Oxford University Press, [s.d.].

TAVES, Max. 2016. Can virtual reality get you to pay for porn again? CNET. Disponível em: <https://www.cnet.com/news/can-virtual-reality-get-you-to-pay-for-porn-again/>. Acesso em: 07 jul. 2017.

THANK YOU VERY MUCH FOR MAKING HISTORY WITH US! STAY TUNED FOR UPCOMING DATES. #CAMCON2018. Disponível em: <http://www.camming-con.com/>. Acesso em: 17 dez. 2018.

THE ECONOMIST. 2015. Naked Capitalism. **The Economist**, 26 set. 2015. Disponível em: <http://www.economist.com/news/international/21666114-internet-blew-porn-industrys-business-model-apart-its-response-holds-lessons>. Acesso em: 07 jul. 2017.

THOMSEN, Michael. MindGeek Is Both Plaintiff And Defendant In Two New DMCA Lawsuits. Forbes, 30 nov. 2015. Disponível em: <http://www.forbes.com/sites/michaelthomsen/2015/11/30/mindgeek-is-both-plaintiff-and-defendant-in-two--new-dmca-lawsuits/>. Acesso em: 07 jul. 2017.

VAAS, Lisa. 2017. Age verification legislation will lead to porn habit database. Security Boulevard. Disponível em: <https://securityboulevard.com/2017/11/age-verification-legislation-will-lead-to-porn-habit-database/>. Acesso em: 07 jul. 2017.

VALENTE, Mariana Giorgetti; NERIS, Natalia; RUIZ, Juliana; Bulgarelli, Lucas. O corpo é o código: estratégias jurídicas de enfrentamento ao Revenge Porn no Brasil. Internet Lab, 2016. Disponível em: <https://www.academia.edu/27140410/O_CORPO_%C3%89_O_C%C3%93DIGO_ESTRAT%C3%89GIAS_JUR%C3%8DDICAS_DE_ENFRENTAMENTO_AO_REVENGE_PORN_NO_BRASIL>. Acesso em: 07 jul. 2017.

WONDRACEK, Gilbert; HOLZ, Thorsten; PLATZER, Christian; ENGIN, Kirda; KRUEGEL, Christopher. 2010. Is the Internet for Porn? An Insight Into the Online Adult Industry. Harvard University. Disponível em: <http://www.econinfosec.org/archive/weis2010/papers/session2/weis2010_wondracek.pdf>. Acesso em: 07 jul. 2017.

WOSICK, Kassia R. 2015. Pornography. In: Handbook of the Sociology of Sexualities. Editado por John DeLamater and Rebecca F. Plante. *Handbooks of Sociology and Social Research*. [S.l.]: Springer International Publishing, [s.d.]. p. 413-433.

III

TUTELA DAS COMUNICAÇÕES E SEGURANÇA NA ERA DIGITAL

PRIVACIDADE, VIGILÂNCIA E INTELIGÊNCIA NO BRASIL: O MARCO LEGAL E SUAS LACUNAS[1]

PEDRO AUGUSTO P. FRANCISCO
JAMILA VENTURINI

INTRODUÇÃO

A Internet comercial no Brasil teve seu início em 1994. Desde então, ela foi elemento central de uma série de mudanças tecnológicas cuja base pode ser resumida no aumento da capacidade de digitalização e processamento de dados, com cada vez mais velocidade. Essas mudanças trouxeram para a ordem do dia discussões sobre o direito à privacidade, na sua dimensão individual e subjetiva. Uma liberdade negativa, na medida em que enseja uma obrigação de não-fazer. Ninguém pode ter sua privacidade violada sem um motivo legítimo e legal.

Com o intuito de controlar as atividades de vigilância por parte do Estado – cada vez mais baseadas em avançadas tecnologias digitais de coleta e processamento de dados – houve o crescimento de uma demanda por transparência e por mecanismos que permitam à sociedade saber que tipo de informação esse Estado tem sobre a população.

Por sua vez, as motivações do Estado para obter informações sobre indivíduos são diversas e não são novas. Desde o século XVIII, quando a própria ideia de "população" entra no vocabulário e na racionalização do Estado, arte de governar passou a ser dependente da capacidade do agente governante de obter dados sobre aquilo que será governado (FOUCAULT, 2004). Tampouco são novos os abusos decorrentes das atividades de vigilância. O que as tecnologias digitais trazem são novas modalidades de obtenção

1 Parte desse texto se baseia no relatório da pesquisa *Privacy and surveillance in the digital age: a comparative study of the Brazilian and German legal frameworks*, elaborado por Anja Dahlmann, Jamila Venturini, Marcel Dickow e Marilia Ferreira Maciel. O relatório foi publicado em 2015 e contou com a revisão técnica de Bruno Bioni e Geraldo Prado.

de informações e escala, de um modo nunca antes visto. Essa escala inclui um importante aspecto: o surgimento de uma indústria privada de vigilância baseada não só em agentes tradicionais do setor – tais como a Logos Technologies,[2] a Hacking Team[3] e Harris Corp.,[4] para citar apenas alguns que atuaram junto ao governo brasileiro em diferentes circunstâncias[5] –, mas também em atores que não eram tradicionalmente percebidos como instrumentos de vigilância e que passaram a ser agentes centrais nesse ecossistema, como Microsoft, Google, Facebook e Yahoo,[6] de modo que já não é possível se discutir vigilância e privacidade sem levá-los em consideração.

Se talvez o papel do setor privado e, particularmente, das empresas de Tecnologias da Informação e Comunicação (TIC) não estivesse tradicionalmente no foco das discussões sobre vigilância e privacidade, é preciso evidenciar que hoje essa é uma preocupação transversal para setores que vão do governo à sociedade civil. As denúncias sobre as atividades de vigilância em massa realizadas pelos Estados Unidos e parceiros organizados no grupo conhecido como "Five Eyes" certamente tiveram um papel central em chamar a atenção para essa questão.[7] O escândalo parece ter materializado preocupações pré-existentes com o aumento da capacidade de vigilância do Estado por meio das tecnologias digitais e, com isso, gerado uma grande discussão sobre a ameaça que a coleta e o processamento massivo de dados podem representar aos direitos fundamentais.

---

2 LOGO TECHNOLOGIES. About us. Disponível em: <https://www.logostech.net/about-us/>. Acesso em: 29 ago. 2017.

3 HACKING TEAM. About us. Disponível em: <http://www.hackingteam.it/about.html>. Acesso em: 29 ago. 2017.

4 HARRIS. About Harris. Disponível em: <https://www.harris.com/about>. Acesso em: 29 ago. 2017.

5 THE WEEK. Disponível em: <http://theweek.com/articles/640048/going-olympics-brazil-watching>; <http://www.cartacapital.com.br/sociedade/olimpiadas-no-brasil-201cpremiam201d-a-industria-da-vigilancia>. Acesso em: 7 jul. 2016, e VICENTE, João Paulo. Como as Olimpíadas ajudaram o Brasil a aumentar seu aparato de vigilância social. MOTHERBOARD, 7 jul. 2016. <https://motherboard.vice.com/pt_br/article/como-o-brasil-aprimorou-seu-aparato-de-vigilancia-social-para-as-olimpiadas>. Acesso em: 29 ago. 2017.

6 THE GUARDIAN. Microsoft, Facebook, Google and Yahoo release US surveillance requests. Disponível em: <https://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests>. Acesso em: 29 ago. 2017.

7 Para mais informações sobre o "Five Eyes" ver: PRIVACY INTERNATIONAL. Privacy International Launches International Campaign For Greater Transparency Around Secretive Intelligence Sharing Activities Between Governments. 23 out. 2017. Disponível em: <https://www.privacyinternational.org/node/51>. Acesso em: 29 ago. 2017.

As denúncias despertaram reações em diversos setores e, ao menos num primeiro momento, motivaram reformas e iniciativas nacionais e internacionais que buscavam garantir níveis maiores de proteção à privacidade na era digital. O governo brasileiro foi um dos principais protagonistas desse debate. No âmbito internacional, liderou as discussões sobre a necessidade de um marco legal para a governança e o uso da Internet e de princípios básicos de proteção dos direitos humanos. Junto ao governo alemão propôs uma resolução sobre privacidade na era digital, que foi finalmente adotada pela Assembleia Geral das Nações Unidas (ONU), convocando os Estados-membros a revisar seus procedimentos, práticas e normas relacionadas à vigilância de comunicações.[8]

Já no âmbito nacional, além da realização de uma "CPI da Espionagem", a aprovação do Marco Civil da Internet – que já vinha sendo discutido no Congresso – e a realização do encontro NETmundial em parceria com a Internet Corporation for Assigned Names and Numbers (ICANN), marcaram a resposta brasileira aos escândalos de vigilância massiva. Do mesmo modo, o Decreto 8.135, aprovado em novembro de 2013, pretendia garantir a segurança das comunicações da administração pública federal.

Frente a esse cenário, o objetivo desse trabalho é apontar, ainda que brevemente, os desafios que enfrentam os formuladores de políticas públicas no campo da privacidade e da vigilância, levando em consideração a mudança nas tecnologias digitais. Partimos da compreensão de que a segurança nacional e o combate à criminalidade podem legitimamente justificar a vigilância das comunicações em situações excepcionais – afinal, nenhum direito é absoluto – mas que são necessárias regras claras que garantam a obediência a princípios de direitos humanos como a necessidade, proporcionalidade, o devido processo legal e a transparência.

Na primeira parte deste artigo, fazemos uma breve exposição de algumas normas existentes no Brasil sobre privacidade, confidencialidade das comunicações e atividades de inteligência, numa tentativa de identificar como o país vem lidando com o desafio de equilibrar segurança pública e nacional com a proteção de direitos individuais. Essa exposição vai mostrar que o cenário não é de um total vazio regulatório. A proteção constitucional à privacidade é forte, assim como a Lei de Interceptação Telefônica (Lei 9296/1996) e o mais recente Marco Civil da Internet (Lei 12965/2014), entre outras normas, incluem regras e garantias relacionadas ao tema.

8 ESUBSCRIPTION TO UNITED NATIONS DOCUMENTS. Resolution adopted by the General Assembly on 18 December 2013. Disponível em: <http://undocs.org/A/RES/68/167>. Acesso em: 29 ago. 2017.

Contudo, tal como demonstraremos na segunda parte, isso não significa que haja clareza quanto aos procedimentos que devem ser observados nas atividades de vigilância das comunicações e de inteligência. A própria lei de interceptações pode ser considerada satisfatória do ponto de vista da proteção dos direitos humanos, porém carece de especificação de procedimentos para a interceptação e não foi suficiente para conter abusos. Particularmente, quando se trata de novas tecnologias, a ausência de regras e garantias específicas é preocupante dado (i) o histórico de uso extensivo da vigilância de comunicações pelas forças policiais e de inteligência no Brasil e (ii) a capacidade de intrusão na vida privada dessas tecnologias e o potencial que o tratamento massivo de dados (para além do conteúdo das comunicações) possui em termos de identificação de hábitos pessoais. Com relação às atividades de inteligência, o marco legal é tão escasso que sequer existe menção na Constituição. A lacuna nas definições e limites sobre como deve operar a inteligência de Estado no Brasil faz com que o cenário seja, ao mesmo tempo, aberto à abusos por parte do poder público e carente de ações que permitam que ela se desenvolva com eficiência.

O MARCO LEGAL BRASILEIRO PARA PRIVACIDADE, VIGILÂNCIA DAS COMUNICAÇÕES E INTELIGÊNCIA

Desenvolvimentos recentes no marco legal brasileiro oferecem uma abordagem inicial para uma estrutura regulatória que concilia a necessidade de promover um maior acesso à informação e, ao mesmo tempo, proteger a privacidade os cidadãos. Exemplos disso são o Marco Civil da Internet e a Lei de Acesso à Informação. Uma análise mais detalhada das normas existentes, porém, parece evidenciar que ainda falta um marco legal abrangente que dê conta dos novos desafios à privacidade na era digital.

No Brasil, o princípio da presunção de inocência, o direito à privacidade, a inviolabilidade do domicílio e a confidencialidade das comunicações gozam de proteção constitucional. A Constituição assegura ainda o direito à liberdade de expressão, acesso à informação e ao *habeas data* – regulado pela Lei 9.507/1997 –, ou seja, o direito de acesso a dados pessoais detidos pelo Estado por parte do titular e de retificá-los. O país também assinou e ratificou diversos tratados de direitos humanos que garantem o direito à privacidade, incluindo a Declaração Universal dos Direitos Humanos (DUDH), o Pacto Internacional dos Direitos Civis e Políticos, e a Convenção Americana de Direitos Humanos.[9]

9 Segundo o artigo 5, parágrafo 3º da Constituição (incluído pela emenda 45/2004), tratados e convenções internacionais sobre direitos humanos internalizados por meio da aprovação nas duas casas do Congresso Nacional em dois turnos e por três quintos dos votos de seus membros são equivalentes a emendas constitucionais.

EXCEÇÕES À CONFIDENCIALIDADE DAS COMUNICAÇÕES

A Constituição estabelece que é inviolável o sigilo das comunicações exceto por ordem judicial para fins de investigação criminal ou instrução processual penal. O mesmo artigo também prevê que as hipóteses e a forma de derrogação do sigilo serão estabelecidas em lei. No caso, foi a Lei Nº 9.296/1996, que definiu os critérios para a interceptação das comunicações telefônicas.

Segundo ela, a interceptação telefônica ou telemática pode ser requerida apenas por autoridade policial ou por representante do Ministério Público, na investigação criminal e na instrução processual penal. A autoridade requerente deve (i) apresentar indícios razoáveis de que o sujeito praticou delito punível com reclusão nos termos do Código Penal brasileiro e (ii) demonstrar que a prova não pode ser obtida por outros meios. O procedimento está sujeito ao controle judicial e a interceptação pode ser autorizada por um período máximo de 15 dias, que pode ser estendido por mais 15 dias caso se demonstre que isso é essencial para a obtenção de provas para a investigação. O Ministério Público deve sempre ser notificado pela polícia quando da execução de qualquer interceptação autorizada.

A Corte Interamericana de Direitos Humanos (CIDH) reconheceu que

> [...] considerando que [a interceptação telefônica] pode representar uma séria interferência na vida privada, tal medida deve estar fundamentada em lei, que deve ser precisa e indicar regras claras e detalhadas sobre a matéria, tais como as circunstâncias nas quais essa medida pode ser adotada; as pessoas autorizadas a solicitá-la, ordená-la e executá-la; o procedimento a seguir, entre outros elementos. (ESCHER, 2009, *on-line*).

A Corte afirmou ainda que "para que esteja conforme com a Convenção Americana uma ingerência deve cumprir com os seguintes requisitos: a) estar prevista em lei, b) perseguir um fim legítimo e c) ser idônea, necessária e proporcional".[10] Nesse sentido, as condições definidas na Lei 9.296/1996, estão, em grande medida, de acordo com as recomendações da CIDH.

O Judiciário brasileiro, porém, parece ter adotado uma interpretação um tanto ampla das limitações à interceptação telefônica. Com relação à duração da interceptação, em ao menos duas ocasiões diferentes, o STF

10 Segundo o artigo 5, parágrafo 3º da Constituição (incluído pela emenda 45/2004), tratados e convenções internacionais sobre direitos humanos internalizados por meio da aprovação nas duas casas do Congresso Nacional em dois turnos e por três quintos dos votos de seus membros são equivalentes a emendas constitucionais.

decidiu que ela pode ser estendida múltiplas vezes.[11] Em um dos casos, a decisão prorrogando a interceptação foi renovada por um período de 7 meses.[12] [13] Uma das possíveis justificativas para esse tipo de interpretação seria uma excessiva rigidez e consequente inaplicabilidade da Lei 9.296/1996. Essa posição foi defendida pelo Ministro Sepúlveda Pertence do Supremo Tribunal Federal em audiência pública durante a CPI dos Grampos Telefônicos.[14]

Cabe relembrar que, até a aprovação da Lei No 9.296/1996, o STF havia adotado uma interpretação conservadora do dispositivo constitucional relativo à confidencialidade das comunicações em favor da proteção da privacidade. Em uma decisão de 1993, o Tribunal invalidou uma pena de prisão após considerar que ela havia decorrido de uma escuta ilegal.[15] De acordo com a decisão, independentemente de ordem judicial, a interceptação das comunicações telefônicas não seria válida até que procedimentos específicos fossem definidos por lei. Portanto, qualquer prova obtida direta ou indiretamente por meio de escuta ilegal também seria considerada invá-

11 HC 83515/RS, rel. Min. Nelson Jobim, 16.9.2004 e Inq 2424/RJ, rel. Min. Cezar Peluso, 19 e 20.11.2008.

12 HC 83515/RS, rel. Min. Nelson Jobim, 16.9.2004.

13 Para assinalar a natureza desproporcional da decisão tomada em um estágio anterior desse julgamento, Prado (2006) comparou as disposições da Constituição Federal acerca da duração permitida para fins de investigação criminal com a duração para situações de estado de emergência previstas na Constituição (estado de defesa e estado de sítio). Nos termos da Constituição, o estado de defesa pode ser declarado quando há uma ameaça à ordem pública ou à paz social e pode durar até 60 dias, ao longo dos quais a confidencialidade das comunicações será restringida. O estado de sítio, por sua vez, pode ser declarado por 30 dias caso o estado de defesa não seja efetivo ou caso ocorra guerra ou ataque internacional. Prado argumenta que se a Constituição limita restrições aos direitos fundamentais em caso de crises nacionais graves, seria desproporcional permitir escutas ilimitadas em processos criminais, uma possibilidade que as decisões do STF supracitadas parecem ter deixado em aberto.

14 Na página 107, o relatório afirma "No tocante ao prazo, o ministro afirmou que o prazo de 15 dias é muito curto, e decorrem daí as razões da jurisprudência ter flexibilizado esse prazo. Mais do que as prorrogações, o que assusta o ministro é a facilidade da autorização". CÂMARA DOS DEPUTADOS. RELATÓRIO. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/53a-legislatura-encerradas/cpiescut/relatorio-final-aprovado/Relatorio-Final-Versao-Final.pdf>. Acesso em: 07 mar. 2018.

15 HC 69.912-0/RS, rel. Min. Sepúlveda Pertence, 30.06.1993.

lida. Em 1996,[16] o STF confirmou a posição de que todas as interceptações telefônicas seriam consideradas ilegais até que a exceção constitucional à confidencialidade das comunicações fosse regulamentada. A decisão mencionava a existência de leis detalhadas em países da América do Norte e da Europa e aumentou a pressão pela aprovação da Lei Nº 9.296.

OUTRAS NORMAS E LIMITES DA LEI 9.296/1996

Alguns atos administrativos da Agência Nacional de Telecomunicações (Anatel), que regula o fornecimento de serviços de telefonia fixa, móvel e de comunicação de dados,[17] buscaram garantir a confidencialidade das comunicações e detalhar procedimentos para a interceptação telefônica. Pode-se mencionar a Resolução Nº 73/98, a Resolução Nº 426/2005, a Resolução Nº 477/2007 e a Resolução Nº 614/2013, que determina que as prestadoras devem divulgar dados relativos à suspensão do sigilo das telecomunicações para as autoridades competentes e estabelece que os registros de conexão devem ser mantidos pelo prazo mínimo de um ano.

Cabe observar que esses atos administrativos de alguma maneira buscam detalhar os procedimentos para execução das escutas telefônicas, uma vez que a lei correspondente não o faz. As investigações sobre vazamentos realizadas nos últimos anos parecem indicar que esse pode ser um dos pontos mais frágeis do marco regulatório atual, que não permite controlar a implementação técnica das decisões de interceptação.

Nos termos da Lei 9.296/1996, o ato de (i) interceptar comunicações telefônicas e sistemas de informática ou (ii) violar a confidencialidade assegurada por lei sem autorização judicial ou com objetivos não autorizados em lei é considerado um crime punível com detenção de 2 a 4 anos e multa.

METADADOS E RETENÇÃO OBRIGATÓRIA DE DADOS

No que diz respeito às comunicações que ocorrem por meio da Internet, a Lei 9.296/1996 prevê sua aplicação às chamadas comunicações telemáticas. A Lei 12.965/2014 (Marco Civil da Internet) vai além ao determinar regras relativas aos chamados metadados. De acordo com o Artigo 29 do Working Party:

---

16 HC 73.351-4/SP, rel. Min. Ilmar Galvão, 09.05.1996.

17 A Anatel foi criada pela Lei Geral de Telecomunicações (Lei No 9.472/1997), que define ainda que os usuários dos serviços de telecomunicação têm direito à privacidade dos documentos de cobrança e na utilização de seus dados pessoais pela prestadora.

> Metadados são todos os tipos de informação sobre a ocorrência de uma comunicação, exceto pelo conteúdo da conversa. Eles podem incluir o número de telefone e o endereço de IP da pessoa que realizar a chamada ou enviar o e-mail, o tempo e a localização da informação, o tema, o destinatário, etc. Uma análise pode revelar informações sensíveis sobre pessoas caso, por exemplo, sejam discados números de centros médicos ou religiosos.[18]

A condição jurídica desses dados é um tanto confusa no ordenamento jurídico brasileiro. A redação do dispositivo constitucional relativo ao direito à inviolabilidade das correspondências, das comunicações telegráficas, dos dados, e das comunicações telefônicas (Art. 5º, XII) permitiu a interpretação de que o sigilo se aplica apenas ao tráfego de dados (NUCCI, 2006).

Enquanto alguns juristas entendem que a redação é clara em garantir a inviolabilidade (i) da correspondência e das comunicações telegráficas (ii) de dados e das comunicações telefônicas, salvo, no último caso (ii) mediante ordem judicial para fins de investigação criminal ou instrução processual penal, outros interpretam o termo "comunicações" de forma estrita (FERRAZ JÚNIOR, 1993). Segundo tal interpretação, o sigilo se restringiria à transmissão de informações, sejam elas feitas por meio de correspondência, telégrafo, dados ou telefone. No caso de dados, isso significaria que o sigilo apenas seria protegido no momento da transmissão e não quando eles estivessem armazenados. Se na primeira interpretação a confidencialidade de comunicações telefônicas e de dados – transmitidos ou armazenados – só poderia ser suspensa "para fins de investigação criminal ou instrução processual penal", na segunda o nível de proteção aos dados armazenados seria inferior.

A última interpretação tem prevalecido na jurisprudência do STF, com ao menos duas decisões sustentando que a cláusula se refere à comunicação de dados para justificar a legalidade da apreensão de equipamentos contendo dados privados após concessão de autorização judicial para tal fim.[19] Com o avanço da Internet e das comunicações digitais, que se baseiam em um ecossistema global de armazenamento e processamento de dados, tal interpretação permite supor que o acesso a metadados ou outros tipos de dados – inclusive de geolocalização – armazenados em servidores dentro ou fora do país não estaria condicionado às mesmas regras impostas para o acesso ao conteúdo das comunicações.

---

18 Artigo 29 Data Protection Working Party. Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes. 2014. JUSTICE AND CONSUMERS. Article 29 Working Party. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf>. Acesso em: 07 mar. 2018.

19 MS 21.729, rel. Min. Marco Aurélio, 5.10.1995 e RE 418.416-8 SC, rel. Min. Sepúlveda Pertence, 10.05.2006.

Ainda assim, tais dados e metadados, segundo as definições existentes, poderiam ser considerados dados pessoais, ou seja, relativos a pessoas naturais identificadas ou identificáveis. No Brasil, a proteção a dados pessoais é derivada da garantia constitucional da igualdade, liberdade e dignidade humana, assim como da intimidade e da vida privada. Porém, é possível dizer que até a promulgação do Marco Civil da Internet em 2014, não se tratava de um direito explicitamente reconhecido no ordenamento jurídico brasileiro.

PROTEÇÃO DE DADOS PESSOAIS

Até 2018, o Brasil não contava com uma lei geral de proteção de dados. A tutela do tema no país ocorria por meio de normas como o Código de Defesa do Consumidor (Lei No 8.078/1990), a Lei 9.507/1997 sobre o *habeas data*, a Lei de Acesso à Informação (Lei No 12.527/2011), a Lei No 12.414/2011 sobre bancos de dados com informações de adimplemento e o já mencionado Marco Civil da Internet (Nº 12.965/2014).[20] Essas normas incorporaram, ainda que de modo setorial, uma série de princípios e direitos fundamentais para a proteção de dados no marco legal brasileiro, como o direito de acesso, retificação das informações coletadas, à notificação em caso de coleta sem consentimento, a limitação temporal de retenção de dados, entre outros.

Principalmente por conta da aplicação do Código de Defesa do Consumidor, o Supremo Tribunal de Justiça (STJ) chegou a expressar preocupações sobre a dimensão da coleta e do processamento de dados pessoais desde a década de 1990. Como exemplo, a sentença proferida pelo Ministro Ruy Rosado de Aguiar, no âmbito do Recurso Especial 22.337/RS, de 1995, reconheceu que o controle unificado das atividades do indivíduo permite um conhecimento abrangente e detalhado sobre sua vida pública e privada, o que constitui uma violação da privacidade. Reconhecia que ainda que isso pode ser utilizado para fins lícitos – como a prevenção ou repressão de crimes – mas que permite também a opressão política ou econômica, "contradizendo o direito e a moral".

Mais recentemente, a Lei No 12.527/2011, ao regulamentar o direito de acesso a informações garantido pela Constituição, foi a primeira em definir um conceito de "informações pessoais". A lei delimita ainda as situações

20 Com o surgimento de novos desafios à proteção de dados, os legisladores tanto da Câmara dos Deputados quanto do Senado desenvolveram projetos de lei relativos ao tema. O Ministério da Justiça também conduziu uma consulta pública entre janeiro e julho de 2015 sobre a minuta de um projeto de lei apresentado ao Congresso em maio de 2016. Foi somente em julho de 2018 que um desses projetos, o PLC 53/2018, foi aprovado no Congresso Nacional. No momento de fechamento deste artigo o projeto de lei aguardava a sanção presidencial.

em que informações pessoais detidas pelo Estado poderão ser acessadas por terceiros. Apesar de não incorporar regras para a coleta de informações por parte de agentes e órgãos públicos, a Lei de Acesso à Informação determina que o processamento de dados pessoais deve respeitar a intimidade, a vida privada, a honra e a imagem.

Finalmente, o Marco Civil da Internet surgiu como alternativa a propostas legislativas de criminalização de certas práticas na Internet[21] e tornou-se importante referência internacional, não apenas por abarcar garantias e disposições progressistas, tal como o princípio de neutralidade de rede, mas também por ter sido construída a partir de um amplo processo de consultas públicas até chegar no Congresso.[22] Apesar de não ter sido idealizada inicialmente para incluir disposições específicas sobre privacidade e proteção de dados, após o vazamento de informações sobre as atividades de vigilância global realizadas pela NSA e governos associados, esses eixos foram intensificados em resposta aos escândalos internacionais de vigilância em massa.[23]

---

21 Esse foi o caso do projeto de lei 84/99, conhecido como "Lei Azeredo", que previa, por exemplo, penas de até quatro anos de prisão por desbloqueio ou realização "jailbreak" em um telefone móvel, ou pela transferência de músicas de um tocador de MP3 para um computador.

22 A Secretaria de Assuntos Legislativos do Ministério da Justiça (MJ-SAL) e o Centro de Tecnologia e Sociedade da FGV Direito Rio (CTS-FGV) desenvolveram uma parceria para condução de uma consulta pública e criaram uma plataforma em um site de Cultura Digital para envio de comentários. O processo de consulta pública foi dividido em duas fases. Na primeira, que começou em outubro de 2009 e durou pouco mais de 45 dias, um texto contendo os princípios gerais para a regulação da internet foi posto em consulta. Os participantes podiam detalhar esses princípios e propor novos tópicos a serem incluídos na futura lei. Na segunda fase, uma minuta de projeto de lei, baseada nas sugestões recebidas, foi posta em consulta. Os comentários foram incorporados pela MJ-SAL e pelo CTS e a minuta do projeto de lei foi enviada ao Congresso. Durante o tempo em que o projeto de lei esteve no Congresso, sete audiências públicas foram realizadas com a participação de 62 membros da sociedade civil e 374 sugestões do público foram reunidas e levadas em consideração na elaboração do texto final na Câmara dos Deputados.

23 Na abertura da 68ª Sessão da Assembleia Geral das Nações Unidas, a presidente Dilma Rousseff definiu vigilância em massa como uma "violação ao direito internacional", "um desrespeito à soberania nacional" e uma "grave violação aos direitos humanos e às liberdades civis". A presidente também mencionou a necessidade de desenvolver uma estrutura para governança e uso da internet e de criar mecanismos para assegurar que princípios básicos sejam garantidos, tais como o princípio da privacidade, da liberdade de expressão e da neutralidade da rede. Posteriormente, a Alemanha e o Brasil propuseram conjuntamente uma resolução na Assembleia Geral das Nações Unidas sobre o direito à privacidade na era digital.

Assim, na forma como foi aprovada, a lei regulamenta aspectos importantes sobre a proteção de dados, buscando conceder aos usuários de internet um nível mais alto de proteção. Entre as garantias previstas no Marco Civil da Internet, estão que: (i) as informações pessoais dos usuários não devem ser transferidas para terceiros sem consentimento livre, expresso e informado; (ii) os usuários têm o direito de acessar informações claras e completas sobre a coleta, o uso, o armazenamento, o processamento e à proteção de seus dados pessoais, que podem apenas ser usados para finalidades que (a) justifiquem sua coleta, (b) não sejam vedadas pela legislação e (c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso; (iii) os usuários têm o direito ao consentimento sobre a coleta, o uso, o armazenamento e o processamento de dados pessoais e (iv) os usuários têm o direito de solicitar exclusão definitiva de seus dados pessoais após o término das relações entre as partes exceto nos casos previstos na lei.

O Marco Civil prevê ainda que qualquer cláusula contratual que viole a confidencialidade das comunicações privadas pela Internet deve ser considerada nula. Desse modo, o Marco Civil incorporou explicitamente dois princípios internacionalmente conhecidos de proteção de dados: a transparência e a finalidade[24], e consolidou direitos já previstos no Código de Defesa do Consumidor.

RETENÇÃO DE DADOS

Como ocorreu em diferentes países,[25] o Brasil introduziu gradualmente em seu ordenamento jurídico disposições que determinavam que empresas privadas armazenassem dados e metadados dos usuários por períodos pré-determinados para fins de investigações criminais. A medida evidencia o quanto os legisladores e outras autoridades administrativas compreenderam a importância dessas informações, cada vez mais abundantes e muitas vezes geradas de forma passiva – pelo mero uso de determinada tecnologia –, para identificar indivíduos.

24 Contribuição do governo brasileiro ao relatório do Alto Comissariado das Nações Unidas para os Direitos Humanos sobre o direito à privacidade na era digital (2014). UNITED NATIONS HUMAN RIGHTS. Contributions from stakeholders: Right to privacy in the digital age. Disponível em: <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/Contributions.aspx>. Acesso em: 7 mar. 2018.

25 A Europa, por exemplo, aprovou em 2006 uma Diretiva de Retenção de Dados (Diretiva 2006/24/EC) que foi implementada em países como a Romênia e a Alemanha (nos dois casos, as leis de retenção de dados foram declaradas inconstitucionais). A Diretiva foi finalmente anulada pelo Tribunal de Justiça da União Europeia em 2014.

Entre as normas que preveem este tipo de mecanismo estão a Lei Nº 12.850/2013 sobre o crime organizado, que prevê que as empresas telefônicas devem manter os dados sobre a origem e o destino das chamadas por um período de cinco anos e disponibilizá-los para autoridades policiais e o Ministério Público sem, no entanto, especificar se o acesso estaria sujeito à autorização judicial. A Lei 12.850/2013 sobre o crime organizado também determina que empresas de transporte devem disponibilizar acesso direto a bases de dados sobre reservas e registros de viagens para juízes, promotores de justiça e autoridades policiais.

O Marco Civil prevê um período de doze meses de retenção para registros de conexão e um período de seis meses de retenção registro de acesso a aplicações de internet. A lei define registros de conexão como o conjunto de informações referentes à data e hora de uma conexão à internet, sua duração e o endereço IP utilizado no acesso. Registros de acesso a aplicações de internet, por sua vez, são definidos como o conjunto de informações referentes à data e à hora de uso de uma aplicação de internet a partir de um determinado endereço IP. A Lei estipula que provedores de conexão são proibidos de armazenar registros de aplicações e que os provedores de aplicações não devem armazenar registros de acesso de outras aplicações, exceto mediante consentimento do usuário. Nos termos da lei, as provedoras são apenas obrigadas a fornecer acesso aos registros retidos mediante ordem judicial específica.

A única exceção prevista no Marco Civil é relacionada à disponibilização de informações sobre qualificação pessoal, afiliação e endereço a autoridades administrativas sem ordem judicial.

Dispositivo similar pode ser encontrado na Lei Nº 9.613/1998 sobre lavagem de dinheiro, que prevê que o Ministério Público e as autoridades policiais terão acesso aos dados sobre qualificação pessoal, afiliação e endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de Internet e administradoras de cartão de crédito, independentemente de autorização judicial e na Lei Nº 12.850/2013.[26]

26 A constitucionalidade das disposições da Lei nº 12.850/2013 relacionada ao (i) acesso a dados sem ordem judicial (art. 15), (ii) retenção por empresas telefônicas de dados relativos a origem e ao destino de chamadas telefônicas por cinco anos (art. 17, ver acima) e (iii) criminalização da recusa de oferecer dados solicitados a autoridades policiais e ao Ministério Público (art. 21) está sendo atualmente questionada no STF pela Associação Nacional das Operadoras Celulares (ACEL). Ver ADI 5063/DF, rel. Gilmar Mendes.

ATIVIDADES DE INTELIGÊNCIA

O sistema de inteligência brasileiro foi criado pela Lei Nº 9.883/1999 com o objetivo de preservar a soberania nacional, defender o Estado democrático e a dignidade humana.

Ainda que não haja uma definição internacionalmente unificada de inteligência, Sherman Kent identificou três de seus principais aspectos (KENT, 1966): inteligência enquanto conhecimento seria o produto da análise de informações que servem ao processo decisório; a) inteligência enquanto organização englobaria órgãos governamentais que contribuem para a inteligência; b) inteligência enquanto atividade seria o processo de obtenção, análise e disseminação de informações. O aspecto organizacional da inteligência é bem definido pelas leis nacionais. A Lei Nº 9.883/1999 criou a Agência Brasileira de Inteligência (ABIN), responsável pelo planejamento, execução, coordenação, supervisão e controle das atividades de inteligência no país. Uma comissão legislativa composta por 12 membros –sendo seis do Senado e seis da Câmara dos Deputados – é responsável pela supervisão das atividades da ABIN.

O Decreto 4.376/2002 detalhou ainda a organização e o funcionamento do sistema de inteligência brasileiro, sobretudo em relação a sua composição. Quatro alterações foram feitas para inclusão de novos membros no sistema que, atualmente, é composto de 19 membros. De acordo com o decreto, cada um dos membros deveria, entre outros: (i) planejar e executar ações relativas à obtenção e integração de dados e informações; (ii) intercambiar informações necessárias à produção de conhecimentos relacionados às atividades de inteligência e contra-inteligência; (iii) fornecer à ABIN informações relacionadas à defesa das instituições e dos interesses nacionais.

Ainda que a definição de inteligência seja parecida com a que já está prevista no artigo 1º da Lei No 9.883/1999, o decreto define contra-inteligência como atividades com a finalidade de neutralizar inteligência adversa ou qualquer ação que possa ameaçar a segurança de informações sensíveis à segurança nacional.

Alguns dos parâmetros relevantes para as atividades do sistema de inteligência são descritos no Decreto 3.505/2000 que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; na Lei 8.159/91, que dispõe sobre a política nacional de arquivos públicos e privados e no Decreto 7.845/2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informações confidenciais com qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Apesar de ser mencionada explicitamente em ambas as normas, há mais de duas décadas o Brasil carece de uma política nacional específica para inteligência.[27] A falta de uma legislação abrangente para lidar com as atividades de inteligência revela limitações no Sistema de Inteligência brasileiro relacionadas à necessidade de desenvolvimento de normas específicas para operações do dia-a-dia e de modernização de mecanismos de vigilância, o que é realizado pelo Parlamento.

PARA ALÉM DO MARCO LEGAL: AS LACUNAS E OS PROBLEMAS

No que tange a proteção à privacidade diante da vigilância estatal e a regulamentação das atividades de inteligência, o Brasil não vive um vazio legislativo. Contudo, um olhar superficial sobre o marco legal não nos permite observar os problemas existentes, que certamente se agravam com a introdução das tecnologias digitais.

Apesar de estar em grande medida alinhada com os padrões internacionais de direitos humanos, a aplicação da Lei de Interceptações Telefônicas segue um grande desafio. Além de duas CPIs sobre o tema, o Brasil foi condenado pela Corte Interamericana de Direitos Humanos em 2009 pela violação do direito à privacidade no caso Escher *et al.*, que tratava do monitoramento das conversas telefônicas de ativistas do direito à terra no estado do Paraná. A interceptação durou 49 dias e, de acordo com a Comissão Interamericana de Direitos Humanos (CIDH), o Estado não forneceu provas de ter seguido o procedimento legal para a extensão da duração da interceptação. A sentença final concluiu "que as interceptações e gravações das conversas telefônicas objeto deste caso não observaram os artigos 1º, 2º, 3º, 4º, 5º, 6º e 8º da Lei No. 9.296/96 e, por isso, não estavam fundadas em lei". Em consequência disso, a Corte decidiu que o Estado havia violado o direito à privacidade estabelecido no Artigo 11 da Convenção Americana.

Além disso, a incerteza jurídica quanto à condição e ao nível de proteção de metadados e dados pessoais, junto à introdução de mecanismos de retenção de dados nos últimos anos, pode trazer novos riscos à privacidade e

27 Senado brasileiro (14 de julho de 2015). Brasil está há duas décadas sem política nacional de inteligência, alertam especialistas. SENADO NOTÍCIAS. Brasil está há mais de duas décadas sem política nacional de inteligência, alertam especialistas. Disponível em: <http://www12.senado.leg.br/noticias/materias/2015/07/14/brasil-esta-ha-mais-de-duas-decadas-sem-politica-nacional-de-inteligencia-alertam-especialistas>. Acesso em: 07 mar. 2018.

à liberdade de expressão. Como reconheceu o Tribunal de Justiça da União Europeia ao declarar inválida a Diretiva da União Europeia 2006/24/EC – a Diretiva de Retenção de Dados –, "não é inconcebível que a retenção dos dados em questão pode afetar o uso, de assinantes e usuários registrados, dos meios de comunicação abrangidos na diretiva afetando, desse modo, o exercício da liberdade de expressão" e "[a] retenção de dados para a finalidade de possível acesso a eles pelas autoridades nacionais competentes […] afeta direta e especificamente a vida privada".[28]

Vale ressaltar que os legisladores brasileiros começaram a introduzir esses dispositivos no ordenamento jurídico nacional pouco após a aprovação da Diretiva de Retenção de Dados europeia, de 2006, – a Lei No 12.850/2013 sobre crime organizado já prevê a retenção de registros telefônicos, por exemplo. Apesar de alguns Estados-membro que implementaram as leis sobre retenção de dados terem gradualmente declarado-as inconstitucionais e apesar da Diretiva ter sido finalmente anulada em 2014, isso não levou a questionamentos similares no Brasil.

Em relação às atividades de inteligência, a situação é ainda mais grave. A omissão do tema durante o processo de redemocratização, iniciado em 1985, foi acompanhada da preservação do Serviço Nacional de Informações (SNI), um remanescente da ditadura militar que só viria a ser extinto em 1990. Para alguns especialistas, a manutenção do SNI durante esses anos foi resultado de uma percepção de que o órgão já não possuía a força de outrora, bem como devido ao fato de que sua extinção era um pleito associado aos políticos da esquerda, de modo que muitos parlamentares não queriam se envolver em uma disputa ideológica. De qualquer forma, a ideia era que, ao não atribuir importância constitucional às atividades de inteligência, esperava-se que esta seria deixada em segundo plano, o que acabaria enfraquecendo-a, diminuindo assim os poderes dos órgãos de inteligência (GONÇALVES, 2008a; BITENCOURT, 1992).

O resultado disso é que não há na Constituição Federal sequer uma menção às atividades de inteligência. Sem parâmetros constitucionais explícitos, torna-se difícil conciliar a tensão entre o sigilo necessário a essas atividades e a obrigação do Estado em oferecer transparência aos seus cidadãos. Tal como afirma Gonçalves (2008b), a falta de amparo constitucional deixou o Brasil com uma legislação efêmera ao tratar das

28 Grand Chamber, Digital Rights Ireland Ltd. (C–293/12) v. Minister for Communications, Marine and Natural Resources. 8.04.2014. Parágrafos 28 e 29. EUR-LEX.EUROPA. JUDGMENT OF THE COURT (Grand Chamber). Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1>. Acesso em: 07 mar. 2018.

competências e atribuições da ABIN e dos órgãos do SISBIN. Sem isso, não existe uma noção clara dos mecanismos de controle da atividade de inteligência, deixando esses serviços sujeitos a desvios de conduta e vulneráveis a mudanças conjunturais em sua estrutura, organização e missão.

As mesmas limitações constitucionais à vigilância das comunicações tampouco foram eficazes em prevenir abusos em relação às atividades de inteligência no período democrático. Pelo contrário, a legislação limitada em relação à inteligência e a ausência de especificações sobre os procedimentos a serem adotados pela ABIN implicam em uma série de vazios regulatórios que, por um lado não previnem a realização de atividades de vigilância ou o acesso a informações dos cidadãos e, por outro, não delimitam o que seria ou não permitido. Além disso, as obrigações de transparência e prestação de contas e o formato da agência de supervisão das atividades de inteligência não estão devidamente detalhados ou claros.

Com o fim da ditadura e, em sequência o enfraquecimento e extinção do SNI, não houve um movimento consistente de construção de um sistema de inteligência que o substituísse. Com isso, diversos atores foram ocupando esse lugar vago, conforme seu poder de atuação. Esse cenário acabou favorecendo a atuação de outras instituições públicas e privadas nas atividades de inteligência, que ganharam poderes e uma margem maior de operação a partir de interpretações sobre as escassas leis sobre o tema. Hoje, no Brasil, há uma ausência de compreensão sobre o papel das agências e instituições voltadas para a inteligência e um certo estranhamento em relação ao papel dessa atividade em um regime democrático.

CONSIDERAÇÕES FINAIS: A NECESSIDADE DE MAIS DEFINIÇÕES LEGAIS

A expansão da Internet e de tecnologias de informação e comunicação contribuiu para o fortalecimento da capacidade de vigilância do Estado, que passou a empregar novos mecanismos de monitoramento e controle. Contudo, se por um lado esse Estado se apropria de recursos cada vez mais avançados de vigilância e coleta de dados, a sociedade também passa a ter acesso a meios que a torna capaz de demandar informações do governo, a partir da institucionalização de mecanismos para o acesso à informação. Normas como a Carta de Serviços ao Cidadão (Decreto 6.932/2009) e a Lei de Acesso à Informação (Lei 12.527/2011) servem de medidas compensatórias na relação de poder entre Estado e sociedade. Além do acesso a tecnologias capazes mitigar a intromissão estatal – e de outros agentes – na vida privada, como é o caso da criptografia, por exemplo.

Contudo, apesar da possível compensação legal para o desequilíbrio informacional entre Estado e cidadãos, a capacidade e implementação de tecnologias na área de vigilância e avançou nos últimos anos em grande medida sem controle social.

Como fica evidente a partir da análise normativa e dos problemas e limitações apresentados, o marco existente para a vigilância das comunicações na era digital não dá conta do cenário atual em que o acesso a dados armazenados e inclusive a metadados associado a uma capacidade razoável de processamento pode revelar ainda mais sobre os hábitos mais íntimos dos indivíduos do que a gravação de suas comunicações. Nesse sentido parece ser necessário retomar as discussões sobre a Lei de Interceptações Telefônicas, mas ir além no debate sobre o que de fato se busca proteger constitucionalmente quando se trata de confidencialidade das comunicações e quais as particularidades que devem ser levadas em consideração quando se fala especificamente em comunicações digitais. Na época da sua criação, optou-se por uma lei enxuta, com o intuito de evitar uma ingerência do Estado nas comunicações privadas. Ocorre que isso tornou a lei suscetível a interpretações que acabaram flexibilizando-a e, consequentemente, fragilizando suas garantias. Com o tempo, essa fragilidade tornou-se ainda maior.

No âmbito das atividades de inteligência, é preciso esclarecer, por meio de lei, qual papel será desempenhado pelos órgãos integrantes do Sistema Brasileiro de Inteligência. A Política Nacional de Inteligência, publicada em 2016, bem como a Estratégia Nacional de Inteligência, de 2017, pouco esclarecem nesse sentido. Esta última chega a mencionar expressamente que as atividades de inteligência devem respeitar os direitos e as garantias fundamentais expressos na Constituição, bem como elenca os princípios éticos que as orientam: respeito, imparcialidade, cooperação, discrição, senso crítico e excelência. Contudo, essas determinações não são suficientes. É necessário delimitar o papel e os modos de atuação da ABIN, bem como o papel das polícias, da área de inteligência do Ministério Público e das Forças Armadas. Essa delimitação vai permitir o fortalecimento desse tipo de atividade, ao mesmo tempo em que vai prevenir abusos. Por fim, se debruçar sobre o detalhamento legal dos limites e papéis dos órgãos de inteligência significa responder à pergunta a respeito do lugar que essa atividade deve ocupar em um regime democrático. Do modo como está, nos parece que as lacunas serão preenchidas da pior forma possível.

REFERÊNCIAS

BITENCOURT, Luis Antônio. *O poder legislativo e os serviços secretos no Brasil, 1964-1990*. Brasília: Faculdades Integradas Católica de Brasília, 1992.

CÂMARA DOS DEPUTADOS. RELATÓRIO. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/53a-legislatura-encerradas/cpiescut/relatorio-final-aprovado/Relatorio-Final-Versao-Final.pdf>. Acesso em: 07 mar. 2018.

DAHLMANN, Anja ***et al.*** Privacy and Surveillance in the Digital Age**:** a Comparative Study of the Brazilian and German Legal Frameworks. 2016 Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/16672>. Acesso em: 07 mar. 2018.

ESCHER ***et al.*** vs. Brasil no parágrafo 131. 2009. Disponível em: <http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf>. Acesso em: 07 mar. 2018.

ESUBSCRIPTION TO UNITED NATIONS DOCUMENTS. Resolution adopted by the General Assembly on 18 December 2013. Disponível em: <http://undocs.org/A/RES/68/167>. Acesso em: 29 ago. 2017.

EUR-LEX.EUROPA. JUDGMENT OF THE COURT (Grand Chamber). Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1>. Acesso em: 07 mar. 2018.

FOUCAULT, Michel. ***Segurança, território e população***: curso dado no Collège de France (1977-1978). São Paulo: Martins Fontes, 2004.

GONÇALVES, Joanisval B. Conhecimento e poder: a atividade de inteligência e a Constituição brasileira. In: Bruno Dantes; Eliane Cruxên; Fernando Santos; Gustavo Ponce de Leon Lago (Orgs.). ***Constituição de 1988:*** o Brasil 20 anos depois (v. III – A Consolidação das Instituições). Brasília: Senado Federal, Instituto Legislativo Brasileiro, p. 591-607, 2008b.

GONÇALVES, Joanisval B. ***Sed Quis Custodiet Ipso Custodes?:*** o controle da atividade de inteligência em regimes democráticos: os casos de Brasil e Canadá. 2008. 797p. Tese (Doutorado em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2008a.

HACKING TEAM. About us. Disponível em: <http://www.hackingteam.it/about.html>. Acesso em: 29 ago. 2017.

HARRIS. About Harris. Disponível em: <https://www.harris.com/about>. Acesso em: 29 ago. 2017.

JUSTICE AND CONSUMERS. Article 29 Working Party. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf>. Acesso em: 07 mar. 2018.

KENT, Sherman. ***Strategic Intelligence for American World Policy.*** Princeton, NJ: Princeton University Press, 1966.

LOGO TECHNOLOGIES. About us. Disponível em: <https://www.logostech.net/about-us/>. Acesso em: 29 ago. 2017.

MELLO, Cesar A. B. D. *Curso de Direito Administrativo*. refund. ampl. e atual. São Paulo: Malheiros, 2001.

NUCCI, G. de Souza. *Leis penais e processuais penais comentadas*. São Paulo: Revista dos Tribunais, 2006.

PRADO, Geraldo. *Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça.* Rio de Janeiro: Lumen Juris, 2006.

PRIVACY INTERNATIONAL. Privacy International Launches International Campaign For Greater Transparency Around Secretive Intelligence Sharing Activities Between Governments. 23 out. 2017. Disponível em: <https://www.privacyinternational.org/node/51>. Acesso em: 29 ago. 2017.

SENADO NOTÍCIAS. Brasil está há mais de duas décadas sem política nacional de inteligência, alertam especialistas. Disponível em: <http://www12.senado.leg.br/noticias/materias/2015/07/14/brasil-esta-ha-mais-de-duas-decadas-sem-politica-nacional-de-inteligencia-alertam-especialistas>. Acesso em: 07 mar. 2018.

THE GUARDIAN. Microsoft, Facebook, Google and Yahoo release US surveillance requests. Disponível em: <https://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests>. Acesso em: 29 ago. 2017.

THE WEEK. Disponível em: <http://theweek.com/articles/640048/going-olympics--brazil-watching>; <http://www.cartacapital.com.br/sociedade/olimpiadas-no--brasil-201cpremiam201d-a-industria-da-vigilancia>. Acesso em: 7 jul. 2016.

UNITED NATIONS HUMAN RIGHTS. Contributions from stakeholders: Right to privacy in the digital age. Disponível em: <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/Contributions.aspx>. Acesso em: 7 mar. 2018.

VICENTE, João Paulo. Como as Olimpíadas ajudaram o Brasil a aumentar seu aparato de vigilância social. MOTHERBOARD, 7 jul. 2016. <https://motherboard.vice.com/pt_br/article/como-o-brasil-aprimorou-seu-aparato-de-vigilancia-social-para-as-olimpiadas>. Acesso em: 29 ago. 2017.

INFORMAÇÕES DE DEFESA E SEGURANÇA NACIONAL: ENTRE A LEGITIMIDADE DO SEGREDO E O DIREITO À INFORMAÇÃO

KARINA FURTADO RODRIGUES

INTRODUÇÃO

De onde vem o direito dos Estados de gerar e guardar segredos? Se os segredos não podem ser evitados e, por conseguinte, os quisermos "democráticos", quais serão os processos pelos quais um segredo se torna legítimo? Este estudo pretende explorar as nuances que envolvem o sigilo e a transparência no campo da defesa nacional – envolvendo, por conseguinte, as Forças Armadas.

De maneira geral, as leis de acesso à informação vêm estabelecendo novos limites para restrições de acesso a documentos públicos. Começa-se a implementar a transparência como regra e o sigilo como exceção, restringindo-o ao mínimo necessário através de medidas *de jure* e *de facto*.

Em termos *de jure*, diversos padrões internacionais para o acesso à informação vêm surgindo, como nos Princípios em Legislação de Liberdade de Informação da Artigo 19 (1999), e nos Tshwane Principles (OPEN SOCIETY JUSTICE INITIATIVE, 2013), tratando especificamente da área de defesa e segurança nacional.

Contudo, se para estabelecer a regra da transparência há que se modificar o sigilo como regra, torna-se mister compreender as facetas que envolvem o sigilo de informações em sua prática cotidiana: *de facto*, o que ainda impera para informações de defesa e segurança nacional é o direito ao sigilo. O ônus da prova de que uma informação deveria ser transparente ou não ainda é do cidadão.

Os vazamentos de informações sigilosas do governo americano sobre monitoramento de comunicações, sem mandado judicial, levantaram um intenso debate sobre a prática do sigilo e sobre até que ponto as agências de defesa nacional se inserem nos princípios democráticos. Fato é que as

agências de defesa nacional escondem informações muito facilmente, sem pesos e contrapesos eficientes até mesmo em democracias ditas avançadas (KATYAL; CAPLAN, 2008; KLAUS, 2016).

Isto nos remonta aos trabalhos de Bentham – em Thompson (1999) – e Colaresi (2014), que exploram a capacidade do Estado em gerar segredos além do que se pode acessar através das leis; e também ao de Sagar (2013), que defende que não há formato institucional capaz de evitar o abuso do sigilo, e que o receio de que haja vazamentos de informação seria a única forma de conter esses abusos.

A era da informação também traz muitos e desconhecidos desafios para a defesa nacional, e um coadjuvante essencial é a tecnologia. Através dela é possível promover o compartilhamento instantâneo e sem custos de um sem número de informações. Do ponto de vista da teoria do mosaico,[1] informações contidas em plataformas de dados abertos, transparência ativa, passiva ou quaisquer outros registros *on-line* também podem ser usados contra os Estados e, consequentemente, contra seus cidadãos.

Ao mesmo tempo, ela abre portas para o engajamento da sociedade com a eficiência e efetividade das políticas públicas. A crise da democracia representativa gerou a necessidade de novos arranjos em que a participação é muito mais direta. Pode-se tentar contestar os benefícios resultantes desta participação, mas fato é que governos têm de lidar com isso e com repercussões públicas muito maiores do que se podia imaginar há alguns anos atrás (KEANE, 2011; MICHENER, 2012).

Se as relações de poder historicamente construídas se baseiam no Estado como "principal" e os cidadãos como "agentes", a tecnologia também trabalha para o inverso – e ao que realmente se propõe a democracia. A mesma lógica da teoria do mosaico, focada nos inimigos do estado pode ser aplicada à militância da sociedade civil em utilizar estes dados para expor casos de corrupção, má gestão e violação de direitos, obrigando o poder constituído a dar satisfações.

Posto isto, este estudo se divide em cinco seções, além desta introdução. A segunda seção trata sobre a lógica por detrás do Estado como definidor do que é "bem-comum" e, por conseguinte, definidor de qual informação deve ser secreta ou não, e como ela é desafiada pela visão corporativista do Estado. A terceira seção explora os pesos e contrapesos relativos à capacidade de segredo existentes, seja pela via institucional, seja pelo medo de exposição – vazamentos de informação.

1 Teoria do Mosaico: a partir de pequenos fragmentos de informação, atores tidos como inimigos podem compreender estratégias maiores de defesa de um Estado, resultando em risco para a segurança nacional. Tratarei mais deste tópico na seção 2.

A quarta seção apresenta uma análise do direito ao segredo e do direito à informação em defesa nacional no Brasil, mostrando como se configuram os pesos e contrapesos do sigilo no país. A sexta e última seção apresenta as considerações finais e aponta para futuros estudos.

DEMOCRACIAS COM SEGREDOS: ENTRE A LÓGICA E O DILEMA

A coexistência de capacidade de segredo e participação democrática traz em si antagonismo, na medida em que apesar da democracia, existe em seu seio instituições de natureza não democrática. Este é o chamado "dilema do segredo" nas democracias. Para compreender o primeiro e mais antigo lado da moeda – a capacidade de gerar e manter segredos –, é preciso compreender seu uso e a necessidade de usá-la.

De acordo com Thompson, "o conflito não é essencialmente entre segredo e democracia, mas surge dentro da ideia do processo democrático em si. Algumas das melhores razões para o sigilo podem ser encontradas nos mesmos valores democráticos que advogam contra o sigilo" (THOMPSON, 1999, p. 182, tradução nossa).

Um documento de caráter sigiloso[2] geralmente faz referência a uma informação que, se publicitada irrestritamente, pode causar danos a terceiros ou inviabilizar determinada ação. No âmbito da defesa nacional, o excesso de transparência poderia colocar em risco inclusive a segurança de pessoas e do próprio país, em face da revelação de estratégias a inimigos (LORD, 2006; SCHOENFELD, 2010).

Colaresi (2014) versa sobre diversos casos ocorridos durante a Segunda Guerra Mundial e a Guerra Fria em que o sigilo atuou de três formas diferentes: (1) na antecipação aos fatos, (2) na capacidade de enganar o inimigo e (3) na inutilização de capacidades de inimigos só tiveram sucesso com a plena utilização do sigilo.

Nesta mesma lógica, o principal agente responsável pelo cálculo deste dano é o próprio criador e utilizador daquela informação, o que traz novamente a essência do dilema do segredo nas democracias – quem, quando e como verificar esta avaliação, especialmente quando se relacionam a ações altamente sensíveis para a segurança nacional?

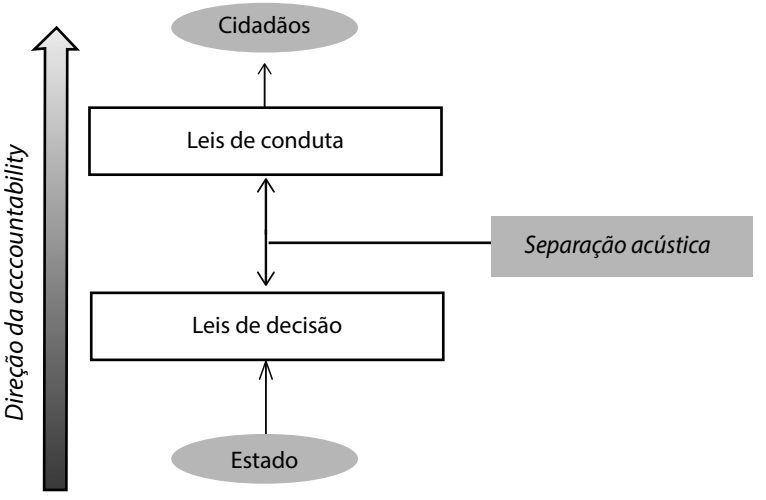
2 No âmbito da arquivologia, são três as categorias de documentos sigilosos: aqueles relativos à (1) defesa nacional, (2) à vida privada das pessoas e (3) àqueles protegidos por lei, como sigilo industrial, científico, de propriedade intelectual e investigativo (DUCHEIN, 1983). Neste estudo foca-se apenas nos segredos de defesa nacional.

A ideia de que o Estado, e não os cidadãos, tem ingerência sobre o sigilo de informações está presente nos trabalhos de um dos mais progressistas autores clássicos da temática da transparência, Jeremy Bentham.[3]

Em sua visão utilitarista do Direito, Bentham parte do princípio de que o Estado e o Direito deveriam proporcionar aos seus cidadãos o máximo de utilidade possível, onde utilidade se traduziria em uma ideia de felicidade ou bem comum. Em nome desse bem comum, o Estado teria carta branca para desenhar sistemas de leis que, inclusive, poderiam servir para enganar seus cidadãos (THOMPSON, 1999).

Esta lógica se reflete no modelo de Direito Penal formulado por ele em que os cidadãos pensariam existir certa lei de pena capital, sem que ela realmente fosse colocada em prática. O autor sugere que a lei de pena capital poderia ser vigente como "lei de condução", ou seja, existindo somente no papel para gerar coerção preventiva. Do outro lado, nas "leis de decisão", o Estado se encarregaria de manter encarcerados – mas nunca os privar da vida – os presos condenados sob tal pena. A diferença entre as leis de conduta e as leis de decisão é o que ele chama de separação acústica das leis (THOMPSON, 1999).

Figura 1 – Separação acústica



Fonte: Adaptação de Thompson (1999).

3 Filósofo e jurista famoso por ser um dos precursores do utilitarismo e por conceber a ideia da prisão Panóptico, explorada por Foucault.

A ideia parece arcaica por envolver algo tão sensível como a pena de morte. Contudo, sua lógica está presente em diversos casos de políticas de defesa nacional e inteligência: são aquelas que, desde sua criação, nunca vislumbraram a ideia de serem publicitados, inclusive de acordo com os ditames da lei ou de seus representantes.

No caso do escândalo sobre o programa de vigilância global pela National Security Agency (NSA) dos Estados Unidos, a "lei de condução" – que pode não se refletir necessariamente em uma lei, mas também na ausência de legislação restritiva – consistiu na afirmativa de que tal programa não existia – ele precisava se manter secreto para ser levado a cabo com eficiência.

A lei de decisão, por sua vez, estipulava inclusive a supressão de direitos constitucionais como o da privacidade. Prova disto é que o programa operava com o consentimento de alto escalão do governo e só veio à tona através de uma quebra ilegal de sigilo (KATYAL; CAPLAN, 2008; SAGAR, 2013).

A incongruência no pensamento de Bentham é que, apesar de sua visão utilitarista do direito, também advoga por uma transparência total e permanente das ações de atores do Estado, colocando a publicidade dos atos do governo como o grande antídoto para a tentação ao abuso de poder, e o segredo como o vilão de um governo por se opor aos princípios de livre mercado (BENTHAM, 1843; GAONKAR; MCCARTHY, 1994; HOOD; HEALD, 2006).

Na prática, quando o assunto é inteligência e defesa, a visão utilitarista da busca por um "bem comum" definido mais pelo Estado do que por outros atores ainda se sobressai à visão da publicidade e participação democráticas. Como afirma Colaresi (2014, p. 3, tradução nossa), "[…] a habilidade de se guardar segredos em democracias não é uma exceção, e sim a regra".

Contudo, se Bentham não explicita a radical mudança na definição de bem-comum entre sua "diferença acústica" nas leis e a defesa da publicidade como valor maior, outras correntes – como os estudos sobre corporativismo[4] – se propuseram a debatê-la.

No corporativismo de Stepan[5] (1980), o Estado figura como único ator legítimo para definir as ações necessárias para se alcançar o "bem-comum".

4 Este conceito se opõe à perspectiva pluralista das políticas públicas, que considera a competição livre de atores autônomos em uma democracia (COLLIER, 1995). Veja também Romano (2009) em sua análise das perspectivas pluralista e elitista em políticas públicas.

5 Há diversas definições de corporativismo. Uma corrente enfoca o Estado como agente corporativista independente (COLLIER, 1995; STEPAN, 1980) e outra que enfoca a subordinação do Estado a interesses e grupos privados (SIAROFF, 1999) Neste estudo foca-se na primeira perspectiva.

Contudo, o Estado se orienta também por suas próprias metas e sobrevivência, constituindo-se como ator independente e não como representante do povo.

Em decorrência disto, líderes políticos institucionalizariam ampla e legalmente diversas formas de participação, no intuito de evitar governar por coerção. Contudo, essa participação ocorre sob tutela do Estado, e os participantes teriam apenas papel consultivo. Isto também pode significar alguns grupos específicos de civis ganhando privilégios de participação enquanto o Estado gerencia estes privilégios de acordo com seus próprios interesses (STEPAN, 1980).

Um Estado corporativista traz consequências para as instituições que nele habitam: neste contexto seus atores institucionais tendem a não confiar em tomadores de decisão e legisladores, levando a um comportamento de autoproteção generalizado das instituições (PION-BERLIN; UGUES; ESPARZA, 2012).

De acordo com Pion-Berlin *et al* (2012), isto é precisamente o que acontece com as Forças Armadas latino-americanas que, ao não confiarem na definição de bem comum imposta pela liderança política civil – corporativista e auto interessada – assume posturas e ações também corporativistas e de sobrevivência.

O debate sobre corporatismo ainda ilustra diversos casos de monopólio de decisões em política pública na América Latina, e o setor de defesa nacional é um deles. Contudo, o conceito vem perdendo seu poder explicativo em face da emergência de diversas outras formas de participação e mobilização populares (COLLIER, 1995). Como afirma Keane (2011), um novo tipo de relação entre sociedade civil e Estado vem ganhando força, o que ele chama de democracia monitorial. Este tipo de democracia é caracterizado pela multiplicação de estruturas de controle, sejam internas ou externas ao próprio Estado.

Estas novas estruturas fomentam uma aproximação ao pluralismo na medida em que desconcentram o poder tradicionalmente mantido pelas elites, tanto na sua forma de executores de políticas – poder Executivo – e formuladores de leis – poder Legislativo –, quando como detentores da informação e formação de opinião pública – mídia.

Contudo, conforme Klaus (2016) aponta, as Forças Armadas são as instituições que menos aderiram às reformas de transparência, respaldadas na crença mítica da incorruptibilidade do soldado, da alta confiança nos militares como instituição – em detrimento dos políticos – e, inclusive, em uma nostalgia pelo autoritarismo no caso de países que passaram por ditaduras.

O bem-comum no âmbito da defesa nacional, por conseguinte, ainda permanece velado por uma separação acústica de difícil mensuração, mas desafiada pela crescente cultura de transparência que, aos poucos e com alguns vazamento de informações, atinge as forças armadas e de inteligência.

PESOS E CONTRAPESOS

A legitimidade da sociedade civil em "saber" é algo novo e ainda enfrenta muitas dificuldades principalmente no que tange à qualidade e inteligibilidade das informações (MICHENER; BERSCH, 2013). Se pesquisadores encontram barreiras no acesso à informação nos três poderes,[6] com perguntas sem relação com atividade sensíveis do Estado, imagina-se que as dificuldades no campo da defesa nacional sejam ainda maiores.

Dentre as instituições democráticas existentes, as forças armadas são as que mais tiveram sucesso em manter sua capacidade de gerar e manter segredos. Narcís Serra (2010) afirma que os militares foram capazes de preservar "domínios reservados" de políticas públicas, conhecimento e informação, mantendo assim algumas prerrogativas que antes lhe eram facultadas nos regimes militares anteriores à terceira onda democrática.

Como assegurar que o segredo não está sendo usado para acobertar violações da lei? Para resolver essa questão, há de se discutir pesos e contrapesos possíveis neste contexto de sigilo, tanto através do controle direto dos cidadãos quanto através de vias indiretas.

Vários organismos internacionais vem traçando diretrizes gerais a serem seguidas na seção de exceções das leis (ARTICLE 19, 2006; OPEN SOCIETY JUSTICE INITIATIVE, 2013). Com isto, colocou-se que o sigilo e as restrições a informações deveriam estar bem descritos na lei e em decretos decorrentes. Admitiu-se também que as exceções são necessárias, mas que devem ser restritas a interesses específicos.

Um exemplo emblemático da necessidade de sigilo é o caso da encriptação de códigos de comunicação militares. A divulgação deste tipo de informação poderia ser extremamente danosa às atividades de defesa, não só por expor comunicações atuais, mas também porque geralmente estes códigos são incrementos de códigos mais antigos. No entanto, informações menos sensíveis – como o orçamento anual dedicado a operações

6 Diversas foram as avaliações de transparência realizadas pelo Programa de Transparência Pública da FGV e pelo Artigo 19 mostrando o baixo retorno a pedidos de acesso à informação e à baixa qualidade das respostas (MICHENER; VELASCO; FURTADO, 2014; MONCAU *et al.*, 2015).

antiterroristas – não pode ser considerado ameaçador automaticamente, devendo ser aberto ao público (OPEN SOCIETY JUSTICE INITIATIVE, 2006; RODRIGUES, 2013).

Contudo, não há um consenso na literatura sobre quais estruturas são capazes de restringir a discricionariedade dos burocratas de defesa na questão do sigilo. Colaresi (2014) defende a via institucional para regular o segredo. Sagar (2013), por sua vez, desacredita de mecanismos institucionais afirmando que apenas vazamentos de informação – ou o medo deles – seria um controle efetivo. As próximas subseções exploram cada uma destas visões.

CONTROLE PELA VIA INSTITUCIONAL

Há diversas formas democráticas de se moderar segredos que não imporiam barreiras às ações das agências de segurança, ao mesmo tempo que permitindo a criação de consenso, confiança e avaliação retrospectiva destas políticas por parte da população e grupos interessados. Seria necessário levantar o véu do segredo apenas o suficiente para que fosse assegurada a ausência de ineficiência, corrupção e ações puramente corporativistas (MENDEL, 2008; MICHENER, 2010; SCHULHOFER, 2010; STEPAN, 1980; THOMPSON, 1999).

Dentre os diversos mecanismos institucionais de controle do segredo presentes na literatura, estão os seguintes:

- Publicação de lista com motivos pelos quais se pode classificar documentos ou restringir o acesso a eles

Ao obrigar o agente do Estado a enquadrar a informação em um tipo de motivo de classificação, restringe-se as possibilidades de mal-uso da classificação. De acordo com os Princípios de Tshwane (OPEN SOCIETY JUSTICE INITIATIVE, 2013), a lista de motivações para classificação – princípio 9 – inclui:

1. informação sobre ações em andamento,
2. informações sobre produção, capacidades, armamento e sistemas militares,
3. informações sobre medidas específicas para salvaguardar o território;
4. informações de inteligência; informações sensíveis concedidas por terceiros.

Nota-se aqui que, dentre as recomendações está o registro por escrito de todas as informações e comunicações – o que nem sempre é feito.

- Teste de dano e de interesse público

Este teste consiste na avaliação do dano *versus* os benefícios de se socializar a informação, feita por terceiros não envolvidos com a produção da informação. De acordo com o relatório da OSF (2006) e com Mendel (2008), este mecanismo poderia ser utilizado para liberar informações mesmo que estas pudessem causar algum dano à defesa ou a informações pessoais – tudo depende do consenso que o interesse público é maior do que estes danos.

Há também autores que não concordam com este tipo de teste. De acordo com García (2009), a utilização da justificativa de "interesse público" para se ter acesso a determinada informação não seria suficiente para sua abertura, uma vez que a própria segurança nacional poderia ser categorizada como de interesse público.

Uma forma de solucionar parcialmente este dilema é através da criação de uma lista de tópicos considerados de alto interesse público, limitando tanto o sigilo quanto a transparência. Dentre os tópicos comumente listados nas leis de acesso à informação figuram possíveis violações de direitos humanos – presente na lei mexicana e brasileira; informações relevantes e urgentes sobre a segurança pública, saúde e desastres naturais – presente na lei armênia; além de informações sobre o real desempenho da economia, educação e meio ambiente (OPEN SOCIETY JUSTICE INITIATIVE, 2006; RODRIGUES, 2013).

- Criação de órgão de controle autônomo, responsável pela liberdade de informação

Isto pode incluir ou não o poder de sanção do órgão que, principalmente no que tange à gestão de arquivos das forças armadas, ainda é bastante débil (HOTT, 2005).

Contudo, Michener (2011, p. 11) sustenta que além da sanção, uma importante ferramenta é a do incentivo à transparência. "Os defensores da liberdade de informação devem assegurar que os incentivos à transparência sejam consideravelmente suficientes para dissuadir o sigilo".

É importante ressaltar que neste processo de monitoramento também se insere a manutenção de arquivos e a destruição de documentos (NEUMAN; CALLAND, 2007), itens essenciais quando se fala de documentos de defesa nacional. São justamente estes documentos os mais afetados pela situação arquivística de um país, já que em teoria só estarão disponíveis ao público depois de desclassificados – depois de 5 a 50 anos do dia em que foram criados.

- Estabelecimento de tempos-limite para a restrição de acesso a uma informação.

De acordo com Hood e Heald (2006), esta é a chamada transparência em retrospecto, seguindo a lógica de que o custo de tornar uma informação pública decresce com o tempo. A transparência em retrospecto é uma das ferramentas mais utilizadas pelos governos para resguardar informação e, ao mesmo tempo, ferramenta controle e acesso a informações por parte da sociedade civil.

- Liberação do documento com somente as partes classificadas ocultas e elaboração de versões públicas de documentos e diretrizes classificados

Um problema comum em relação a sigilo é a negação da informação por completo, mesmo quando somente parte do documento é sigiloso. De acordo com Mendel (2008), somente uma passagem sigilosa não é motivo suficiente para determinar a restrição total de acesso: mecanismos a liberação de documentos com apenas fragmentos restritos já é mecanismo amplamente debatido no âmbito internacional. Além disto destaca-se a prática da elaboração de versões públicas de documentos, presente na LAI mexicana. Um documento cujo interesse público é grande, mas de teor altamente sensível, pode ser publicado em versão que permita o controle social sem danificar a política na qual está inserido (COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2012).

CONTROLE PELO MEDO DE EXPOSIÇÃO

Sagar (2013) afirma que estes novos designs institucionais nunca serão suficientes para controlar a capacidade de sigilo do Estado. Para ele "o único mecanismo de controle realmente confiável para monitorar o uso do segredo de Estado não coaduna com valores morais e políticos e, especialmente, com as regras democráticas" (SAGAR, 2013, p. 3, tradução nossa).

O autor defende que a única forma de exercer pressão sobre os governantes para não manter segredos escusos é a ameaça de vazamentos de informação. A lógica dele é a seguinte: qualquer que seja o ator responsável por monitorar os segredos de Estado vai ter suas próprias razões para fazer mal-uso do segredo ou da transparência indevida (SAGAR, 2013).

No caso de instituições autônomas de controle, a própria forma de indicação de seu chefe já ofereceria dicas sobre como a instituição vai atuar; as comissões legislativas poderiam fazer uso político das informações sensíveis a que possuírem acesso (SAGAR, 2013); o judiciário, como mostra Pozen

(2014), muitas vezes prefere não discordar com as decisões de sigilo do Executivo por uma diversidade de razões mas, principalmente, porque não domina suficientemente o tópico de defesa nacional para julgar.

Fica claro aqui que a perspectiva de Sagar é a de um Estado corporativista em que suas instituições também vão atuar em benefício próprio na tentativa de sobreviver, e não a favor do onipresente e nebuloso "bem-comum" das teorias de Bentham.

De fato, nas democracias pode haver diferentes graus de institucionalização do vazamento de informações através do estabelecimento ou não de proteção a *whistleblowers*.[7] Vale ressaltar que nem sempre a presença de leis de proteção a denunciantes se traduzem em práticas fortes.

No caso dos Estados Unidos, Ramirez (2007) afirma que a lei americana de então trazia ainda muitos perigos e dificuldades para ser utilizada pelo cidadão comum. A utilização da denúncia por parte de membros do governo também vem sendo alvo de grandes debates, principalmente no que toca o perdão a Edward Snowden. As opiniões variam entre a responsabilização penal por vazamentos que afetem a segurança nacional (SCHOENFELD, 2010), e a proteção do direito de denunciar inclusive em casos em que a defesa do país está em jogo (SAGAR, 2013).

Uma pergunta que ainda permanece é a seguinte: aqueles que vazam informações são traidores, espiões ou denunciantes? Se se parte de cada uma dessas concepções, cada visão divergente poderia ser justificada com louvor. Entretanto, no caso dos Estados Unidos é crescente a defesa da opinião de que os responsáveis por vazamentos cujo objetivo era de trazer questões para o debate público, deveriam ser tratados como denunciantes, e não como traidores ou espiões (PAPANDREA, 2014).

SEGREDO À BRASILEIRA

Como se estrutura hoje a capacidade de segredo no Brasil e quais são os mecanismos de pesos e contrapesos existentes? O Brasil possui um histórico de longos períodos não democráticos. Tomando por base desde o Estado Novo, passando pela turbulenta janela democrática de 1945-1964, perpassando pelo regime militar de 1964 a 1985, o Brasil foi marcado

7 A proteção a denunciantes é, inclusive, um dos princípios de direito à informação elaborados pela Artigo 19 (MARTINS, 2011).

por reformas lentas e incrementais no que tange o acesso à informação (HOTT, 2005).[8]

Decerto houve muitos avanços na transparência governamental brasileira desde a democratização. São exemplos destes avanços a Lei de Arquivos de 1991 (Lei 8.159), a Lei Complementar 131/2009 que estabelece maior transparência às finanças públicas e, por fim, a Lei de Acesso à Informação de 2011 (Lei 12.527).

Contudo, as mudanças institucionais no âmbito de transparência em defesa são, muitas vezes questionadas em sua profundidade (KLAUS, 2016), assumindo um processo de característica gradual, sem grandes choques exógenos, através da superposição de leis e da reinterpretação de regulamentos (MAHONEY; THELEN, 2010).

Até 2005, a abertura dos arquivos da repressão pelo do governo Lula parecia um alvo inatingível Contudo, depois de pressões da imprensa e de diversos grupos da sociedade civil, o presidente Lula assina o decreto 5.584/2005, estipulando o recolhimento de quaisquer documentos gerados pelos órgãos de repressão durante a ditadura militar (HOTT, 2005; RODRIGUES, 2013).

Após este marco, o próximo grande avanço legal em termos de acesso a documentos de defesa nacional foi a Lei de Acesso à Informação. Nota-se que o processo de aprovação da lei foi foco de caloroso debate no Senado, tendo como figura central o então presidente da Comissão de Relações Exteriores e Defesa Nacional (CRE) Fernando Collor (RODRIGUES, 2013).

A grande bandeira da CRE, respaldada por diplomatas e militares, era relativa à permanência da premissa de sigilo eterno de documentos, incluída na legislação brasileira a partir do decreto 4.553/2005.[9] Foram cerca de quatro meses de espera pela aceitação da CRE de que isto não mais seria possível. As resistências militares e diplomáticas se aquiesceram e a lei foi aprovada pela presidenta Dilma Rousseff, juntamente com a criação da Comissão Nacional da Verdade (RODRIGUES, 2013).

---

8 Para um estudo amplo das leis e decretos referentes a documentos sigilosos no Brasil até 2004, veja a dissertação de mestrado de Hott (2005), intitulada *O acesso aos documentos sigilosos: um estudo das comissões permanentes de avaliação e de acesso nos arquivos brasileiros.*

9 A qual o presidente Fernando Henrique disse que assinou "sem querer", nos últimos dias de seu governo (REVISTA VEJA, 2011).

A Lei de Acesso à Informação e decretos posteriores[10] abriram um importante precedente para o exercício do direito de informação: obrigaram qualquer ente público a ter de dar uma resposta a uma petição individual do cidadão – e isto incluiu as Forças Armadas. Contudo, deixou de lado alguns pontos importantes de controle institucional já bem conhecidos pela academia e organizações internacionais pró-transparência. Dentre os mecanismos institucionais de pesos e contrapesos presentes na Lei 12.527 estão:

- lista com motivos possíveis para classificação, presente no Artigo 23. Dentre os motivos de classificação relacionados à defesa nacional estão os incisos I, V e VIII;[11]
- estabelecimento de tempos-limite para a restrição de acesso, presente no artigo 24 que estipula prazos; e 27, que indica as autoridades com poder de classificação. Documentos ultrassecretos possuem acesso restrito por 25 anos,[12] prazo este renovável apenas uma vez;[13] documentos secretos têm restrição de 15 anos e documentos reservados uma restrição de 5 anos.
- liberação do documento com somente as partes classificadas ocultas. Este mecanismo é estipulado no artigo 7º, parágrafo 2.[14] Em relação à elaboração de versões públicas de documentos e diretrizes classificadas, infelizmente não há dispositivo que permita este tipo de acesso.

Dentre as ferramentas de controle ausentes ou menos desenvolvidas na legislação brasileira estão as seguintes:

- teste de dano e de interesse público. Esta ferramenta não é formalizada na lei e existe parcialmente através de dois mecanismos:

---

10 Decreto 7724/2012, que regulamenta a lei 12.527 e o decreto 7845/2012, que regulamenta o tratamento de informações sigilosas e cria o Núcleo de Segurança e Credenciamento.

11 São passíveis de classificação as informações cuja divulgação irrestrita possam: "I - I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; V - prejudicar ou causar risco a planos ou operações estratégicas das Forças Armadas; VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações".

12 Art. 24, parágrafo 1º.

13 Art. 35, parágrafo 2º.

14 Lei 12.527/11, art. 7, parágrafo 2º: "§ 2o Quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo."

através da possibilidade de se mover recursos a respostas consideradas insatisfatórias e através da aplicação do artigo 21 da lei, que estipula que não se pode negar acesso a informações concernentes a direitos fundamentais e violações de direitos humanos. Em relação aos recursos, a lei 12.527 prevê todo o processo dentro do próprio Executivo,[15] o que pode ser limitador de sua eficiência. A última instância recursal, a Comissão Mista de Reavaliação de Informações,[16] é composta por dez diferentes Ministérios, sem procedimentos e tópicos de interesse público explicitados legalmente além daquele no artigo 21º da lei de acesso.

- Criação de órgão de controle autônomo responsável pela liberdade de informação: A lei de Acesso à Informação estipulou a Controladoria Geral da União (CGU) como órgão fiscalizador do cumprimento da lei de acesso, contudo, não a proveu de autoridade direta sobre as entidades públicas obrigadas. Ou seja, a CGU – agora dentro do Ministério da Transparência – tem de contar com a boa vontade dos órgãos em cumprir com a lei, estipulando apenas diretrizes a serem seguidas. O mesmo ocorre em relação aos arquivos civis e militares: a CGU não tem autoridade sobre eles, tampouco o Arquivo Nacional e a CONARQ, trazendo incertezas sobre a manutenção e destruição de registros dentro dos arquivos militares brasileiros.

A partir do exposto, percebe-se que há falta de poder de sanção e de arbítrio qualificado no acesso a documentos de segurança nacional. A ausência de uma entidade garantidora da lei de acesso, bem como a ausência de órgão arquivístico da mesma natureza leva à simples crença na boa vontade daqueles que geram, mantém e destroem informações.

No que tange o controle do segredo pelo medo de exposição, a ausência de uma lei que trate do tema do *whistleblowing* é impeditivo para muitas denúncias contra corrupção (OLIVEIRA, 2015). Curiosamente, o único tipo de denúncia regulamentado e ativo é o da delação premiada, que geralmente só acontece quando o denunciante pode tirar vantagens privadas. "Ao contrário do delator, o agente *whistleblower* não está envolvido na organização criminosa. É um terceiro sabedor de informações relevantes, seja por decorrência do exercício direto do seu trabalho, seja por razões eventuais" (OLIVEIRA, 2015, p. 6).

15 Bem diferente dos Estados Unidos, onde há grande judicialização da contestação de respostas consideradas insuficientes ou indevidas (SCHULHOFER, 2010).

16 Sua composição é definida no artigo 46º do decreto 7.724/2012 e suas competências no artigo 47 do mesmo decreto.

CONSIDERAÇÕES FINAIS

Este estudo se propôs a abordar o dilema do segredo de defesa nacional nas democracias e mostrar em linhas gerais qual é a capacidade de segredo das Forças Armadas brasileiras. Na primeira seção discutiu-se como o Estado vem sendo historicamente considerado como o detentor da definição de bem comum. A partir do momento em que este poder é dado ao Estado, ele acaba detendo também o poder de definir o que deve ser escondido da população.

Contudo, a literatura corporativista desafia esta visão de que o Estado deve ser o único ator legítimo na definição do bem comum. De acordo com Stepan (1980), o Estado não é uma junção de opiniões da sociedade, mas sim um ator autônomo que na busca de sobrevivência, poderá também coloca seus próprios interesses na frente daqueles do bem-comum.

O embate entre o direito de informação e o direito de sigilo ainda permanece não resolvido, especialmente quando se aprofunda nos pesos e contrapesos do sigilo. Diversos autores vêm pensando maneiras institucionais de se colocar freios no abuso do sigilo. Entretanto, autores como Sagar (2013) defendem que sempre haverá novas formas de se reter informação e que outros atores estatais são igualmente não confiáveis em relação ao Executivo e às Forças Armadas.

O Brasil não está imune. Apesar de possuir alguns mecanismos de controle, não possui estruturas institucionais com poder de sanção nem relativas à Lei de Acesso à Informação, tampouco à gestão de arquivos militares – incluindo a criação, manutenção e destruição de documentos. Além disto, não possui legislação na temática da denúncia – *whistleblowing* –, o que gera desincentivos para que atores internos levem a público casos de corrupção.

REFERÊNCIAS

ARTICLE 19. The Public's Right to Know: Principles on Freedom of Information legislation. *International Standards Series*, p. 1, 1999.

ARTICLE 19. A Model Freedom of Information Law Article 19, 2006. Disponível em: <http://www.article19.org/resources.php/resource/1796/en/>. Acesso em: 5 abr. 2013.

BENTHAM, J. *The Works of Jeremy Bentham*. Londres: W. Tait, Simkin Marshall and Co., 1843. v. 2.

COLARESI, M. P. *Democracy Declassified*: The Secrecy Dilemma in National Security. EUA: Oxford University Press, 2014.

COLLIER, D. *Trajectory of a Concept:* "Corporatism" in the Study of Latin American Politics. In: SMITH, Peter (Ed.). Latin America in comparative perspective, Londres: Routledge, 1995.

DUCHEIN, M. *Los Obstáculos que se oponen al acceso, a la utilización y a la transferencia de la información conservada en los archivos:* un estudio del RAMP. França: Organizacion de las Naciones Unidas par la Educacion, la Ciencia y la Cultura, 1983.

GAONKAR, D. P.; MCCARTHY, R. J. Panopticism and Publicity: Bentham's Quest for Transparency. *Public Culture*, v. 6, n. 3, p. 547-575, 1994.

GARCÍA, G. Derecho de Acceso a la informacion en Chile: nueva regulación e implicancias para el sector de la Defensa Nacional. *Estudios Constitucionales*, v. 1, n. 7, p. 137-175, 2009.

HOOD, C.; HEALD, D. (Eds.). *Transparency:* the Key to Better Governance? London: Oxford University Press, 2006.

HOTT, D. F. M. *O acesso aos documentos sigilosos: um estudo das comissões permanentes de avaliação e de acesso nos arquivos brasileiros.* Brasília: Faculdade de Ciência da Informação, Universidade de Brasília, 2005.

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS. El Derecho del Acceso a la Información Pública en las Américas: Estándares Interamericanos y comparación de marcos legales. OAS official records, 2012.

KATYAL, N.; CAPLAN, R. The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent. *Stanford Law Review*, v. 60, n. 4, p. 1023-1077, 2008.

KEANE, J. Monitory Democracy? In: MERKEL, Wolfgang; KEANE, John; ALONSO, Sonia. *The Future of Representative Democracy*. Cambridge: Cambridge University Press, 2011.

KLAUS, L. C. O. Transforming Armed Forces Through Military Transparency: Open Government Challenges in a World of Secrecy. *Transforming Government: People, Process and Policy*, v. 10, n. 1, 2016.

LORD, K. M. *The Perils and Promise of Global Transparency*. Nova York: State University of New York Press, 2006.

MAHONEY, J.; THELEN, K. *Explaining Institutional Change*: Ambiguity, Agency, and Power. Nova York: Cambridge University Press, 2010. v. 23.

MARTINS, P. L. Acesso à informação: um direito fundamental e instrumental. *Acervo*, [S.l.], v. 24, n. 1, p. 233-244, 2011.

MENDEL, T. *Freedom of Information:* a Comparative Legal Survey. 2. ed. Paris: Unesco, 2008.

MICHENER, R. G. The Surrender of Secrecy: Explaining the Emergence of Strong Access to Information Laws In Latin America. (Tese de Doutorado) University of Texas, 2010.

MENDEL, T. *Liberdade de informação:* uma síntese dos dilemas de conformidade e suas possíveis soluções. São Paulo: Artigo 19, 2011. (Estudos em Liberdade de Informação)

MENDEL, T. Freedom of Information in Latin America. 2nd National Information Law Conference. Anais… Canberra, Australia: 2012. Disponível em: <http://gregmichener.com/Michener-Talk-Australian-National-University.pdf>. Acesso em: 12 abr. 2017.

MICHENER, R. G.; BERSCH, K. Identifying Transparency. *Information Polity*, v. 18, n. 3, p. 233-242, 2013.

MICHENER, R. G.; VELASCO, R.; FURTADO, K. Avaliação Geral. In: MICHENER, R. G.; MONCAU, L. F. M.; VELASCO, R. (Eds.). *Estado Brasileiro e transparência*: avaliando a aplicação da Lei de Acesso à Informação. Rio de Janeiro: [s.n.: s.d.].

MONCAU, L. F. M; MICHENER, R.G. BARROS, M. G; VELASCO, R. B. *Avaliação de transparência do Ministério Público.* Rio de Janeiro: Fundação Getúlio Vargas, 2015.

NEUMAN, L.; CALLAND, R. Making the Access to Information Law Work: the Challenges of Implementation. In: FLORINI, A. (Ed.). *The Right to Know:* transparency for an open world. Nova York: Columbia University Press, 2007.

OLIVEIRA, J. M. F. *A urgência de uma legislação whistleblower no Brasil.* Textos para discussão nº 175. Brasília: Núcleo de Estudos e Pesquisas da Consultoria Legislativa, 2015.

OPEN SOCIETY JUSTICE INITIATIVE. *Transparency & Silence*: a Survey of Access to Information Laws and Practices in 14 countries. Nova York: OSF, 2006.

OPEN SOCIETY JUSTICE INITIATIVE. *TSHWANE Principles:* Global Principles on National Security and the Right to Information. [S.l: s.n.: s.d.].

PAPANDREA, M. Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment. *BUL Rev.*, v. 94, n. 2, p. 449-544, 2014.

PION-BERLIN, D.; UGUES, A. J.; ESPARZA, D. Self-Advertised Military Missions in Latin America: What is Disclosed and Why? In: KARAKATSANIS, N. M.; SWARTS, J. (Eds.). *Political and Military Sociology*: an annual review. Londres: Transaction Publishers, 2012.

POZEN, D. E. The Mosaic Theory, National Security, and the Freedom of Information Act. *The Yale Law Journal*, v. 38, n. 2, p. 201-232, 2014.

RAMIREZ, M. K. Blowing the Whistle on Whistleblower Protection: a Tale of Reform versus Power. *University of Cincinnati Law Review*, v. 76, p. 183-233, 2007.

REVISTA VEJA. FHC diz que criou sigilo eterno sem querer. Revista Veja, 2011. Disponível em: <http://veja.abril.com.br/noticia/brasil/fhc-diz-que-criou-sigilo-eterno-sem-querer>. Acesso em: 12 abr. 2017.

RODRIGUES, K. F. *Relações civis-militares e as leis de acesso à informação na América Latina e no Brasil*. 2013. Dissertação (Mestrado) – Escola Brasileira de Administração Pública e de Empresas, Fundação Getúlio Vargas, 2013.

ROMANO, J. O. *Política nas políticas: um olhar sobre os estudos na agricultura*. Rio de Janeiro: EDUR/Mauad, 2009.

SAGAR, R. *Secrets and Leaks*: The Dilemma of State Secrecy. Woodstock: Princeton University Press, 2013.

SCHOENFELD, G. *Necessary Secrets*: National Security, the Media, and the Rule of Law. Nova York: W. W. Norton & Company, 2010.

SCHULHOFER, S. J. Secrecy and Democracy: Who Controls Information in the National Security State? Public Law and Legal Theory Research Paper Series. *Working Paper*, n. 15, p. 10-53, 2010.

SERRA, N. *The Military Transition*. Cambridge: Cambridge University Press, 2010.

SIAROFF, A. Corporatism in 24 industrial Democracies: Meaning and Measurement. *European Journal of Political Research*, v. 36, n. 2, p. 175-205, 1999.

STEPAN, A. *Estado, corporativismo e autoritarismo*. Rio de Janeiro: Paz e Terra, 1980.

THOMPSON, D. F. Democratic Secrecy. *Political Science Quarterly*, v. 114, n. 2, p. 181-193, 1999.

SECURITIZAÇÃO E A GOVERNANÇA DA SEGURANÇA CIBERNÉTICA NO BRASIL

LOUISE MARIE HUREL

Conforme novas Tecnologias da Informação e Comunicação (TIC) se tornam mais acessíveis e, portanto, mais presentes em diferentes esferas da sociedade, economia, cultura e política, crescem os interesses de grandes empresas e governos em se tornarem protagonistas na determinação das normas e padrões para a segurança das mesmas (DEIBERT, 2003; DEIBERT, 2014; MUELLER, 2010). Ataques como o da Estônia em 2007, o vírus Stuxnet nas centrífugas iranianas em 2011, e os ataques ao partido democrata estadunidense em plena campanha presidencial em 2016 contribuíram para a centralização da segurança cibernética nas relações entre Estados.

Da mesma forma, crescem os riscos associados à conexão de dispositivos, sensores e infraestruturas em larga escala. Neste cenário, a infecção de códigos maliciosos, o roubo de informações e a exploração de vulnerabilidades em sistemas de informação e comunicação tornam-se atividades corriqueiras. Em especial, contribuem para o reposicionamento da segurança cibernética – enquanto fenômeno social e técnico (BOWKER; STAR, 1999) – na agenda de segurança doméstica e internacional (DUNN CAVELTY, 2012). Este foi o caso do ataque de negação de serviço (DDoS) WannaCry que, em 2017, afetou o funcionamento de computadores tanto na América do Norte quanto na Europa e na América do Sul atingindo, inclusive, o sistema de saúde no Reino Unido (GReAT, 2017). Nas Relações Internacionais, tais dinâmicas se traduziram na expansão horizontal – desafio compartilhado entre setores — e vertical — área de alta prioridade internacional – dos temas de segurança cibernética (DUNN CAVELTY, 2012, p. 104).

No Brasil, o tema ganha destaque com a inserção do espaço cibernético como um dos setores estratégicos para a defesa e segurança nacional. E ganha novas proporções, condições e estruturas dentro de um contexto de sucessivos megaeventos. Grande parte da literatura atual de Relações Internacionais sobre o estado da segurança cibernética no Brasil procurou

traçar um desenvolvimento histórico; compreender processo de institucionalização e securitização do tema dentro do Ministério da Defesa (CEPIK *et al.*, 2014; LOBATO; KENKEL, 2015; SOUZA; ALMEIDA, 2016).

Em contrapartida, o artigo analisa o processo de institucionalização da cibersegurança no contexto do ciclo de megaeventos no Brasil – tal como a Rio+20, Copa das Confederações, Copa do Mundo e Olimpíadas – para expor os limites da teoria de securitização e propor uma nova perspectiva, a da governança da segurança cibernética. O objetivo da articulação do conceito de governança da segurança cibernética surge com a necessidade de se analisar e visualizar práticas que não somente aquelas ligadas a organismos governamentais – atentando para potenciais e presentes práticas, demandas e espaços de colaboração entre setores.

Esta visão põe em cheque o papel do Estado como protagonista na regulação do espaço cibernético e legítimo garantidor da segurança dos usuários. Ao mesmo tempo que este permanece um ator relevante, compartilha de menor grau de assimetria relacional com empresas privadas e indivíduos (*hackers*), no que diz respeito à possibilidade de atuação (NYE, 2010). Estes e outros desafios ressaltam o alto grau de *complexidade* e de *complexificação* que corta transversalmente os debates sobre segurança em uma era conectada. *Complexidade*, neste caso, se refere a diversidade de atores, tecnologias, instituições e práticas; e *complexificação*, por outro lado, remete aos *processos* e mecanismos de governança — normas, princípios, regras e práticas — que caracterizam os diferentes graus de coordenação entre atores na resposta a incidentes cibernéticos

Conforme veremos, a segurança cibernética depende de uma rede de atores e de processos que possuem graus variados de cooperação e coordenação entre si – e envolvem temas como crimes cibernéticos,[1] privacidade,[2] segu-

1 A tipificação de crimes e delitos cibernéticos previstas pela Lei Carolina Dieckmann serve como um exemplo sobre a forma com a qual é possível normatizar uma interpretação de segurança que passa pelo estabelecimento de fronteiras jurídicas referentes aos crime no (ou pelas vias do) ciberespaço.

2 No seu Relatório do Rapporteur Especial da ONU para o Direito à Privacidade na Era Digital direcionado ao Conselho de Direitos Humanos, Joseph Cannataci destaca que um crescente número de Estados insistem em tratar o espaço cibernético como campo pertencente ao tradicional teatro de operações de atividades de inteligência. Tal concepção coloca em risco o usuário, o qual pode ter seus dados pessoais e sua atividade online monitorada em nome da segurança nacional (A/HRC/31/64, 2016. p. 6).

rança nacional, proteção de infraestruturas críticas, respostas a incidentes cibernéticos e estabelecimento de padrões técnicos (MUELLER, 2010).[3]

Esse artigo situa o debate sobre segurança cibernética no Brasil dentro de uma perspectiva mais ampla, colocando os esforços para a consolidação do tema no âmbito do Ministério da Defesa em perspectiva com configurações institucionais diversas e multifacetadas no processo de resposta a incidentes cibernéticos. Governança, nesse sentido, refere-se ao processo de coordenação reflexiva, ou seja, a circunstâncias nas quais atividades rotineiras se tornam problemáticas e/ou precisam ser revisadas (HOFMANN *et al*., 2014).

O artigo se divide em duas partes. A primeira tem por objetivo propor uma reflexão conceitual-teórica sobre segurança cibernética à partir das Relações Internacionais. A seção introduz os principais pontos da teoria da securitização e a sua relação com a crescente literatura sobre cibersegurança das RI. Em seguida, expõe os limites da teoria securitização no que diz respeito ao reconhecimento da participação de outros setores – para além de Estados – em responder a ameaças cibernéticas ao ilustrar a formação internacional de regimes complexos de segurança (HUREL, 2016). O artigo apresenta o conceito da governança da segurança cibernética como alternativa para uma visão estadocêntrica de segurança nacional.

A segunda parte expõe a dimensão prática da relação entre a securitização e governança da segurança cibernética; recorre ao desenvolvimento do sistema de segurança e defesa[4] à partir do ciclo dos megaeventos no Brasil e chama a atenção para a relação de órgãos da Administração Pública Federal (APF) com outros setores na resposta a incidentes. A seção destaca os mecanismos de colaboração e os processos legislativos criados e/ou decorrentes do ciclo de megaeventos de forma a ilustrar a governança da segurança cibernética à nível nacional.

Cabe ressaltar que esse trabalho não tem pretensões de esgotar o debate acerca da governança da cibersegurança, mas sim o de identificar a diversidade de respostas, arranjos institucionais, atores e mecanismos de cooperação que integram os processos que reconfiguram a segurança cibernética enquanto conceito e conjunto de práticas.

---

3 Ao tratar sobre a governança da cibersegurança, DeNardis (2014. p. 86-106) procura explorar a forma com a qual a segurança é articulada por meio de políticas e recomendações não só no âmbito nacional e internacional, mas por dinâmicas e atores que entrecortam uma suposta divisão de níveis – setor privado, CERTs, grupos *antiphishing*.

4 De acordo com a Política Nacional de Defesa de 2012, defesa refere-se "[a]o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas". (BRASIL, 2012)

SEGURANÇA CIBERNÉTICA: UM CONCEITO EM CONSTRUÇÃO

Dentro do campo das Relações Internacionais, a teoria da *securitização* (BUZAN *et al.*, 1998) surge como uma tentativa de: (i) ampliar as fronteiras dos estudos de segurança para além do escopo de segurança nacional e dos estudos estratégicos e militares ao propor uma divisão de cinco setores referentes à segurança: militar, político, econômico, social e ambiental (BUZAN *et al.*, 1998, p. 20-23; BOURNE, 2014, p. 12); (ii) e de compreender como ameaças e riscos se tornam "problemas de segurança". Portanto, o conceito se refere ao processo no qual uma ameaça é demarcada como prioridade[5] (CEPIK *et al.*, 2014); BUZAN *et al.*, 1998), e procura entender como um determinado ator ou grupo de atores visa legitimá-la como alvo de medidas emergenciais e de caráter excepcional – por meio de práticas discursivas (ONUF, 1989; BALZACQ, 2011) e não-discursivas.

A despeito da já antiga integração entre os estudos de segurança e a utilização do ciberespaço para fins político-estratégicos,[6] os atentados de 11 de setembro, e o súbito escalonamento do terrorismo como parte de uma "guerra global", marcam uma mudança na relação sócio-política entre segurança e o espaço cibernético. Cepik, Canabarro e Borne (2014) argumentam que tais atividades "levadas a cabo por redes de computacionais" se transformaram em assuntos de segurança nacional e internacional. Contudo, vale destacar que a securitização[7] do espaço cibernético não se limita ao combate ao terrorismo (CANABARRO *et al.*, 2014; HUREL, 2016a), mas, mais especificamente, à

5 Também chamado de *objeto de referência* ou *objeto ameaçado* – em inglês, *referent object* (Ver: BUZAN *et al.*, 1998).

6 Apesar da afirmação se referir a Arquilla e Ronfeldt (1997 e 2001), tais referências podem ser complementadas por: Dunn Cavelty (2012) para a associação entre o espaço cibernético e processos de militarização; Nye (2010) para o desenvolvimento da noção de "cyberpower"; e Kramer (2009) para a relação entre segurança nacional e poder cibernético.

7 A teoria da securitização foi desenvolvida pela Escola de Copenhague e teve início com Buzan, Waever e Wilde (1998). A partir de uma revisão de literatura sobre a forma com a qual as teorias clássicas de Relações Internacionais retratam o conceito de segurança, os autores propuseram uma análise que levasse em consideração o processo de consolidação de uma ameaça existencial vis à vis uma audiência que pudesse (ou fosse persuadida) a legitimá-la. A partir da urgência, da legitimação da ameaça e da necessidade de tornar algo (objeto de referência) seguro justifica-se portanto a adoção de medidas extraordinárias para que o objeto ameaçado se torne seguro (CEPIK *et al.*, 2014) . Alguns exemplos de securitização, para além do terrorismo, seriam questões concernentes a segurança alimentar, segurança humana ou segurança ambiental – no qual eleva-se o objeto de referencia à prioridade de segurança nacional e existencial.

associação do mesmo como sinônimo da segurança nacional e à sucessivos processos e políticas que tratam – e demarcam – ameaças a partir de lógicas militarizadas (DUNN CAVELTY, 2012; DEIBERT, 2003).

Uma das consequências da securitização do espaço cibernético é o deslocamento das noções de segurança presentes no imaginário da população – usuários – para uma interpretação que à associa a medidas excepcionais em detrimento da proteção da segurança nacional (MAURER, 2017). As revelações do Snowden, e o acesso à informação sobre programas como o PRISM,[8] fornecem uma perspectiva de como práticas de vigilância em massa foram internalizadas dentro da legislação e de processos de monitoramento por parte de agências de inteligência nos Estados Unidos (A/HRC/31/64, 2016) e como, parcerias público-privadas, jogaram para o escanteio a privacidade – e o direito a tal – em nome da segurança nacional (GREENWALD, 2014).

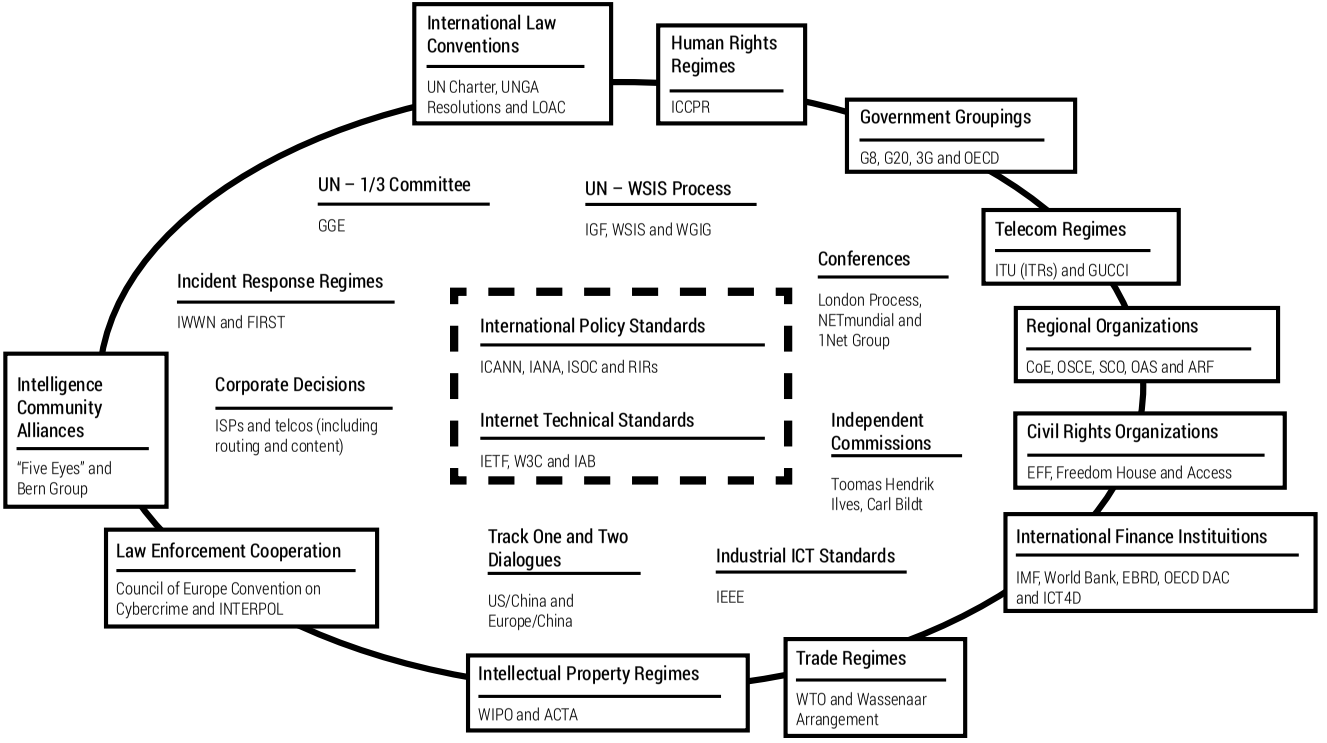
Por mais que a teoria da securitização se enquadre dentro de uma processo de expansão dos estudos de segurança (BOURNE, 2014, p. 12-13), Buzan e Hansen (2009) chegam a conclusão de que, na prática, o Estado e lideranças políticas continuam sendo os principais atores capazes de securitizar – ou seja, determinar o que constitui uma ameaça. A próxima seção apresenta o conceito de governança como uma alternativa que abarca, mas não se limita à associação da segurança cibernética à segurança nacional.

GOVERNANÇA DA SEGURANÇA CIBERNÉTICA: UMA VISÃO GERAL

A principal questão que permeia o debate sobre a governança da segurança cibernética concentra-se no desafio de compreender a complexa relação entre atores, espaços e processos que a lapidam conceitual e tecnicamente (NYE, 2014). Não compete à um só fórum e/ou ator endereçar os desafios distribuídos neste campo – uma vez que este abrange desde o operador de redes até formuladores de política. No entanto, o conjunto desses espaços aponta para a falta de consenso sobre responsabilidades, indefinição sobre competências e mecanismos compartilhados para responder à ataques – ex: DDoS, *phishing*, infiltração de sistemas, ataques em infraestruturas críticas e entre outros (ver: DEIBERT, 2014; DENARDIS, 2014).

8 Programa da Agência Nacional de Segurança (NSA) que permitia a coleta de dados diretamente dos servidores de grandes empresas como Facebook, Yahoo, Apple, Google e Youtube (ver: GREENWALD, 2014. p. 108-112).

Figura 1 – The Regime Complex for Managing Global Cyber Activities



Fonte: NYE, 2014, p. 8.

Conforme proposto na figura acima o arranjo institucional e as interações entre os fatores técnicos, socioeconômicos e políticos da governança da segurança cibernética compõem um complexo ecossistema, também chamado de *regime complex*. Tal visualização contribui para a conceitualização da governança da cibersegurança como um campo, pois apresenta as instituições e arranjos normativos que permeiam a relação entre os diferentes setores. Nye argumenta:

> "Em um espectro de institucionalização formal, um ecossistema complexo é uma figura intermediária, localizada entre um único instrumento legal, de um lado, e arranjos fragmentados no extremo oposto. Apesar de não existir um regime único de governança do ciberespaço, há um conjunto de normas e instituições fracamente acopladas, localizado entre uma instituição integrada, que impõe a regulação por meio de regras hierárquicas, e práticas e instituições altamente fragmentadas, sem nenhum núcleo identificável e com conexões inexistentes." (NYE, 2014, p. 7, tradução minha)[9]

Ao mesmo tempo que Estados engajam na formulação de diretrizes político-institucionais no âmbito nacional, também se fazem presentes em fóruns multilaterais e multissetoriais. Criado em 1998, o United Nations Group of Governmental Experts in the Field of Information and Telecommunications Security (UNGGE) foi dos principais espaços internacionais para o diálogo sobre normas para a segurança cibernética – contou com a presença de 25 países, incluindo o Brasil que assumiu a moderação entre 2014 e 2015. Em 2015, o relatório do GGE reconheceu a aplicabilidade do direito internacional para o uso das tecnologias da informação e comunicação (TICs). Contudo, em 2017 o grupo falhou em atingir consenso. Tal acontecimento abriu espaço para iniciativas advindas do setor privado, público, academia e sociedade civil na promoção de cooperação e confiança internacionalmente.

Paralelamente, arranjos flexíveis, inovadores e representativos da comunidade técnica, academia, e setor privado – por exemplo, Convenção Digital de Genebra e o Cybersecurity Tech Accord[10] – ganham protagonis-

9 No original: "On a spectrum of formal institutionalization, a regime complex is intermediate between a single legal instrument at one end and fragmented arrangements at the other. While there is no single regime for the governance of cyberspace, there is a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages".

10 Conjunto de mais de 40 empresas assinaram o Cybersecurity Tech Accord – o qual prevê princípios basilares para a proteção de usuários e clientes contra incidentes cibernéticos internacionalmente.

mo dentro do ecossistema da segurança cibernética. Conferências como a Global Conference on Cyberspace (GCCS)[11] e o Fórum da Governança da Internet (IGF) também contribuem para a construção de diálogos entre partes à nível global, e possuem estruturas de coordenação menos rígidas e restritas. A GCCS, apresenta uma organização institucional que conta com a predominância de empresas privadas e governos – apesar de ser comumente criticada pela difícil integração de grupos da sociedade civil (HUREL, 2016). Também destaca-se o papel do Fórum Internacional da Governança da Internet (IGF) que reúne representantes de diferentes setores e promove um debate mais amplo sobre boas práticas e desafios da segurança cibernética por meio de iniciativas como o o Best Practice Forum (BPF) sobre cibersegurança, Grupos de Resposta a Incidentes de Segurança (CSIRTs) e *spam* (ver: IGF, 2017).

Ao fomentar progressivos esforços para a conciliação entre as dimensões operacional, técnica e política da segurança em contextos de crescente digitalização e aplicação de novas tecnologias – tal como IoT, algoritmos e inteligência artificial –, tais iniciativas visam atender a um espectro de sectores. Um exemplo é a Global Commission on the Security and Stability of Cyberspace (GCSSC). Lançada no início de 2017, a Comissão conta com um comissariado de especialistas de diversos países e tem por objetivo conectar diálogos internacionais com comunidades e setores, bem como promover conscientização de riscos compartilhados entre as diferentes partes. Esta atua por meio da organização de seminários com pesquisadores e especialistas, da participação dos comissários em eventos internacionais e interação com usuários em listas de e-mails. Tais esforços resultaram em propostas de princípios gerais –tal como a proteção do núcleo público da Internet contra ataques cibernéticos – para a segurança e estabilidade de atividades na e por meio de redes (GLOBAL, 2017).

No entanto, grande parte da governança da segurança cibernética é regida por atores privados e arranjos público-privados (DENARDIS, 2014; HUREL e LOBATO, 2018; WOLFF, 2015). Empresas como Kaspersky Lab, Symantec, CrowdStrike e entre outras, trabalham na identificação

11 A GCCS, também conhecida como London Process surge em 2011 como uma tentativa de criar uma ampla plataforma de discussão capaz de abordar os desafios e oportunidades para o ciberespaço. A conferência bi-anual também lançou o Global Forum on Cyber Expertise em 2015 visando atender a necessidade de promover debates mais propositivos e inclusivos sobre políticas para o espaço cibernético. Apesar da sua gradual abertura a participantes de grupos da sociedade civil e academia, o forum e o GFCE carregam críticas sobre a efetiva inclusão e participação desse *pool* mais diverso (HUREL, 2016).

de incidentes e fornecimento de serviços – *software*, assistência técnica, relatórios – relacionados à segurança de sistemas e redes. No que diz respeito ao estreitamento das relações público-privadas, em 2016, o governo brasileiro firmou parceria com a Microsoft para o estabelecimento de um Centro de Transparência com o intuito de servir o país e a região da América Latina com o "acesso a importantes informações relacionadas à segurança cibernética de programas da Microsoft com foco em inteligência, proteção contra malwares (ameaças online) e segurança para combater os crimes cibernéticos" (MICROSOFT, 2016).

A crescente sofisticação e desenvolvimento de ataques cibernéticos e o concomitante interesse de governos em responder incidentes com contra-ataques – também denominado direito à *hack-back* – contribuiu para o reposicionamento do grandes empresas no diálogo internacional sobre normas. Em fevereiro de 2017, o CEO da Microsoft, Brad Smith subiu no palco da conferência anual da RSA[12] para propor o estabelecimento de uma Convenção de Genebra para o ciberespaço. Seu principal argumento era que faziam-se necessárias novas soluções para desafios relacionados à segurança cibernética, sendo o maior deles a garantia dos direitos dos usuários e de maior previsibilidade sobre o comportamento dos Estados no espaço cibernético. A proposta não só aponta para o desafio, à nível internacional, de pensar sobre a construção de garantias, normas e práticas relacionadas à segurança cibernética, mas retrata a constante tensão entre o papel desempenhado pelo Estado vis à vis atores privados e grupos da sociedade civil na governança da segurança cibernética. O que nos remete à questão de o que significa "produzir segurança" e quais atores estão – e devem estar – envolvidos nesse processo. O afunilamento da noção de cibersegurança associada à segurança nacional também representa, neste caso, a redução do número de atores legítimos dentro desse regime global (HUREL, 2016).

A segunda parte do artigo detalha o processo de desenvolvimento de mecanismos, organismos e políticas dentro do Brasil; também busca retratar a tensão normativa e regulatória que surge a partir da estruturação da segurança cibernética como algo que, uma vez securitizado, torna-se, *a priori*, ator, neste caso, o Estado. Por outro lado, a consolidação de um regime

12 A RSA é uma das principais conferências internacionais sobre temas relacionados a segurança da informação e acontece quatro vezes ao ano – Estados Unidos, Europa, Ásia e Emirados Árabes Unidos. Em 2017, a primeira conferência aconteceu entre os dias 13 e 17 de fevereiro em San Francisco.

SEGURANÇA CIBERNÉTICA E OS MEGAEVENTOS NO BRASIL

O histórico da segurança cibernética pode ser observado, dentro do contexto brasileiro, como um processo que inicialmente se estrutura a partir de políticas e organismos na área da segurança da informação na esfera da Administração Pública Federal (APF). Em 2000, sob os auspícios do Conselho de Defesa Nacional, instituiu-se a Política de Segurança de Informação e o Comitê Gestor da Segurança da Informação[13] como o intuito de estabelecer diretrizes, princípios e objetivos para o desenvolvimento de normas, tecnologia nacional e capacitação de entidades da APF (BRASIL, 2000). Com o passar dos anos, o aparato institucional relacionado a segurança de redes, segurança da informação e segurança cibernética continuou a se desenvolver principalmente em áreas ligadas ao (i) sistema de inteligência brasileiro – com o Gabinete de Segurança Institucional da Presidência da República (GSI-PR), a Agência Brasileira de Inteligência (ABIN) e o Departamento de Segurança da Informação e Comunicações (DSIC) – e (ii) a governança da Internet no Brasil (SOUZA; ALMEIDA, 2016, p. 391-394) – com o Comitê Gestor da Internet (CGI.br) em 1995, o CERT.br[14] em 1997 e o Núcleo de Coordenação do ponto BR em 2005.

No entanto, no âmbito do Ministério da Defesa, o reconhecimento do espaço cibernético como um dos três setores estratégicos – ao lado do setor nuclear e espacial – para a defesa e segurança nacional na Estratégia Nacional de Defesa em 2008 (ESCRITÓRIO, 2016) marca o início do processo de consolidação do setor cibernético não mais como um sub-tema fragmentado em diferentes agências governamentais, mas como parte da

13 O documento define segurança da informação como a "proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento" (BRASIL, 2000).

14 O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é o organismo encarregado de "receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet brasileira" e se enquadra dentro da estrutura do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) do Comitê Gestor da Internet no Brasil (CGI.br). Dentre as suas principais atividades estão: (i) o tratamento de incidentes; (ii) o treinamento de outros grupos de resposta a incidentes e conscientização de diversos sectores – o que inclui a promoção de boas práticas de segurança por meio de materiais ou palestras; e (iii) a análise de tendências de ataques.

formação de um complexo regime de segurança e defesa nacional cibernéticas.[15] A Estratégia integra um processo político-estratégico específico de estruturação do desenvolvimento tecnológico nacional para fins militares e cooperação entre as Forças Armadas.[16]

MEGAEVENTOS: PROPULSORES PARA A GOVERNANÇA DA SEGURANÇA CIBERNÉTICA?

Grande parte da institucionalização da segurança cibernética no Brasil se dá em meio ao ciclo de megaeventos – iniciados pouco antes de 2012 com a Rio+20 – e em resposta aos escândalos de espionagem de 2013. Em 2010, as portarias 666 e 667 colocaram em funcionamento o Núcleo de Defesa Cibernética (Nu CDCiber) no âmbito do Exército e, em 2012, o Centro de Defesa Cibernética (CDCiber)[17]. Desde então, foi atribuído ao CDCiber a responsabilidade pela coordenação e integração das atividades de defesa cibernética no âmbito do Ministério da Defesa.[18] Na revisão da END realizada em 2012, ficou acordado o detalhamento das prioridades do desenvolvimento do setor cibernético. Dentre elas, destacou-se o fortalecimento do CDCiber com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas (ComDCiber) (BRASIL, 2012).

15 Souza e Almeida (2016) dividem o surgimento de políticas e instituições voltadas para segurança cibernética no Brasil de acordo com as três categorias desenvolvidas por Buzan *et al*. (1998) para lidar com a relação entre questões públicas e segurança: não-politizada, politizada e securitizada. A divisão se dá da seguinte forma: "até o ano 2000, não politizado; a partir de então, politizado, [tendo como marco inicial o lançamento do Livro Verde da Sociedade da Informação e a Política de Segurança da Informação em 2000]; e em 2008, se inicia um processo de securitização". Ver Souza e Almeida (2016, p. 386-392) para uma descrição detalhada das políticas que sustentam a demarcação de cada período.

16 Vale ressaltar também que, de forma a dar prosseguimento a implementação das diretrizes estabelecidas pela END de 2008, o Exército Brasileiro instituiu o setor cibernético no âmbito das Forças Terrestres (ESCRITÓRIO, 2016) – integrando o cenário de projetos associados aos setores estratégicos dentro das Forças Armadas do Brasil (Exército com o cibernético, Aeronáutica com o projeto espacial e a Marinha com o projeto do submarino nuclear).

17 "Cabe lembrar que a END, adotada pelo Brasil em 2008, atribuiu ao Exército o papel de integrar e coordenar as Forças Armadas do país no que diz respeito às atividades de defesa relativas ao setor cibernético." (CANABARRO *et al*., 2014. p. 171). Ver Brasil, 2008.

18 Ver: Portaria nº. 3.028 de 14 de novembro 2012.

Em 2011, inciou-se um ciclo de iniciativas que fomentaram novos canais para a cooperação entre diferentes agências e setores na área de segurança pública e cibernética. Este foi o caso da criação Secretaria Extraordinária de Grandes Eventos, no mesmo ano, com o objetivo de promover a integração entre órgãos federais, estaduais nessas áreas frente aos megaeventos (MENDES, 2011). No ano seguinte, a portaria No. 2.221 de 20 de agosto de 2012 estabeleceu orientações para a atuação do Ministério da Defesa nas atividades dos Grandes Eventos, dentre estas o emprego temporário das forças armadas na *segurança e defesa cibernética* para proteção das cidades-sede (GABINETE, 2012). No entanto, antes que o CDCiber começasse a operar oficialmente em 2012, o grupo hacker LulzSec Brasil tirou do ar o *site* da Presidência da República, do governo brasileiro e da Petrobrás. O incidente contou com a resposta do Serviço Federal de Processamento de Dados (SERPRO) no processo de mitigação e restabelecimento da rede (AMOROSO, 2011).

Estes eventos elucidam, em parte, o processo de institucionalização da segurança cibernética associado a contextos permeados por preocupações com de ameaças à segurança nacional e pública – por exemplo, o terrorismo, ciberterrorismo e ataques à infraestruturas críticas. A Rio+20 se destaca como o primeiro evento no qual uma estrutura de defesa cibernética nacional foi concebida para lidar com a segurança das redes (Nu CDCiber) (CAMPUS, 2013). Entretanto, a Jornada Mundial da Juventude (2013), Copa das Confederações (2013), Copa do Mundo (2014),[19] as Olimpíadas e Paralimpíadas (2016) também fazem parte do processo de desenvolvimento do Sistema Militar de Defesa Cibernética (ver: CAMPUS, 2013; SOUZA; ALMEIDA, 2016).

No entanto, redes de colaboração forjadas para responder à incidentes cibernéticos transcendem o escopo restrito das Forças Armadas. Durante a conferência Rio+20, o grupo Anonymous atacou e comprometeu 26 *sites* em protesto ao evento. Respostas ao ataque #OPHackInRio foram realizadas pelo Centro de Monitoramento Cibernético, o qual integrava o CDCiber, Forças Armadas, Polícia Federal (ROHR, 2012) e parceiros como o CERT.br e o CTIR.gov – os quais eram responsáveis pela divulgação de notificações e alertas a outros órgãos públicos e privados (BRAUN, 2012).

19 De acordo com o então chefe do CDCiber, general Paulo Sergio Melo de Carvalho, para além da proteção das infraestruturas críticas, o Centro também se dedica "[a] o fortalecimento da segurança, a produção de respostas a incidentes de redes, a incorporação de lições aprendidas e a proteção contra ataques cibernéticos, além da atualização doutrinária" (DEFESA, 2014).

No entanto, a rápida estruturação de instituições dentro do Ministério da Defesa (por exemplo, GSI e Forças Armadas) traz profundas tensões para uma visão que destaque uma distribuição de competências para órgãos associados à segurança em sua dimensão política e operacional. Ao mesmo tempo que os megaeventos estimularam a formação de redes de coordenação entre instituições, a Comissão Parlamentar de Inquérito (CPI) da Espionagem avaliava o processo de consolidação da estrutura político-estratégica para a segurança cibernética atrelada a segurança nacional no país.[20] Tendo sido designada para "investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos" a Comissão recomendou a elaboração de uma Estratégia Nacional de Segurança Cibernética para "melhorar segurança e resiliência da infraestrutura dos serviços nacionais", o delineamento das "principais medidas de segurança cibernética para o Estado brasileiro" por meio de "ações coordenadas entre os setores público e privado" (RELATÓRIO, 2014, p. 141-142). Em resposta, o Departamento de Segurança da Informação e Comunicações (DSIC) lançou a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018".

Conforme apontado, a consolidação da segurança e defesa cibernética no âmbito nacional é marcada por sucessivas políticas[21] que surgem com o intuito de guiar atividades dentro da APF e das Forças Armadas, mais especificamente.[22] Tais desenvolvimentos se respaldam em duas demandas; externamente, visa atender às ameaças e riscos decorrentes e esperados no contexto dos grandes eventos sediados no país; internamente, busca desenvolver capacidades e instituições com competências para responder politicamente e tecnicamente a ameaças.

---

20 A *Nota Técnica da Sociedade Civil para CPI de Crimes Cibernéticos* desenvolvida pela Coding Rights e IBIDEM aprofunda a análise das contribuições e desafios para o desenvolvimento da segurança cibernética no Brasil. Para mais detalhes, ver: CPI DE CRIMES CIBERNÉTICOS. Sumário Executivo. Disponível em: <https://cpiciber.codingrights.org/sumario-executivo/>. Acesso em: 19 dez. 2018.

21 E que ganham tração na agenda nacional, em grande medida, no período do Ministro da Defesa Celso Amorim (DEFESA, 2014).

22 O desenvolvimento institucional do CDCiber integra um processo mais amplo no qual políticas e diretrizes alimentam tentativas de promover robustez, interoperabilidade e cooperação dentro do Ministério da Defesa. Sendo assim, cabe notar a Política Cibernética de Defesa (2012), a Doutrina Militar de Defesa Cibernética (2014) e da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (2015) como indicadores importantes do da formalização da política nacional para a segurança cibernética.

Reflexões sobre a securitização da segurança cibernética no Brasil, dentro do arcabouço teórico, permanecem extremamente relevantes para a ilustração do íntimo relacionamento entre contexto, processos, construções de ameaças e formulação de respostas. Ao mesmo tempo que segurança cibernética ganha notoriedade dentro da agenda nacional, as respostas se concentram, em grande medida, no papel e estruturas do Ministério da Defesa, Exército e Forças Armadas – mais especificamente, por meio da consolidação do Sistema Militar de Defesa Cibernética.[23]

O exercício proposto por esse artigo é o de compreender que, a despeito da assimetria de competências e capacidades de atuação por parte das entidades supracitadas, assegurar a estabilidade, segurança e resiliência de sistemas e computadores *não se restringe a um modelo específico, mas se revela no encontro de organismos com diferentes* modus operandis –, especialmente no contexto dos megaeventos.

Este é o caso dos Grupos de Resposta a Incidentes. Em contraste ao modelo hierarquizado do CDCiber, os CSIRTs geralmente operam por meio de sistemas colaborativos, dependendo de redes de confiança entre os especialistas que integram as equipes (SCHMIDT, 2012).[24] Enquanto o CERT.br atua como ponto central para as notificações de incidentes de segurança no Brasil, os CSIRTs possuem composições bastante diversas – vão desde grupos "ad hoc" voltados para o âmbito local (ex: universidades) até grupos regionais, nacional e/ou de caráter privado[25] – um exemplo é o Centro de Tratamento de Incidentes de Segurança e Redes de Computadores da Administração Pública Federal (CTIR Gov).[26] Além da diversidade do caráter institucional, o processo de resposta a incidentes

23 "[O] Sistema Militar de Defesa Cibernética do País, […] atua em cinco áreas de competência: Doutrina, Operações, Inteligência, Ciência e Tecnologia e Capacitação de Recursos Humanos. Sua finalidade é proteger e explorar o Setor Cibernético" (EXÉRCITO, 2015).

24 Mueller (2010) também aponta que esse modelo de produção de segurança em redes colaborativas menos hierarquizadas inclui, mas não está limitada a, provedores de acesso à Internet, *registrars*, organizações antiphishing, fóruns de discussão

25 Ver: CERT. CSIRT FAQ. Disponível em: <https://www.cert.br/certcc/csirts/csirt_faq-br.html>. Acesso em: 19 dez. 2018.

26 Ver: CTIR. Sobre o CTIR Gov. Disponível em:<http://www.ctir.gov.br/sobre-CTIR-gov.html>. Acesso em: 19 dez. 2018.

faz parte de redes de colaboração[27] entre CSIRTs e o CERT.br na troca de informações, coordenação ou notificação.

A estruturação do CERT.br é resultado de um processo de consolidação de um modelo para a segurança das redes no Brasil que foi gerado a partir da preocupação com os riscos que poderiam surgir com a abertura e expansão da Internet comercial (ARQUIVO, 2002; NIC, 1996). A produção colaborativa – também chamada de *peer production of security* –, é caracterizada pelo (i) compartilhamento de informações de maneira não-proprietária – permitindo a reutilização dos dados para fins não-comerciais; (ii) estabelecimento de mecanismos de cooperação não deterministicamente baseados em relações hierárquicas; (iii) operacionalizados, preferencialmente, de forma descentralizada (SCHMIDT, 2012).

Os megaeventos contaram com resposta coordenada entre CERTs, CSIRTs e outros órgãos envolvidos na segurança cibernética durante os eventos. Inclusive, foi criado o Rio 2016 CSIRT com o objetivo de atender a segurança das Olimpíadas e promover maior cooperação na identificação de ataques – e operou como parte da relação entre CDCiber, Centro de Coordenação de Segurança e Defesa Cibernética (CCSDCIBER),[28] CTIR Gov o CERT.br e entre outros (CERT, 2016).

A relação entre CSIRTs caracteriza a coexistência de um modelo de cooperação alternativo à securitização concentrada no papel do Estado. De acordo com o CERT.br, a segurança cibernética dos megaeventos não é possível se realizada por um só grupo ou setor; necessitando, portanto, de canais fomentem comunicação e compartilhamento de informações entre os organizadores, técnicos de operadoras e outros CSIRTs (HOEPERS, 2014). Em 2014, ano da Copa do Mundo no Brasil, o número de incidentes foi

27 "O relacionamento entre diversos CSIRTs e organizações de segurança pode facilitar o compartilhamento de estratégias de resposta e a geração de alertas para potenciais problemas. Os CSIRTs podem trabalhar em conjunto com outras áreas da organização de maneira pró-ativa, garantindo que novos sistemas sejam desenvolvidos e colocados em produção tendo preocupação com a segurança e em conformidade com as políticas de segurança do site. Eles podem ajudar a identificar áreas vulneráveis da organização e, em alguns casos, realizar análise de vulnerabilidades e detecção de incidentes". Cf.: CERT. CSIRT FAQ. Disponível em: <https://www.cert.br/certcc/csirts/csirt_faq-br.html>. Acesso em: 19 dez. 2018.

28 Dentro desse contexto, o CCSDCIBER realizou a "coordenação da resposta e o tratamento dos Incidentes de Segurança Cibernéticos que representam violações de segurança nas redes de interesse" do Ministério da Defesa (COMDCIBER, 2016).

excepcionalmente mais alto se comparado com os anos anteriores – totalizando em mais de um milhão reportados.[29]

As mudanças decorrentes do encontro entre regimes e estruturas, tais como os CSIRTs e o Sistema Militar de Defesa Cibernética, fazem parte de um processo de *coordenação reflexiva.* Conceitualmente, a coordenação reflexiva integra a noção de governança da segurança cibernética ao referir-se a momentos críticos nos quais rotinas e práticas de resposta a incidentes se tornam insuficientes e/ou problemáticas, necessitando, portanto, de revisão (ver: HOFMANN *et. al*, 2014). Este foi o caso do ciclo de megaeventos desencadeados desde a Rio+20. Não só proporcionaram um contexto favorável para o fortalecimento do setor militar, mas mobilizaram atores que transcendem o escopo de atuação desse grupo, gerando novas formas de colaboração frente à ameaças cibernéticas e nacionais. Esse contexto teve um papel importante na redefinição de práticas de resposta a incidentes cibernéticos — tanto *intra-organizacionais* quanto *inter-organizacionais*. Atentar para a *coordenação reflexiva* que sustenta a cooperação na resposta a incidentes e a governança da segurança cibernética nos permite (i) identificar processos de coordenação no contexto dos megaeventos e (ii) questionar a suficiência dos mecanismos e possibilidades de cooperação existentes. Dentro dessa perspectiva, a governança da segurança cibernética deve ser compreendida enquanto um processo, (GIDDENS, 1984) indissociável do espectro de atores que contribuem para a ressignificação das práticas, instituições e tecnologias que a compõem (CASTELLS, 2009)

Contudo, a despeito da cooperação operacional a governança da segurança cibernética no Brasil é claramente marcada por tensões advindas do restrito processo de institucionalização. Conforme apontado pela Nota Técnica da Sociedade Civil para a CPI de Crimes Cibernéticos (NOTA, 2016):

> [A] estratégia nacional ou pactos multilaterais internacionais sobre o tema devem priorizar processos de deliberação de que participem tanto governos quanto empresas, sociedade civil, academia e outros segmentos sociais. Caso contrário, o debate é focado apenas em crime e terrorismo cibernéticos, por uma perspectiva precipitada e estritamente penal e militar da discussão de segurança pública, em detrimento de outros direitos.

Tanto o *Livro verde: segurança cibernética*, publicado em 2010 e a *Estratégia de segurança da informação e comunicações* de 2015 apontam para a interdependência entre governo, setor privado, academia e sociedade civil, respectivamente:

29 Ver a tabela de incidentes reportados ao CERT.br por ano. Cf.: CERT. Estatísticas dos Incidentes Reportados ao CERT.br Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 19 dez. 2018.

> Os desafios da segurança cibernética são muitos, e portanto, é fundamental desenvolver um conjunto de ações colaborativas entre governo, setor privado, academia, terceiro setor, e sociedade, para lidar com o mosaico de aspectos que perpassam a segurança cibernética.
> […] Ficam, assim, evidenciados os vários desafios enfrentados pelo Governo Federal, em especial a carência do estabelecimento de governança efetiva da SIC e da SegCiber, e da segurança dos ativos de informação críticos, e a ausência de um órgão central que exerça coordenação executiva de tais temas, de forma sistêmica e participativa – "multistakeholders" e multissetores, somada a ausência de destaque orçamentário específico e adequado ao tamanho do problema (GABINETE, 2015, p. 14-17).

Na prática esta interdependência provou-se mais desafiadora, recebendo constantes críticas de organizações da sociedade civil e academia. Estes expressaram preocupações com um modelo de política concentrado no papel do Gabinete de Segurança Institucional – e operacionalmente no DSIC e Forças Armadas – e pressionaram por uma abordagem multissetorial no *processo* de elaboração politicas para segurança cibernética e segurança da informação e comunicações (ARTIGO 19, 2016).

Tais desdobramentos revelam que a governança da segurança cibernética é caracterizada pela coexistência de regimes complexos e uma tensão entre a securitização e modelos menos hierarquizados de respostas a ameaças. A combinação entre o caráter nebuloso das medidas levadas a cabo para a garantia da segurança cibernética durante o ciclo de megaeventos, a sua influência na formação do Sistema Militar de Defesa Cibernética e a célere consolidação do setor cibernético dentro do Ministério da Defesa retrata, em grande medida, um contínuo processo de securitização do espaço cibernético como ativo da segurança nacional.

Por outro lado, torna-se cada vez mais latente a demanda por uma reflexão sobre a participação de empresas, academia e sociedade civil nos presentes e futuros desdobramentos da segurança cibernética no Brasil. A clivagem entre a sociedade civil e GSI traz desafios estruturais para o desenvolvimento de políticas e para o progresso de uma governança multiparticipativa no país. Observa-se, também, que operacionalmente a estrutura militarizada do CDCiber depende de parceiros externos como o CERT.br, empresas privadas e outros organismos da APF.

Por fim, o contexto do ciclo dos megaeventos e as revelações do Snowden tiveram profundos impactos sobre a complexificação da governança da segurança cibernética no Brasil – a qual é marcada por dois momentos: (i) a institucionalização da segurança cibernética dentro da Administração Pública Federal e do Ministério da Defesa; e a (ii) CPI da espionagem e de crimes cibernéticos como espaço para vocalização de grupos da sociedade civil sobre a consolidação de um regime nacional centrado no Estado.

Diante da incapacidade de definir espaços – fóruns e contextos – específicos para a segurança cibernética,[30] uma perspectiva de governança propõe a visualização mais ampla de regimes complexos compostos caracterizados por sucessivos processos de *coordenação reflexiva*.

CONCLUSÃO

Apesar do difícil acesso à informação sobre os atores envolvidos na promoção da segurança cibernética durante os diferentes megaeventos – que é um dos desafios presentes para o aprofundamento dos debates sobre governança da cibersegurança –, o papel de estruturas menos hierarquizadas como o CERT.br no processo de capacitação e colaboração torna-se mais evidente à partir da Rio+20.

Em temos gerais, a governança da segurança cibernética passa, não só pela compreensão dos processos de institucionalização da defesa e segurança cibernética no âmbito do Ministério da Defesa, Forças Armadas e Exército Brasileiro, mas também pelo mapeamento do papel do empresas de TIC, a Polícia Federal, ABIN (SOUZA; ALMEIDA, 2016), o Serviço Federal de Processamento de Dados (SERPRO), NIC.br,[31] CERTs, CSIRTs e entre outros.

Enquanto a securitização nos permite visualizar as tentativas do Estado em se tornar o principal interlocutor, identificador e legítimo ator em responder às ameaças cibernéticas, o esforço de assim faze-lo se dá, também, por meio da cooperação e coordenação com outros atores dentro da APF, grupos técnicos, empresas privadas e entre outros.

Por mais que a securitização nos proporcione um diagnóstico do estado da segurança cibernética no Brasil – institucionalização concentrada no Estado – o artigo dá um passo inicial em propor uma mudança teórico-conceitual atente para a *governança* como paradigma norteador para a discussão sobre segurança cibernética. A securitização reforça as estruturas vigentes e deixa pouco espaço para a análise de mecanismos de governança que não aqueles que partem do Estado. A governança da segurança cibernética, coloca em perspectiva papel do CDCiber dentro do complexo ecossistema

30 DeNardis (2014, p. 86-106) foi uma das primeiras a se referir ao termo *cybersecurity* governance, no entanto, ao longo do desenvolvimento o termo torna-se comumente intercambiável, e até menos usado que *network security*. Mueller (2010, p. 159-184) adota *security governance on the Internet*; Deibert (2014. p. 65) *cyberspace governance*; Raymond (2014, p. 23) *governance of cyber security*.

31 O gerenciamento da porta lógica 25 como um exemplo de mitigação de incidentes que marcou o combate ao *spam* no Brasil.

nacional de segurança. Essa abordagem também nos permite identificar a co-dependência do Estado em corpos como o CERTs em levar à cabo operações de resposta a ameaças cibernéticas.

Sendo assim, a consolidação de um regime nacional de segurança cibernética não resulta em uma completa invalidação de processos securitizantes por parte do Ministério da Defesa. Traz nuances para o debate acadêmico sobre segurança cibernética no Brasil ao colocar o papel de estruturas governamentais vis à vis mecanismos de colaboração publico-privados que não necessariamente operam em estruturas hierarquizadas.

Regimes complexos internacionais e nacionais são marcados pela ausência de confiança e a indefinição de competências. Internacionalmente, novas iniciativas multissectoriais buscam endereçar tais desafios; nacionalmente, o país é desafiado a desenvolver capacidades para atender ao crescente número de incidentes.

A segurança de tecnologias emergentes, infraestruturas conectadas e de cidadãos é transversal e abarca desde crimes até direitos humanos – privacidade, acesso à informação. Assim sendo, o artigo aponta para uma crescente demanda por modelos de governança multissectoriais para a segurança cibernética à nível nacional e internacional. Contudo, a possibilidade, emprego e eficácia ainda há de ser avaliada – por exemplo, CPI Crimes cibernéticos.

O debate – em especial nas Relações Internacionais – sobre *securitização* do ciberespaço surge, não só como uma tentativa de compreender a expansão de interesses estatais, mas como uma forma de analisar o papel da cibersegurança como o *objeto de segurança* nacional e o Estado como o *ator legítimo para lidar com o objeto*. Contudo, conceitualizações sobre a relação entre segurança cibernética e o Estado abordam extensivamente questões ligadas a riscos, cibercrime e ameaças, provando-se insuficientes para compreender a relação entre os diferentes grupos de atores envolvidos na governança da cibersegurança. Por isso, esse artigo defende o argumento de que, desenvolvimentos institucionais na área da segurança cibernética devem ser acompanhados de um debate conceitual capaz de identificar a diversidade de atores, processos e contextos neste campo – ao mesmo tempo que não negligenciando assimetrias de poder entre setores.

Desta forma, este artigo é um ensaio inicial que visa contribuir para a tarefa de mapear atores/organismos nacionais e explorar as diferentes relações, processos e atores envolvidos na governança da segurança cibernética. Esse exercício faz parte de um esforço contínuo de compreender a relação entre desenvolvimento tecnológico e desenvolvimentos de mecanismos de governança no Brasil.

REFERÊNCIAS

ABIN. Agência Brasileira de Inteligência: Gabinete de Segurança Institucional. Disponível em: <http://www.abin.gov.br/atuacao/produtos/tecnologia/>. Acesso em: 21 ago. 2017.

AMOROSO, D. Grupo LulzSec tem braço brasileiro e já derrubou páginas governamentais. TecMundo. 2011. Disponível em: <https://www.tecmundo.com.br/seguranca/10947-grupo-lulzsec-tem-braco-brasileiro-e-ja-derrubou-paginas-governamentais.htm >. Acesso em: 21 ago. 2017.

ARQUIVO. NBSO: Monitoração dos incidentes de segurança da Internet no Brasil. NIC.br. 2002. Disponível em: <http://www.nic.br/noticia/na-midia/nbso-monitoracao-dos-incidentes-de-seguranca-de-internet-no-brasil/>. Acesso em: 21 ago. 2017.

BALZACQ, T. *Securitization Theory:* How Security Problems Emerge and Dissolve. Nova York: Routledge, 2011.

BOURNE, M. *Understanding Security*. Londres: Palgrave Macmillan, 2014.

BOWKER, G. C. & STAR SL. Sorting Things Out: Classification and Its Consequences. MA: MIT Press. 1999. 389p.

BRASIL. Política Nacional de Defesa e Estratégia Nacional de Defesa. Ministério da Defesa. Brasília, 2012. Disponível em: <http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 21 ago. 2017.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Presidência da República, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em: 21 ago. 2017.

BRASIL. *Estratégia Nacional de Defesa*. Brasília: Ministério da Defesa, 2008.

BRAUN, D. Exército Prepara Defesa Cibernética da Copa das Confederações. NIC.br. 2012. Disponível em: <http://nic.br/noticia/na-midia/exercito-prepara-defesa-cibernetica-da-copa-das-confederacoes/>. Acesso em: 21 ago. 2017.

BUZAN, B.; HANSEN, L. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press, 2009. 239p.

BUZAN, B.; HANSEN, L.; WAEVER, O.; DE WILDE, J. *Security:* a New Framework for Analysis. Boulder: Lynne Rienner, 1998. p. 1-47.

CAMPUS. CPBR6: Defesa Cibernética em Grandes Eventos. Campus Party. 2013. Disponível em: <https://www.youtube.com/watch?v=WMLFU3F794s>. Acesso em: 21 ago. 2017

CANABARRO, D. R.; CEPIK, M.; BORNE, T. Governança global da internet: tecnologia, poder e desenvolvimento. v. 1 e 2. UFRGS. Porto Alegre, 2014. Disponível em: <https://www.academia.edu/10513610/Governan%C3%A7a_global_da_Internet_Tecnologia_Poder_e_Desenvolvimento_Volume_1_>; e <http://www.

lume.ufrgs.br/bitstream/handle/10183/114399/000953300-02.pdf?sequence=2>. Acesso em: 21 ago. 2017.

CANNATACI, Joseph A. Report of the Special Rapporteur on the Right to Privacy. A/HRC/31/64. Human Rights Council. United Nations. 2016. Disponível em: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/A-HRC-31-64.pdf>. Acesso em: 21 ago. 2017.

CASTELLS, M. Communication Power. Oxford: Oxford University Press. 2009. 592p.

CEPIK, M.; CANABARRO, D. R.; BORNE, T. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: SOUZA, André de M.; Nasser, Reginaldo M.; Moraes, Rodrigo F. (Eds.) *Do 11 de setembro de 2001 à guerra ao terror:* reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014. p.161-186.

CERT. CSIRT FAQ. Disponível em: <https://www.cert.br/certcc/csirts/csirt_faq-br.html>. Acesso em: 19 dez. 2018.

CERT. Estatísticas dos Incidentes Reportados ao CERT.br Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 19 dez. 2018.

COMDCIBER. Processos de tratamento de incidentes empregados pelo CDCiber nos jogos olímpicos e paralímpicos Rio 2016. Fórum CSIRTs 2016, 2016. Disponível em: <https://www.cert.br/forum2016/slides/ForumCSIRTs2016-CDCiber-Processos-Rio2016.pdf>. Acesso em: 21 ago. 2017.

CPI DE CRIMES CIBERNÉTICOS. Sumário Executivo. Disponível em: <https://cpiciber.codingrights.org/sumario-executivo/>. Acesso em: 19 dez. 2018.

CTIR. Sobre o CTIR Gov. Disponível em:<http://www.ctir.gov.br/sobre-CTIR-gov.html>. Acesso em: 19 dez. 2018.

DEFESA. Ministro acompanha trabalho de defesa cibernética na Copa do Mundo. Ministério da Defesa, 2014. Disponível em: <http://www.defesa.gov.br/index.php/noticias/13141-ministro-acompanha-trabalho-de-defesa-cibernetica-na-copa-do-mundo>. Acesso em: 21 ago. 2017.

DEFESA. EB – Defesa cibernética entra em nova fase. Defesanet, 2015. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/19849/EB---Defesa-Cibernetica-entra-em-nova-fase/>. Acesso em: 21 ago. 2017.

DEIBERT, R. J. Bounding Cyber Power: Escalation and Restraint in Global Cyberspace. In: RAYMOND, M.; SMITH, G. (Eds.) *Organized Chaos*.Waterloo, Canada: Centre for International Governance Innovation, 2014. p. 49-68.

DEIBERT, R. J. Black Code: Censorship Surveillance and the Militarization of Cyberspace. *Millennium Journal of International Studies*, Sage Publications, 2003.

DENARDIS, L. *Global War on Internet Governance*. Nova Haven: Yale University Press, 2014. p. 86-106.

DENARDIS, L. Internet Architecture as a Proxy for State Power. IP Justice Journal: Internet Governance and Online Freedom Publication Series, IP Justice, 2015.

DUNN CAVELTY, M. The Militarisation of Cyber Security as a Source of Global Tension. In: BAUMANN, Andrea; MÖCKLY, Daniel; MAHADEVAN, Prem. *Strategic Trends 2012:* Key Developments in Global Affairs. Zurique, Suíça: Center for Security Studies (CSS), 2012. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2007043>. Acesso em: 21 ago. 2017.

ESCRITÓRIO. Defesa Cibernética. Escritório de Projetos do Exército Brasileiro, 2016. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica>. Acesso em: 21 ago. 2017.

EXÉRCITO. O Sistema Militar de Defesa Cibernética protege e explora um setor em constante mudança. Noticiário do Exército. Exército Brasileiro, 2015. Disponível em: <http://www.eb.mil.br/web/midia-impressa/noticiario-do-exercito?p_p_id=56&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=-column-2&p_p_col_count=3&_56_groupId=16541&_56_articleId=6767201>. Acesso em: 21 ago. 2017.

FINNEMORE, M.; HOLLIS, D. Constructing Norms for Global Cybersecurity. Temple University Beasley School of Law**.** *Legal Studies Research Paper*, p. 425-479, 2016.

GABINETE. Livro Verde de Segurança Cibernética no Brasil**.** Gabinete de Segurança Institucional da Presidência da República. 2010.

GABINETE. Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018. Gabinete de Segurança Institucional da Presidência da República, 2015.

GABINETE. Portaria Normativa N. 2.221/MD, de 20 de agosto de 2012. Ministério da Defesa, 2012.

GIDDENS, A. *The Constitution of Society:* Outline of the Theory of Structuration. United Kingdom: Cambridge Polity, 1984.

GLOBAL. Lauch of Global Commission on the Stability of Cyberspace. Global Commission on the Stability of Cyberspace, 2017. Disponível em:<https://cyberstability.org/news/launch-of-global-commission-on-the-stability-of-cyberspace/>. Acesso em: 21 ago. 2017.

GReAT. WannaCry ransomware used in widespread attacks all over the world. SecureList. Kaspersky Lab, 2017. Disponível em: <https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/>. Acesso em: 21 ago. 2017

GREENWALD, G. *No Place to Hide:* Edward Snowden, the NSA, and the U.S. Surveillance State. London: Picador, 2014.

HANSEN, L.; NISSENBAUM, H. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, v. 53, p. 1155–75, 2009. Disponível em: <http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>. Acesso em: 21 ago. 2017.

HOEPERS, C. 15 anos de tratamento de incidentes no Brasil. 1 Fórum Brasileiro de CSIRTs. Núcleo de Informação e Coordenação do Ponto BR, 2012. Disponível em: <https://www.cert.br/docs/palestras/certbr-forum-csirts2012.pdf>. Acesso em: 21 ago. 2017.

HOEPERS, C. Desafios e lições aprendidas no tratamento de incidentes em grandes eventos. CERT.br. Terceiro Fórum Brasileiro de CSIRTs, 2014. Disponível em: <https://www.cert.br/docs/palestras/certbr-forum-csirts2014-02.pdf>. Acesso em: 21 ago. 2017.

HOFMANN, J.; KATZENBACH, C.; GOLLATZ, K. Between Coordination and Regulation: Conceptualizing Governance in Internet Governance. *HIIG Discussion Paper Series*, n. 2014-04, Alexander Von Humboldt Institut for Internet and Society, 2014.

HUREL, L. M. A governança internacional, regional e nacional da internet. Observatório da Internet, 2016b. Disponível em: <http://observatoriodainternet.br/post/a-governanca-internacional-regional-e-nacional-da-internet>. Acesso em: 21 ago. 2017

HUREL, L. M. *Cybersecurity and Internet Governance: Two Competing Fields?* Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais) – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro. p. 86. 2016c.

HUREL, L. M. Ciberterrorismo: o cavaleiro do infoapocalipse. Revista Insight Inteligência, ed. 71. 2016a. Disponível em: <http://insightinteligencia.com.br/pdfs/71.pdf>. p. 84-93. Acesso em: 21 ago. 2017

HUREL, L.M.; LOBATO, L.C. Unpacking Cyber Norms: Private companies as norms entrepreneurs. *Journal of Cyber Policy* ,v.3, n.1, 2018. DOI: 10.1080/23738871.2018.1467942.

IGF. List of Contributions: 2016 IGF BPF Cybersecurity. Internet Governance Forum, 2016. Disponível em: <http://www.intgovforum.org/multilingual/content/list-of-contributions-2016-igf-bpf-cybersecurity>. Acesso em: 21 ago. 2017.

KRAMER, F.D. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. KRAMER, F. D.; STARR, S. H.; WENTZ, L. (Ed.). *Cyberpower and National Security*. Washington: National Defense University Press, 2008.

KRASNER, S. D. Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization*, v. 36, n. 2, 1982.

LOBATO, L. C.; KENKEL, K. M. Discourses of Cyberspace Securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional*, n. 58, v. 2, p. 23-43, 2015. <https://dx.doi.org/10.1590/0034-7329201500202>. Acesso em: 21 ago. 2017.

MENDES, V. Por segurança, governo cria secretaria para megaeventos. O Estadão. 2011. Disponível em: <http://esportes.estadao.com.br/noticias/futebol,por-seguranca-governo-cria-secretaria-para-megaeventos,753329>. Acesso em: 21 ago. 2017

MICROSOFT. Microsoft abre Centro de Transparência no Brasil para atender aos governos da América Latina. Microsoft, 2016. Disponível em: <https://news.microsoft.com/pt-br/microsoft-abre-centro-de-transparencia-no-brasil-para-atender-aos-governos-da-america-latina/ >. Acesso em: 21 ago. 2017.

MUELLER, M. *Networks and States:* The Global Politics of Internet Governance. Cambridge, MA: MIT Press, 2010.

NIC. Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet no Brasil. NIC.br., 1996. Disponível em: <http://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169#4>. Acesso em: 21 ago. 2017.

NOTA. Nota Técnica da Sociedade Civil para a CPI de Crimes Cibernéticos. Coding Rights e Instituto Beta para Internet e Democracia, 2016. Disponível em: <https://cpiciber.codingrights.org/CPICIBER.pdf>. Acesso em: 21 ago. 2017.

NYE, J. Cyber Power. Belfer Center for Science and International Affairs. Harvard Kennedy School: Cambridge. 2010.

NYE, J. The Regime Complex for Managing Global Cyber Activities. Centre for International Governance Innovation. Waterloo, Canada. 2014.

NYE, J. Controlling Cyber Conflict. Project Syndicate, 2017. Disponível em: <https://www.project-syndicate.org/commentary/new-norms-to-prevent-cyber-conflict--by-joseph-s--nye-2017-08>. Acesso em: 21 ago. 2017.

ONUF, N. *World of Our Making*: Rules and Rule in Social Theory and International Relations. Columbia: University of South Carolina Press, 1989.

RELATÓRIO. Relatório Final da CPI da Espionagem. 2014. Disponível em: <https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>. Acesso em: 21 ago. 2017.

ROHR, A. Anonymous ataca sites ligados ao governo em protesto contra a Rio+20. G1, 2012. Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html>. Acesso em: 21 ago. 2017.

SCHMIDT, A. At the Boundaries of Peer Production: The Organization of Internet Security Production in the Cases of Estonia 2007 and Conficker. *Telecommunications Policy*, n. 36, 2012.

SMITH, B. Brad Smith at RSA 2017: The Need for a Digital Geneva Convention. Microsoft, 2017. Disponível em: <https://www.youtube.com/watch?v=C-YvpuJO6pQ>. Acesso em: 21 ago. 2017.

SOUZA, E. A. A.; ALMEIDA, N. N. A Questão da Segurança e Defesa do Espaço Cibernético Brasileiro. *Revista da Escola de Guerra Naval*, Rio de Janeiro, v. 22. n. 2. p. 381-410, 2016.

WOLFF, J. Models for Cybersecurity Incident Information Sharing and Reporting Policies. 43rd Research Conference on Communications, Information and Internet Policy. 2015.

ATUAÇÃO DO MINISTÉRIO PÚBLICO FEDERAL NO COMBATE AOS CRIMES CIBERNÉTICOS

NEIDE M. C. CARDOSO DE OLIVEIRA

1. INTRODUÇÃO

Qualquer pessoa, em qualquer lugar do mundo, conectada à Internet, o mais poderoso meio de comunicação atual, poderá acessar o conteúdo de páginas ilícitas. E é cada vez mais precoce o uso da rede por crianças e adolescentes, deixando-as muito expostas ao assédio de criminosos.

De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), metade dos brasileiros estão conectados à Internet,[1] ou seja, aproximadamente 107 milhões de pessoas, colocando o Brasil como o quinto país do mundo em número de usuários de Internet.[2]

Uma vez postado na rede, perde-se o controle de qualquer conteúdo. O tradicional conselho *pense antes de falar* deve ser hoje adaptado para *pense antes de postar*. Justamente porque um conteúdo publicado na Internet pode ser visto por qualquer pessoa, reproduzido e até maliciosamente modificado, indefinidamente.

E o Brasil é um dos quatro maiores polos de divulgação de pornografia infantil do mundo, concorrendo com os Estados Unidos, Coreia do Sul e

1 Segundo dados da PNAD (Pesquisa Nacional por Amostra de Domicílios), divulgados pelo IBGE, em 18/09/2014, um em cada dez domicílios brasileiros com conexão à Internet acessa a rede por meio de celular ou *tablet*. *"Segundo o Órgão, 85,6 milhões de brasileiros acima de 10 anos de idade (49,4% da população) tinham usado a Internet, pelo menos uma vez, no período de referência dos últimos três meses (últimos 90 dias que antecederam a entrevista) em 2013".*

2 COMPUTERWORLD. Disponível em: <www.computerworld.com.br>. Acesso em: 18. jan. 2016.

Rússia, segundo a ONG italiana Rainbow Phone.[3] Nesse quadro assustador, a Internet é um facilitador do contato entre criminosos, permitindo sua organização em comunidades e troca de informações, fotos e vídeos.

2. ESTRUTURA E ATUAÇÃO

Diante desse cenário apresentado e do aumento da criminalidade virtual incentivado pela insegurança da rede, o Ministério Público Federal criou, em 2003, na Procuradoria da República no Estado de São Paulo (PR/SP), o primeiro grupo especializado de Combate aos Crimes Cibernéticos. Esse grupo, que se iniciou com três procuradores da República, atualmente, conta com dez membros. Logo em seguida, no ano de 2006, um grupo similar foi criado na Procuradoria da República no Estado do Rio de Janeiro (PR-RJ), que possui desde então três membros da capital.

As atribuições desses procuradores abrangem a atuação em todos os processos judiciais e extrajudiciais que envolvem o tema. Também trabalham na eventual celebração de Termos de Compromisso de Integração Operacional, de Cooperação, Recomendações e Termo de Ajustamento de Conduta (TAC); participam ativamente nas operações repressivas, organizadas anualmente, desde 2009, pela Polícia Federal; e auxiliam na realização das Oficinas para educadores sobre o uso seguro e responsável da Internet, que integra o projeto "Ministério Público pela Educação Digital nas Escolas".

Além dos grupos nas Procuradorias da República dos Estados do Rio de Janeiro e de São Paulo, a 2ª Câmara de Coordenação e Revisão do Ministério Público Federal – cuja temática é criminal – diante da moderna criminalidade via meios virtuais criou, em 2011, um Grupo de Trabalho de Combate a Crimes Cibernéticos de alcance nacional. Dele fazem parte dois procuradores regionais da República – com atuação em 2º grau – e oito procuradores da República – com atuação em 1ª instância –, de diversos estados brasileiros, visando abranger todas as regiões do País. Em março de 2017, a 2ª CCR transformou o Grupo de Trabalho em Grupo de Apoio sobre Criminalidade Cibernética, dando-lhe então um caráter permanente.[4]

Considerando que a repressão penal é insuficiente para coibir as práticas nocivas mais comuns na Internet, tornou-se imprescindível que os prove-

3 SAFERNET BRASIL. Disponível em: <http://www.safernet.org.br/site/noticiais/mpf-safernet-assinam-termo-para-prevenir-crimes-Internet-0>. Acesso em: 22 nov. 2010.

4 Portaria nº 2, de 9/03/2017, da 2ª CCR.

dores de conteúdo e serviço assumissem a responsabilidade de informar corretamente aos consumidores de seus serviços acerca dos mecanismos de proteção contra ações danosas. Por isso, o Grupo de Combate a Crimes Cibernéticos da PR–SP firmou, em 2005, o primeiro Termo de Compromisso de Integração Operacional com os provedores de conteúdo sediados em São Paulo, sejam eles brasileiros ou estrangeiros.[5] Entre as cláusulas previstas no termo, além da criação de *posts* em seus serviços para alertar aos seus usuários sobre eventuais condutas criminosas, foi previsto o prazo de seis meses para preservação dos metadados dos usuários, de modo a auxiliar eventuais investigações criminais. Trata-se de cláusula que posteriormente viria a ser prevista em lei, no Artigo 15 do Marco Civil da Internet.

O grupo especializado da PR/RJ firmou, em 2009, Termo similar com os provedores de serviços situados no Rio de Janeiro.

Neste mesmo ano, o grupo da PR/SP assinou o primeiro Termo de Mútua Cooperação com Empresas de Telecomunicações e Internet (provedores de acesso à Internet).[6] Entre suas cláusulas, uma das mais importantes foi a de preservação dos dados cadastrais de seus clientes pelo período de três anos. Essa previsão de guarda também foi repetida no Marco Civil da Internet, porém com um prazo inferior, de apenas um ano. Esse prazo acabou sendo reforçado no Decreto nº 8771/16, que regulamentou o Marco Civil, prevendo também que os dados devem ser excluídos se encerrado o prazo legal.

No âmbito da atuação judiciária, o Ministério Público Federal de São Paulo ajuizou, em 2005, uma Ação Civil Pública[7] em face do provedor de aplicações de Internet, Google Brasil Internet Ltda., em razão do descumprimento de decisões judiciais brasileiras. No auge da existência da rede de relacionamento Orkut, no qual o Brasil figurava como o segundo maior mercado mundial, atrás apenas da Índia, a empresa se recusava a colaborar com as investigações criminais de maus usuários de seus serviços. Foi somente em 2008, com a instauração da Comissão Parlamentar de Inquérito (CPI) da Pedofilia no Senado Federal, o sigilo de álbuns fechados do Orkut foi afastado pelo Senado. Os álbuns fechados eram utilizados por alguns usuários como veículo de compartilhamento de pornografia infantil. Diante

5 À época, os provedores estrangeiros IG, AOL, UOL e o brasileiro Terra, entre outros. Ver em: MINISTÉRIO PÚBLICO FEDERAL DO BRASIL. Disponível em: <www.prsp.mpf.mp.br-prdc-dhumint>. Acesso em 18 jan. 2016.

6 MINISTÉRIO PÚBLICO FEDERAL DO BRASIL. Disponível em: <www.prsp.mpf.mp.br/sala-de-imprensa/noticias_prsp/noticia-9426>. Acesso em: 10 jul. 2017.

7 Autos nº 2006.61.00.018332-8 – 17ª Vara Cível da Subseção Judiciária de São Paulo.

dessa decisão do Parlamento brasileiro, a empresa Google Brasil finalmente firmou com a Procuradoria da República em São Paulo, no bojo na CPI da Pedofilia, um Termo de Ajustamento de Condutas.[8] Ficou determinado que a PR/SP fosse comunicada sempre que houvesse a remoção de páginas criadas por usuários brasileiros por indícios de veiculação de pornografia infanto-juvenil. A empresa já fazia esse tipo de comunicado ao National Center for Missing and Exploited Children (NCMEC), uma ONG americana responsável pela Central Nacional de Denúncias dos EUA, que, por obrigação prevista em lei, recebe denúncias de veiculação de pornografia infantil de todos os provedores de conteúdo americanos.

Em termos de ações de capacitação, no âmbito nacional, o Grupo de Apoio é responsável pela política institucional de atuação e capacitação dos membros do Ministério Público Federal, voltada para efetiva repressão aos crimes cibernéticos. Essa capacitação é realizada por meio de cursos de treinamento para os novos procuradores que ingressam na carreira – no Curso de Ingresso e Vitaliciamento (CIV) –[9] bem como para aqueles que já estão na carreira.[10] Desde 2015, juízes federais também são convidados para participarem do curso e ministrarem palestras.[11] É cediça a falta de conhecimento técnico do corpo jurídico de qualquer instituição pública, que não trabalhe com a temática relacionada à Internet, como é o caso da Magistratura, Ministério Público e Defensoria Pública, tanto federais como estaduais, em todo o País. A falta desse conhecimento especializado é notada nas eventuais decisões atécnicas proferidas com base em pedidos igualmente não técnicos. Por volta de 2012/2013, algumas faculdades de direito incluíram em suas grades disciplinas relacionadas ao direito digital ou eletrônico. No entanto, a realidade impõe ao profissional do direito trabalhar cada vez mais com crimes que ocorrem pela Internet, ou em que nela são praticados. O combate aos crimes cibernéticos é tema da ordem do dia em razão da universalização da Internet e caminho sem volta para a sociedade contemporânea.

---

8 MINISTÉRIO PÚBLICO FEDERAL DO BRASIL. Informativo 8. Disponível em: <http://www.mpf.mp.br/o-mpf/csmpf/documentos-e-publicacoes/informativos/anos-anteriores/INFORMATIVO-8.pdf/at_download/file>. Acesso em: 10 jul. 2017.

9 Em 2012, 2013, 2014 e 2015, com o curso sobre a "Atuação do MPF no Combate aos Crimes Cibernéticos".

10 Cursos organizados pela Escola Superior do Ministério Público da União – ESMPU em 2012, 2013, 2014, 2015, 2016, 2017 e 2018.

11 Curso "Os crimes cibernéticos e a atuação do Ministério Público Federal, do Judiciário Federal e da Polícia Federal", realizado na PR/SP, de 20 a 22 de out/2015 e o curso "Os crimes Cibernéticos no Âmbito da Competência Federal", em nov/2016, promovido pela ESMPU.

Esse curso de capacitação também é ministrado para diversas autoridades, sempre que requisitados, como para diversos Ministérios Públicos Estaduais[12] e para a magistratura federal dos Tribunais Regionais Federais da 2ª e da 3ª Região.[13] Assim como para as Escolas da Magistratura Estadual do Paraná (2018) e do Rio Grande do Sul (2017).

Ainda no âmbito de ações de capacitação, o Grupo de Combate a Crimes Cibernéticos de São Paulo publicou, em 2007, o "Roteiro de Atuação sobre Crimes Cibernéticos", um manual de atuação dividido em duas partes (técnica e jurídica), com modelos de peças processuais e jurisprudência atualizada, para auxiliar no trabalho dos procuradores da República no País. Esse Roteiro foi atualizado em 2013 e 2016 pelos membros do Grupo nacional, e também é distribuído para autoridades em cursos e palestras ministradas pelos membros do referido Grupo.

O Grupo de Apoio também faz um acompanhamento do legislativo nacional e internacional, por meio da elaboração de Notas Técnicas sobre a temática cibernética ou mediante participação em Comissões Parlamentares de Inquérito.[14] A primeira Nota Técnica do grupo, sobre o Marco Civil da Internet, foi enviada, à época, para consulta pública *on-line* aberta pelo Ministério da Justiça; a segunda nota tratou do Projeto Internet.org e o princípio da neutralidade da rede. O grupo participou ainda da elaboração da Nota Técnica assinada por todos os Ministérios Públicos brasileiros, sobre o descumprimento pelas empresas de Internet da legislação brasileira e, por fim, elaboraram a última Nota sobre o Projeto de Lei que trata da alteração do art. 7º, inciso II e III, e revogação do artigo 12, incisos III e IV do Marco Civil.[15] Elaborada, em 2018, Nota Técnica sobre a Convenção de Budapeste e sua compatibilidade com a legislação brasileira. As coordenadoras do Grupo participaram da audiência pública no Supremo Tribunal

12 Ministérios Públicos Estaduais do Distrito Federal/2016; Amazonas/2015; Maranhão/2015; Minas Gerais/2016; Porto Alegre/2016; Rio de Janeiro/2016; São Paulo/2017.

13 Os cursos "Os Aspectos Internacionais no Combate aos Crimes Cibernéticos", organizado pela EMARF/RJ em ago/2015 e abr/2016. E palestras no curso organizado pela EMARF/SP, em nov/2016.

14 Participação ativa na CPI da Pedofilia, em 2008 e na CPI dos Crimes Cibernéticos, cujas coordenadora e coordenadora adjunta do então GT de Combate a Crimes Cibernéticos, as procuradoras Neide M. C. Cardoso de Oliveira e Fernanda Domingos, respectivamente palestraram na audiência pública ocorrida em 10/09/2015.

15 A Nota Técnica foi distribuída para os líderes de partidos e para o gabinete da presidência da República, no dia 08/12/2016, ocasião em que o referido projeto seria votado e foi retirado de pauta.

Federal sobre ações ADIN nº 5527/DF e ADPF nº 403/SE, relacionadas ao bloqueio do WhatsApp e reunião promovida no STF sobre a ADC 51/STF.

No plano internacional, o Grupo de Apoio colabora com organismos supranacionais, tal como fez ao preencher os questionários sobre crimes cibernéticos no Brasil para o Escritório das Nações Unidas sobre Drogas e Crime (UNODC) e para a Organização dos Estados Americanos (OEA), sempre que solicitado pelo Ministério das Relações Exteriores.[16]

O Ministério Público Federal participa, nacional e internacionalmente, de seminários e eventos relacionados à temática da Internet. Entre os maiores eventos sobre o tema no mundo, podemos destacar o Internet Governance Forum (IGF), organizado pela ONU.[17] Membros dos grupos do MPF participam anualmente do IGF desde 2007; assim como já ministraram cursos sobre crimes cibernéticos em Quito/Equador (2015) e em Montevideo/Uruguai (2012). Integraram a delegação brasileira na VII Reunião sobre Crime Cibernético da OEA, em Washington/EUA (2012) e na reunião informal da ONU sobre a futura elaboração de uma convenção de combate aos crimes cibernéticos, em Viena/Áustria (2013). Estavam presentes e palestraram nas Conferências "Octopus" sobre a Convenção de Budapeste,[18] em Estrasburgo/França (2013, 2014 e 2018), entre outros eventos. Também têm participado da discussão internacional sobre o projeto Jurisdiction & Internet, como no caso das reuniões promovidas pelo Conselho da Europa, em Paris/França (julho e novembro/2016), tão em voga em países europeus e no Brasil, em razão das decisões judiciais brasileiras de suspensão de serviço de provedor de aplicações de Internet, como o WhatsApp, em razão do descumprimento de decisões judiciais.

Por fim, terminando a descrição da atuação do MPF no combate aos crimes cibernéticos, é preciso dizer que a prevenção também é uma preocupação constante dos Grupos. Estes apoiam e participam, desde a sua primeira edição, no Brasil, do "SaferInternet Day", atualmente comemorado em 108 países, e que, no Brasil, é organizado pela ONG SaferNet Brasil.[19]

---

16 Em 2014 e 2016, questionários para o UNODC e para a OEA, em 2015.

17 Nas duas últimas edições, a coordenadora do grupo nacional foi convidada para palestrar em dois *Workshops* (IGF/2016 - Guadalajara/México e IGF/2015 - João Pessoa/Brasil).

18 A Convenção de Budapeste é o único documento internacional a dispor sobre crimes cibernéticos, elaborada pelos países integrantes do Conselho da Europa, em 2001.

19 A ONG SaferNet Brasil é uma associação civil sem fins lucrativos e econômicos, sem vinculação político-partidária, religiosa ou racial fundada em 20/12/2005, por um grupo de cientistas da computação, professores universitários, pesquisadores e

Neste dia, por meio de campanhas divulgadas por várias instituições, entrevistas e debates, procura-se discutir com a sociedade civil, operadores do direito, jornalistas e educadores, como podemos ter uma Internet melhor e mais segura para todos.[20]

3. ATRIBUIÇÃO

A repressão ao crime de divulgação de pornografia infantojuvenil praticado pela Internet[21] é de atribuição do Ministério Público Federal, diante da possibilidade de os dados postados na Internet, de forma irrestrita, serem acessados a qualquer momento e em qualquer lugar do mundo, reforçando assim a transnacionalidade do delito. Por conseguinte, caracteriza-se a competência da Justiça Federal. Ademais, o combate a tal crime é previsto em Tratado Internacional, do qual o Brasil é signatário.[22]

O Supremo Tribunal Federal, ao julgar o Recurso Extraordinário nº 628624, em 29 de outubro de 2015,[23] firmou jurisprudência com repercussão geral e assentou a competência da Justiça Federal quanto ao delito de disponibilização e aquisição de material pedopornográfico, quando a publicação do conteúdo ilícito ocorre em ambiente virtual acessível internacionalmente. O mesmo vale para delitos previstos em Tratados ou Convenções internacionais em relação aos quais o Brasil se comprometeu a combater. Assim, não só crimes relacionados à pornografia infantojuvenil como também os crimes de ódio[24,] praticados nas redes de relacionamento internacional como Facebook; Instagram; Twitter, entre outras, configuram a competência da Justiça Federal.

Assim, os grupos do MPF não tratam de crimes de cunho patrimonial na Internet, como a fraude bancária, por exemplo. A atribuição dos grupos

---

bacharéis em direito. Para mais informações, ver: SAFER NET. Disponível em: <www.safernet.org.br>. Acesso em: 10 jul. 2017.

20 A última edição ocorreu em São Paulo, no dia 07 fev. 2017. Ver:

DIA DA INTERNET SEGURA. Disponível em: <www.diadainternetsegura.org.br>. Acesso em: 10 jul. 2017.

21 Previsto no Artigo 241-A, do Estatuto da Criança e Adolescente.

22 Convenção dos Direitos da Criança (ONU) ratificada pelo Brasil, em 24/09/90-Decreto nº 99710, de 21/11/90.

23 Informativo do STF nº 805, publicado em outubro de 2015.

24 Brasil é signatário da Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial, ratificado em 27/03/1968 – Decreto nº 65.810, de 08/12/69.

especializados e do grupo nacional está restrita àqueles crimes de competência federal – previstos em tratados e convenções internacionais – e que violam os direitos humanos na Internet.

No entanto, quando a transmissão, ainda que pela Internet, de fotografias ou imagens com pornografia ou cenas de sexo explícito infantojuvenil ocorrer de maneira individualizada, entre usuários localizados no Brasil, como por meio de troca de *e-mails;* inclusive quando houver o aliciamento de crianças e adolescentes para produção desse material em salas de bate papo (*chats*); a posse desse tipo de material em quaisquer dispositivos informáticos; a injúria racial, entre outros, estamos diante de delitos cuja competência é da Justiça Estadual, e, por consequência, de atribuição do Ministério Público Estadual. Nesses casos, o crime não ultrapassa as fronteiras do Território Nacional.

4. OPERAÇÕES POLICIAIS

Como resultado da cooperação entre Ministério Público Federal, Polícia Federal e a CPI da Pedofilia, em 18.05.2009, foi realizada a chamada operação "Turko" – para cumprir 92 mandados de busca e apreensão em 20 estados e no DF contra usuários do *site* de relacionamento *Orkut*, que usavam o recurso de restrição de acesso aos álbuns de fotografia (os álbuns fechados) para trocar e divulgar material de pornografia infantojuvenil. Essa foi a primeira operação a ser executada após o acordo (TAC) realizado entre o MPF e a Google do Brasil.

Em julho de 2010, ocorreu a operação "Tapete Persa", também envolvendo delitos de abuso sexual e pedofilia. Proveniente de denúncia da Alemanha, no curso da operação foram presas cerca de 20 pessoas, de um total de 120 mandados de busca e apreensão cumpridos em vários estados.

Dois anos depois, no mês de junho, ocorreu a operação "DirtyNet". Trata-se da primeira operação de combate à delitos cibernéticos organizada pela Polícia Federal em nível internacional, que identificou o responsável por criar uma rede fechada, de âmbito global, onde acontecia a troca de arquivos de pornografia infantil, usando a ferramenta Gigatribe.[25] A operação visava 160 alvos brasileiros e estrangeiros, cujas autoridades dos países de origem também foram comunicadas. No dia da operação no Brasil, na qual ocorreu o cumprimento de cerca de 50 mandados de busca e apreensão espalhados por diversos estados, houve também ações simultâneas no Reino Unido e na Bósnia.

25 "Programa de compartilhamento de arquivos que funciona através de grupos fechados".

O MPF participou também da operação "DarkNet I" (2014) e "DarkNet II"(2016), deflagradas a partir de investigação iniciada na Polícia Federal no Rio Grande do Sul,*26* em que se procurou coibir crimes relacionados à pornografia infantil praticados na oculta Rede TOR. Foi a primeira operação na Deepweb,[27] no Brasil. Foram cumpridos 100 mandados judiciais de busca e apreensão, com 55 pessoas presas e 6 crianças resgatadas em situação de abuso durante a investigação. A operação ocorreu simultaneamente em 18 estados do Brasil. Várias postagens feitas por alvos no Brasil e exterior (1579 usuários cadastrados rastreados) foram identificadas, cuja materialidade delitiva foi enviada aos respectivos países para conhecimento e providências cabíveis. Um desdobramento da operação DarkNet II ocorreu, em novembro de 2016, em 17 estados, atingindo aproximadamente 70 alvos. Para a realização dessas operações foi preciso desenvolver técnicas inovadoras para combater crimes na Deepweb, tais como a infiltração policial em grupos *on-line* fechados na Rede TOR. Em 2018, ocorreu a segunda fase da operação "Underground 2", em São Paulo e mais 6 estados (RJ, MG, PE, AC, GO e MA), que mirou grupo de WhatsApp (com participação de estrangeiros) destinado a troca de pornografia infantil.

5. COMO DENUNCIAR

Parte da atuação do MPF no combate aos crimes cibernéticos é mobilizada por meio de denúncias. Para que isso aconteça, qualquer pessoa pode se utilizar dos serviços disponíveis na *home page* das Procuradorias da República em todas as capitais e no Distrito Federal,[28] além dos outros tradicionais canais de comunicação: por telefone ou presencialmente, nas salas de Atendimento ao Cidadão, existentes em todas as Unidades do MPF. Essas denúncias costumam ser feitas por pessoas comuns ou comunidades organizadas no combate a crimes na Internet. Na maioria dos casos, a representação da denúncia não precisa trazer muitas informações, podendo ser iniciada apenas com o endereço eletrônico do *site* onde estaria sendo praticado o crime.

---

26 Operação organizada pela Polícia Federal, sob coordenação da procuradora da República, Jaqueline Buffon, da PR/RS.

27 *Deepweb*, rede em que tudo que nela transita não está indexado na Internet por ferramentas de buscas usuais, é acessível por meio, entre outros, de redes anônimas, como a mais conhecida chamada TOR, que previne que a localização e hábitos de navegação sejam descobertos.

28 Ex: MINISTÉRIO PÚBLICO FEDERAL DE SÃO PAULO. Disponível em: <http://www.mpf.mp.br/sp>. Acesso em: 20 dez. 2018; MINISTÉRIO PÚBLICO FEDERAL DO RIO DE JANEIRO. Disponível em:<www.prrj.mpf.mp.br>. Acesso em: 20 dez. 2018, etc; adaptar de acordo com a sigla do estado correspondente.

Com o intuito de ampliar a capacidade do MPF atuar a partir de denúncias, a 2ª Câmara de Coordenação e Revisão firmou com a ONG SaferNet Brasil e o Comitê Gestor da Internet no Brasil –CGI.br,[29] o Termo de Mútua Cooperação Técnica e Operacional[30] para que seja viabilizado ao MPF o acesso ao banco de dados de denúncias recebidas pela ONG SaferNet Brasil.

6. PREVENÇÃO

A preocupação com a navegação segura na Internet surgiu como consequência da atuação desses grupos de combate a crimes cibernéticos. Percebeu-se que muitas pessoas eram vitimadas por desconhecimento das medidas básicas de segurança e cuidados simples.

Considerando que só a repressão era insuficiente e que a prevenção é o melhor caminho na conscientização das crianças e adolescentes – as principais vítimas dos crimes de aliciamento *online*, difusão de imagens pornográficas e de *cyberbulling* – o Ministério Público Federal, em parceria com a ONG SaferNet Brasil, organizou, de 2009 a 2013, as Oficinas sobre o Uso Seguro e Responsável da Internet para educadores da rede pública e privada de ensino.

A partir das experiências bem-sucedidas em São Paulo e no Rio, o MPF, coordenado pela Procuradoria Federal dos Direitos do Cidadão,[31] por meio dos GT de Comunicação Social e o então GT de Combate a Crimes Cibernéticos da 2ª CCR, em parceria com a SaferNet e o Comitê Gestor da Internet no Brasil, lançou em 2015 o projeto "Ministério Público pela

29 O Comitê Gestor da Internet no Brasil tem a atribuição de estabelecer diretrizes, estratégias relacionadas ao uso e desenvolvimento da Internet no Brasil e diretrizes para a execução do registro de Nome de Domínio, alocação de Endereço IP e administração pertinente ao Domínio de Primeiro Nível ".br". Ver mais em: CGI.BR. Disponível em: <www.cgi.br>. Acesso em: 10 jul. 2017.

30 SAFERNET BRASIL. Disponível em: <http://www.safernet.org.br/site/noticiais/mpf-safernet-assinam-termo-para-prevenir-crimes-Internet-0>. Acesso em: 10 jul. 2017.

31 Outra faceta do Ministério Público, desconhecida por muitos brasileiros, que muitas vezes só o veem como órgão de persecução penal, é a função constitucionalmente prevista de proteção dos direitos individuais indisponíveis, coletivos e difusos da sociedade. Entre esses direitos indisponíveis, está a proteção à imagem da criança e do adolescente na Internet. Essa função é desempenhada e coordenada nacionalmente pela Procuradoria Federal dos Direitos do Cidadão.

Educação Digital nas Escolas".[32] O projeto visou a realização da oficina "Segurança, Ética e Cidadania: Educando para Boas Escolhas *On-line*", voltado para a rede de educação pública e privada. Em seu primeiro ano, 12 capitais e o Distrito Federal sediaram oficinas. Na segunda fase, a referida Oficina foi realizada em todas as capitais do País, assim como em comunidades indígenas de São Paulo.

No dia da Oficina, destinada a professores ou coordenadores pedagógicos indicados pelas Secretarias de Educação Estadual e Municipal, as palestras são acompanhadas pela distribuição de materiais pedagógicos para a introdução do tema em sala de aula. Cada educador aprende a desmistificar a ideia de que deve conhecer de tecnologia para falar sobre noções de ética, cidadania e segurança e se torna responsável pela multiplicação do aprendizado.

O objetivo do material pedagógico é estimular as crianças e adolescentes a aproveitarem todo o potencial da rede, sem se esquecerem de adotar os cuidados necessários neste novo espaço público.

Após cada oficina, são disponibilizadas 3.000 cópias da cartilha "Diálogo Virtual" para as escolas interessadas distribuírem às crianças. Medindo o resultado do projeto, verificou-se que, em dois anos, 20 oficinas capacitaram diretamente 2.887 educadores de 280 municípios em 16 estados, beneficiando 155.004 alunos em atividades de multiplicação nas escolas.

Atualmente, em sua 3º fase, o projeto visa realizar as mesmas Oficinas em cursos de Pedagogia, Psicologia e Serviço Social de Universidades federais, que integrem o Pacto Universitário do MEC, e atingir alunos e professores que interessem em lidar com a temática.

O objetivo deste projeto é a união de esforços na prevenção e combate à pornografia infantil e aos crimes de racismo na Internet. Há um incentivo na educação para todos denunciarem esses crimes sem constrangimento e cobrarem das autoridades a punição dos criminosos, mas, principalmente, aprenderem a usar a Internet de forma ética e segura.

Com o projeto, o Ministério Público Federal e seus parceiros buscam pôr em prática o artigo 26 do Marco Civil da Internet:

> "O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras

32 PROCURADORIA FEDERAL DOS DIREITOS DO CIDADÃO. Disponível em: <www.pfdc.pgr.mpf.mp.br/projetos-finalisticos/educacao-digital-nas-escolas/o-que-e-o-projeto/>. Acesso em: 10 jul. 2017.

práticas educacionais da Internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico."

7. CONCLUSÃO

O Ministério Público Federal, por meio do Grupo de Combate a Crimes Cibernéticos, com sua função de órgão de persecução penal e fiscal da lei, procura cumprir o *mister* constitucional de defensor da sociedade, ao mesmo tempo em que procura prevenir a prática delituosa, por meio da educação, a fim de que crianças e adolescentes cresçam conscientes de seus atos. Assim, ao se tornarem adultos, terão as informações e os incentivos para não praticarem crimes na Internet, tornando-se cidadãos ciosos de seus direitos e deveres no mundo virtual.

REFERÊNCIA

CGI.BR. Disponível em: <www.cgi.br>. Acesso em: 10 jul. 2017.

COMPUTERWORLD. Disponível em: <www.computerworld.com.br>. Acesso em: 18. jan. 2016.

DIA DA INTERNET SEGURA. Disponível em: <www.diadainternetsegura.org.br>. Acesso em: 20 dez. 2018.

MINISTÉRIO PÚBLICO FEDERAL DE SÃO PAULO. Disponível em: <http://www.mpf.mp.br/sp>. Acesso em: 20 dez. 2018.

MINISTÉRIO PÚBLICO FEDERAL DO BRASIL. Disponível em: <www.prsp.mpf.mp.br/sala-de-imprensa/noticias_prsp/noticia-9426>. Acesso em: 10 jul. 2017.

MINISTÉRIO PÚBLICO FEDERAL DO RIO DE JANEIRO. Disponível em:<www.prrj.mpf.mp.br>. Acesso em: 20 dez. 2018.

PROCURADORIA FEDERAL DOS DIREITOS DO CIDADÃO. Disponível em: <www.pfdc.pgr.mpf.mp.br/projetos-finalisticos/educacao-digital-nas-escolas/o-que-e--o-projeto/>. Acesso em: 10 jul. 2017.

SAFER NET. Disponível em: <www.safernet.org.br>. Acesso em: 10 jul. 2017.

SAFERNET BRASIL. Disponível em: <http://www.safernet.org.br/site/noticiais/mpf-safernet-assinam-termo-para-prevenir-crimes-Internet-0>. Acesso em: 10 jul. 2017.

SILVA, Ângelo Roberto Ilha (Org.). *Crimes cibernéticos:* racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2018.

INTERNET E JURISDIÇÃO, ACESSO TRANSFRONTEIRIÇO A DADOS E O CASO IRLANDA MICROSOFT

MELISSA GARCIA BLAGITZ DE ABREU E SILVA

INTRODUÇÃO

A Internet produziu uma revolução. A rede mudou a forma como a sociedade pensa, age e interage. Ela permitiu ampla e irrestrita comunicação e trocas de dados, ignorando fronteiras físicas. A nova realidade modificou profundamente como dados e documentos eletrônicos são armazenados e acessados. Nesse novo quadro, o conceito puramente territorial de jurisdição tornou-se inadequado e obsoleto, e o desenvolvimento de novos critérios um tema urgente.

Enquanto o mundo lida há mais de uma década com os problemas relacionados ao acesso transfronteiriço a provas eletrônicas, isto é, o acesso direto a provas eletrônicas fora das fronteiras do Estado requisitante, o problema apenas despertou maior atenção e interesse nas cortes norte-americanas com o caso Microsoft Irlanda.[1] O longo debate entre Departamento de Justiça e Microsoft nesse caso, embora aparentemente limitado a preceitos da legislação norte-americana, em realidade refletiu a necessidade de novos parâmetros para a definição de jurisdição em um mundo de computadores e nuvens, necessidade esta reconhecida recentemente pela Comissão Europeia, com a apresentação em 17 de abril de 2018 de proposta legislativa sobre provas eletrônicas, denominada E-Evidence.[2]

1 *In the Matter of a Warrant to Search a Certain E-mail Account Controlled And Maintained By Microsoft Corporation,* United States Court of Appeals for the Second Circuit, Docket N. 14-2985, julgado em 14 de julho de 2016.

2 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters. Cf.: EUR-LEX. Document 52018PC0225. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN>. Acesso em: 3 jul. 2018.

Este artigo propõe-se ao breve exame dos principais argumentos apresentados pelo governo norte-americano e a Microsoft, e de como esses argumentos, embora aparentemente limitados à realidade local, espelham questões mais amplas que vêm sendo discutidas em outros países e possuem reflexos na legislação brasileira e no futuro da proteção à privacidade.

O CASO MICROSOFT IRLANDA

Resumidamente, o caso Microsoft Irlanda refere-se a um pedido e posterior expedição de mandado de busca e apreensão para coletar informações e conteúdo de uma conta de *e-mail* mantida e controlada pela empresa Microsoft. A base legal para a decisão inicial, emitida por um magistrado do Circuito de Nova Iorque, é a seção 18 U.S.C. § 2703(a),[3] que impõe a necessidade de mandado de busca e apreensão para a obtenção de conteúdo de e-mails com menos de 180 dias.[4] Houve resistência da empresa na entrega dos dados ao argumento de que eles, apesar de controlados pela Microsoft nos Estados Unidos, estavam armazenados em servidores mantidos pela empresa na República da Irlanda o que, na visão da companhia, demandaria pedido formal de cooperação internacional, sem a possibilidade de acesso direto.

---

3 18 U.S.C. § 2703(a) determina, em tradução livre: "CONTEÚDO DE COMUNICAÇÃO VIA CABO OU ELETRÔNICA ARMAZENADA ELETRONICAMENTE – Um órgão do governo pode requisitar que um serviço provedor de comunicação eletrônica apresente o conteúdo de comunicação via cabo ou eletrônica armazenado eletronicamente em sistema de comunicação eletrônica por menos de cento e oitenta dias apenas mediante de mandado expedido pela corte competente através do procedimento descrito nas Normas de Processo Penal Federal (ou no caso de cortes estaduais, conforme as normas processuais estaduais).

No original: *"CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE. – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction"*

4 É importante observar que a distinção feita pela legislação norte-americana entre e-mails armazenados por mais ou menos de cento e oitenta dias foi modificada por diversas decisões de Cortes Federais aplicando a Quarta Emenda constitucional e o conceito de *"expectativa de privacidade"* definido em *Katz v. United States* (Suprema Corte, 1967, 389 U.S. 347). Hoje, no sistema legal norte-americano, qualquer conteúdo de comunicação eletrônica somente pode ser obtido mediante mandado de busca e apreensão expedido pela autoridade judiciária competente.

Assim, a principal questão em debate nos sucessivos recursos que se seguiram após a autorização inicial se resume a como definir a obtenção de dados guardados fisicamente em um país, mas controlados por empresa que presta serviços no território local. Discute-se se haveria apenas uma questão interna, de acesso a dados controlados por empresa local, independentemente de onde estão fisicamente armazenados, ou uma questão internacional a demandar envolvimento de autoridades estrangeiras e pedido formal de cooperação.

Em suas objeções ao mandado expedido, Microsoft apresentou, essencialmente, quatro argumentos:

d. seção 2703(a) exige a expedição de mandado de busca e apreensão, que somente pode ser cumprido no território sob jurisdição do Juízo expedidor;

e. há presunção contra a aplicação extraterritorial de preceitos da legislação norte-americana, presunção esta que somente pode ser deixada de lado se há a clara intenção da norma legal, expressa em sua linguagem[5], de ser cumprida fora do território norte-americano e nada na lei que autoriza a busca e nem nas regras de procedimento que devem ser seguidas para sua execução contém essa indicação;

f. o mandado expedido autoriza a busca e apreensão no território de outro país;

g. ainda que fosse possível a aplicação extraterritorial da norma, razões de cortesia internacional (*international comity*) a desaconselhariam, pois o Direito Internacional não reconhece o acesso transfronteiriço a dados.

O governo norte-americano, de sua parte, argumentou que:

a. o mandado expedido nos termos da seção 2703(a) é executado como uma requisição e não uma busca e apreensão: é uma ordem para o fornecimento de dados (*compelled disclosure*) e não autorização para entrada forçada e apreensão;

5 No caso *Morrison v. National Australia Bank Ltd.* (130 S.CT. 2869), a Suprema Corte norte-americana decidiu que a legislação local, salvo se houver clara demonstração do contrário pela redação ou intenção declarada do Legislador, somente deve ser aplicada no território sob jurisdição dos Estados Unidos e que tal princípio deve ser observado em todos os casos em que as partes buscam efeitos extraterritoriais na aplicação da lei norte-americana.

b. como tal, o critério a ser empregado é quem controla os documentos ou dados e não o local onde eles estão fisicamente mantidos (*control, not location*).

Na última decisão de mérito proferida no caso, datada de 14 de julho de 2016,[6] a Corte de Apelações do Segundo Circuito concordou com os argumentos da Microsoft e considerou o caso apenas uma questão de extraterritorialidade de norma, aplicando a ele a presunção contra extraterritorialidade acima mencionada. Embora reconhecendo que a questão representa um problema novo que precisa ser analisado com urgência pelo Legislador, a corte concluiu que nem a seção 2703(a), nem a regra 41 do Processo Penal Federal, que disciplina a expedição e o cumprimento de mandados de busca e apreensão, traziam indicativos que permitissem a aplicação extraterritorial, e como o mandado deveria ser cumprido em território irlandês, onde armazenados os dados, sem a extraterritorialidade o Juízo não poderia expedir ordem a ser cumprida fora de sua jurisdição.[7]

Sem adentrar em análise mais profunda da legislação estadunidense, é certo que o argumento utilizado pelo governo norte-americano, de controle ao invés de localização, para definir a jurisdição sobre a prova eletrônica tem respaldo no Direito Internacional, na Convenção de Budapeste sobre Cibercriminalidade, e legislações de diversos países, inclusive o Brasil. Ele também representa uma mudança de paradigma que reflete as peculiaridades da prova eletrônica e as necessidades do mundo conectado nas nuvens.

---

6 A íntegra da decisão pode ser acessada em: DEPARTMENT OF JUSTICE. Case 14-2985, Document 286-1, 07/14/2016, 1815361, Page1 of 43. Disponível em: <https://www.justice.gov/archives/opa/blog-entry/file/937006/download>. Acesso em: 3 jul. 2018.

Em 24 de janeiro de 2017, o 2º Circuito negou pedido do governo norte-americano para que o caso fosse ouvido *em banc,* ou seja, por todos os membros da corte. Ver: KERR, Orin. 2nd Circuit denies rehearing in Microsoft Ireland case by an evenly divided vote. The Washington Post, 24 jan. 2017. Disponível em: <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/01/24/2nd-circuit-denies-rehearing-in-microsoft-ireland-case-by-an-evenly-divided-vote/?utm_term=.678da86781c8>. Acesso em: 3 jul. 2018.

7 Após essa decisão, o caso foi aceito pela Suprema Corte norte-americana, que ouviu argumentos orais em 27 de fevereiro de 2018. Entretanto, em 17 de abril de 2018, a Corte considerou o caso prejudicado, após pedido das partes, em razão da entrada em vigor do CLOUD Act, sancionado em 22 de março de 2018, que deixou expressa a possibilidade de acesso a dados controlados por empresas estadunidenses, ainda que armazenados em outros países, exatamente como defendido pelo Departamento de Justiça daquele país.

A CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIMINALIDADE E O ACESSO À PROVA ELETRÔNICA

A Convenção de Budapeste sobre Cibercriminalidade do Conselho da Europa (CETS no. 185) foi um dos primeiros e até o momento é um dos únicos instrumentos internacionais sobre crimes cibernéticos e prova eletrônica. Originalmente gestada no Conselho da Europa, foi assinada por 63 países, incluindo 17 não europeus.[8]

A Convenção regula detalhadamente crimes cibernéticos e prova eletrônica.[9] Seu principal objetivo é harmonizar a legislação mundial sobre crimes cibernéticos, permitindo melhor uso de mecanismos de cooperação internacional e extradição. Ela contém dispositivos de direito material, descrevendo ofensas criminais, e também dispositivos processuais, incluindo ferramentas de investigação, preservação de dados, requisições de provas, busca e apreensão, e jurisdição internacional e cooperação.

O PRINCÍPIO TERRITORIAL, PROVA ELETRÔNICA E CRIMES CIBERNÉTICOS

O princípio territorial é a regra mais básica para definição de jurisdição. Todo Estado é soberano em seu território e consequência necessária da soberania é a habilidade de legislar, julgar e executar seus julgamentos dentro de seu território. Ele é baseado no fato de que um Estado tem controle sobre as ações, pessoas e coisas dentro de suas fronteiras. Como consequência, um documento ou prova armazenada no território de um Estado e necessária para um procedimento em outro Estado deve ser objeto de um pedido de cooperação internacional em matéria judicial.

O princípio territorial funciona sem maiores problemas em investigações convencionais. Normalmente, crimes são cometidos em um território, por uma pessoa dentro desse território, tendo como vítimas pessoas no território. O mesmo Estado que tem jurisdição territorial para legislar, terá jurisdição territorial para julgar o caso e executar a pena eventualmente imposta.

---

8 Ver: COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 185. Disponível em: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=VsTdZN6J>. Acesso em: 3 jul. 2018.

9 O texto completo em português pode ser encontrado em: COUNCIL OF EUROPE. CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa428>. Acesso em: 3 jul. 2018.

Quando mais de um Estado está envolvido, usualmente há uma ligação territorial que torna fácil identificar qual deles tem jurisdição sobre o caso – o local onde estão as vítimas geralmente está relacionado com o local da prova, ainda que o autor do fato esteja em outro lugar, e essas questões são resolvidas com regras sedimentadas. Crimes tradicionais não representam grandes desafios ao princípio.

O princípio territorial puro, no entanto, simplesmente não funciona para provas eletrônicas e crimes cibernéticos internacionais.[10]

Primeiro, porque crimes cibernéticos, em regra, atingem vítimas por todo o mundo, usando equipamentos espalhados globalmente, com autores conectados na rede a partir de diferentes países. Provas eletrônicas, ainda que relacionadas a crimes tradicionais locais, são normalmente armazenadas em diferentes lugares, por diferentes empresas, de diferentes países, com base em critérios puramente coorporativos – o que funcionar melhor para a operação da empresa responsável pela armazenagem.[11]

Segundo, porque provas eletrônicas podem ser acessadas de qualquer lugar. Independentemente do local onde esteja mantido fisicamente o servidor que armazena os dados, desde que conectado em qualquer tipo de rede, eles poderão ser acessados de qualquer ponto do mundo.

Essa afirmativa um tanto quanto óbvia é crucial e pode levar a resultados desconcertantes quando o princípio territorial é aplicado de forma pura a crimes com provas eletrônicas. De acordo com o princípio em seu conceito mais básico, se um órgão de investigação possui um mandado de busca e apreensão legalmente expedido para apreender um computador e o encontra ligado, exibindo o acesso a uma conta de *e-mail* mantida em servidores localizados em outro país, os agentes não poderão acessar, coletar ou mesmo ler os *e-mails*. Os *e-mails*, nesse exemplo, mesmo nas vistas dos investigadores e acessíveis às pontas dos seus dedos, são na verdade documentos internacionais, sob a jurisdição de outro país, e somente poderão

10 A expressão "crimes cibernéticos internacionais" é até certo ponto um paradoxo porque todos os crimes cibernéticos hoje têm um componente internacional, em maior ou menor grau.

11 Cada vez mais frequente é a utilização de CDN (*content delivery networks*), nas quais o conteúdo fica espalhado em diversos pontos e é enviado ao usuário de forma otimizada conforme sua localização: WIKIPEDIA. Content delivery network. Disponível em:<https://en.wikipedia.org/wiki/Content_delivery_network>. Acesso em: 3 jul. 2018. Nesses casos, a empresa responsável pelos dados simplesmente não sabe onde eles estão fisicamente armazenados, pois a localização é determinada por algoritmos e pode ser alterada a qualquer momento, independente de comando humano.

ser lidos ou acessados mediante autorização desse país, após demorado e laborioso pedido de cooperação internacional.

A conclusão aqui é simples: o princípio territorial em sua forma tradicional não atende às peculiaridades das provas eletrônicas e dos crimes cibernéticos, e a necessidade de novos instrumentos funcionais tem sido objeto de constantes debates entre órgãos de investigação e a academia. A Convenção de Budapeste deu um primeiro passo para solucionar esse dilema.

A CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste contém dois artigos que precisam ser analisados em conjunto quando se pretende entender o novo parâmetro internacional para acesso a provas eletrônicas, que substitui o critério de *localização* pura da prova por *controle* da prova, sem perder de vista a jurisdição territorial ao considerar o local de prestação do serviço.

O primeiro artigo expressamente admite o que é referido como "acesso transfronteiriço a dados informáticos armazenados". Em outras palavras, o dispositivo reconhece que a prova eletrônica é acessível de qualquer lugar do mundo e estabelece, *ex ante*, que os Estados signatários da Convenção poderão, atendidas determinadas circunstâncias, acessar arquivos e documentos que estão fisicamente localizados em outros Estados signatários, mas que podem ser acessados através da rede.[12] A alínea (b) disciplina o exemplo mencionado acima e também estabelece o critério *controle* para a determinação da jurisdição. Nos termos da Convenção, os Estados signatários autorizam previamente que os outros Estados signatários acessem diretamente dados armazenados em seus territórios se a pessoa legalmente autorizada a fornecer esses dados consentir voluntariamente. Isto é, se a pessoa que *controla* a informação consentir, órgãos de investigação poderão acessar a informação, mesmo que armazenada no exterior.

---

12 *In verbis*:

Artigo 32º. – Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma parte pode, sem autorização de outra parte:

a. Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou

b. Aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

Esse dispositivo, entretanto, tem limitações. A primeira é que ele não pode ser aplicado a dados armazenados em países que não são signatários da Convenção. Isso limita o escopo do dispositivo, ainda que a Convenção tenha sido assinada por países que representam grande parte do fluxo de dados via Internet.

A segunda limitação traduz-se na impossibilidade de a informação ser obtida sem o consentimento da pessoa que a controla, o que é agravado pelo fato de, na maioria dos países, os provedores de serviço e de aplicativos não poderem legalmente consentir e ceder informações de seus usuários. O dispositivo, assim, é limitado à pessoa que legalmente controla e detém a informação e consente em auxiliar. Ele não prevê a possibilidade de requisição, mesmo judicial (*compelled disclosure*), e nem de extensão da autorização a terceiros que controlam a informação porque prestam serviços, ausente autorização específica do usuário.[13]

Apesar desses problemas, o dispositivo representa avanço notável, especialmente quando considerado que foi escrito no início dos anos 2000.

O segundo dispositivo está no artigo 18 da Convenção e a legislação doméstica editada para implementá-lo está criando novos dispositivos de Direito Internacional costumeiro e modificando a forma como é definida a jurisdição sobre a prova eletrônica.

O artigo 18 determina que cada Estado signatário "adotará" as medidas legislativas necessárias para "habilitar as suas autoridades competentes" para ordenar a uma pessoa em seu território que forneça "dados informáticos específicos, *na sua posse ou sob o seu controle* e armazenados num sistema informático ou um outro suporte de armazenamento de dados informáticos" (grifo nosso).[14]

---

13 Diversas discussões estão correndo dentro do Conselho da Europa visando aprimorar o acesso transfronteiriço a dados. Relatórios das discussões em inglês podem ser acessados em: <http://www.coe.int/en/web/cybercrime/t-cy-reports>. Acesso em: 3 jul. 2018.

14 *In verbis*:

Artigo 18º. – Injunção

1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:

a. A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controle e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e

O artigo não menciona onde a informação deve estar armazenada, se fora ou dentro do território do requisitante, mencionando apenas que a pessoa requisitada deve ter *controle* sobre os dados e tanto as legislações que implementaram nos Estados-parte os termos da Convenção, como visto abaixo, como o próprio comitê responsável,[15] têm considerado que o local físico de armazenamentos dos dados não define a jurisdição.

Na realidade, as legislações domésticas dos países signatários estão dando força plena ao critério controle, estabelecendo, primeiro, que o fator determinante para a definição de jurisdição sobre prova eletrônica é controle e não localização; e segundo, que um Estado tem plena jurisdição para acessar diretamente essa prova se a empresa que a controla estiver localizada em seu território ou nele prestar serviços, independentemente do local em que estiver fisicamente armazenada. Em verdade, no mundo da computação nas nuvens, o local físico de armazenamento torna-se cada vez mais irrelevante, pois pode mudar em questão de minutos ou

---

b. A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controle, relativos aos assinantes e respeitantes a esses serviços.

1. Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º. e 15º.

2. Para os fins do presente artigo, a expressão "dados relativos aos assinantes" designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:

a. O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b. A identidade, a morada postal ou geográfica e o número de telefone do assinante e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;

c. Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

15 Em março de 2017, o T-CY editou a *Guidance Note # 10*, contendo normas para a interpretação do artigo 18: COUNCIL OF EUROPE. T-CY Guidance Note #10. Production orders for subscriber information. (Article 18 Budapest Convention). Disponível em: <https://rm.coe.int/16806f943e>. Acesso em: 3 jul. 2018. Segundo os novos termos, os Estados parte poderão expedir ordens para obter dados cadastrais, incluindo números IP, localizados outro território desde que o provedor que controla os dados preste serviços no território da parte e os dados se refiram a serviço prestado no território do requisitante.

ser completamente desconhecido, tornando-se essencial quem controla as informações e onde esse controlador presta serviços.[16]

A LEGISLAÇÃO DOMÉSTICA[17] E A JURISPRUDÊNCIA DE PAÍSES EUROPEUS

Como mencionado, na esteira dos dispositivos da Convenção de Budapeste, diversos Estados europeus, signatários ou não da Convenção, elaboraram legislações adotando e expandindo o acesso transfronteiriço a dados e o critério controle.

Os Estados utilizam o artigo 18 para requisitar que empresas prestadoras de serviço em seus territórios forneçam diretamente dados eletrônicos necessários a investigações.[18] Austrália, Espanha e Canadá permitem que

16 A legislação sobre *E-Evidence* proposta pela Comissão Europeia e ora em discussão no parlamento europeu também contém disposições semelhantes, que permitem o acesso a dados controlados por empresas que prestam serviços em território europeu, independente do local de efetivo armazenamento dos dados e mesmo da sede da empresa. A legislação proposta contém soluções para cumprimento de decisões mesmo quando a empresa controladora não possui sede em países do bloco europeu e traz, ainda, dispositivos que permitem solução para hipóteses de conflito de leis quando, por exemplo, a legislação do país onde mantidos fisicamente os dados impede ou dificulta a transferência direta para outros países. A proposta reconhece poucas hipóteses em que as oposições baseadas em conflito de leis apresentadas pelas empresas controladoras dos dados serão aceitas, e mesmo nessas, a depender de efetiva oposição do país onde localizados os dados. A íntegra da proposta, diretriz e regulamento, pode ser encontrada em: EUROPEAN COMMISSION. E-evidence - cross-border access to electronic evidence. Disponível em: <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en>. Acesso em 3 jul. 2018.

17 Extraído de "*Transborder* access and jurisdiction: What are the options", relatório do Subgrupo em Jurisdição e Acesso Transfronteiriço a Dados do Comitê T-CY da Convenção de Budapeste, adotado em dezembro de 2012. Disponível em: CYBERCRIME CONVENTION COMMITTEE. Transborder access and jurisdiction: What are the options? Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8>. Acesso em: 3 jul. 2018.

18 Maxwell, Winston/Wolf, Christopher (2012): A Global Reality: Governmental Access to Data in the Cloud (Hogan Lovells White Paper, 23 May 2012), mencionado pelo relatório do T-CY. O documento original, em inglês, está disponível em: HOGAN LOVELLS. Hogan Lovells White Paper - Government access to Data in the Cloud. Disponível em: <https://www.hoganlovells.com/en/publications/hogan-lovells-white-paper-government-access-to-data-in-the-cloud>. Acesso em: 3 jul. 2018.

órgãos de investigação requisitem de empresas localizadas em seu território informações, independentemente do local de armazenamento. Dinamarca, França e Reino Unido trazem dispositivos semelhantes, com um requisito a mais, permitindo a requisição e o acesso direto quando os dados estão sob o controle de empresa local *e* podem ser acessados de seus territórios.

Ironicamente, no caso Microsoft Irlanda, o próprio governo irlandês apresentou petição como *amicus curiae* informando à Corte de Apelação que, apesar das preocupações da empresa ré com questões diplomáticas que pudessem advir do acesso direto aos dados armazenados no exterior, a legislação irlandesa também autoriza o acesso direto, mediante o critério de controle. O documento, citando decisão da Suprema Corte irlandesa no caso *Walsh v. Irish National Bank*, afirma que a legislação local permite o acesso a dados controlados por empresa irlandesa, independentemente do local em que estão fisicamente armazenados.[19] Importante salientar que a Irlanda assinou, mas não ratificou a Convenção de Budapeste.

Em todos os casos citados, as legislações locais reconhecem que o que determina a possibilidade de acesso direto a provas eletrônicas não é o local de armazenamento destas, mas o local em que está estabelecida, de qualquer forma, ou prestando serviços a empresa que *controla* esses dados. Aplica-se, assim, o princípio territorial, mas não mais focado no local onde fisicamente guardadas as provas, e sim no local de prestação do serviço e de presença da empresa: os fatores considerados passam a ser o local em que prestado o serviço, e ordinariamente colhidos os dados, e o local em que a empresa controladora se faz presente. Órgãos de investigação desses países podem requisitar dados controlados por empresas que prestam serviços em seus territórios independentemente do local onde os dados estão fisicamente armazenados.

O uso do critério *controle/local de prestação do serviço* também tem sido reconhecido pela Jurisprudência dos países europeus.

No caso Licra – Ligue Contre le Racisme et l'Antisémitisme et Union des Édutiants Juifs de France v. Yahoo! Inc. et Société Yahoo! France, o Tribunal de Grande Instance expediu uma ordem determinando que a empresa Yahoo! tomasse todas as medidas necessárias a dissuadir e "tor-

19 O original afirma que: "[h]owever on the central point whether it had power to order production of documents by an Irish registered company by one of its branches situated in a foreign country, the Supreme Court found that it did. The Supreme Court found that the Taxes Consolidation Act empowers the Irish taxation authorities to seek an order that an Irish bank produce records of accounts held by its customers *wherever the information is situated*". O texto, em inglês, pode ser acessado em: <https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2014/09/Ireland-AmicusBrief.pdf>. Acesso em: 3 jul. 2018. (grifo nosso)

nar impossível" a visualização e venda de artigos nazistas na França.[20] O caso prosseguiu em litígio nos Estados Unidos, onde a Corte do Nono Circuito decidiu que Yahoo! não poderia utilizar a Primeira Emenda à Constituição Norte-Americana, que trata da liberdade de expressão, para descumprir a legislação francesa.[21] Em outras palavras, ambas as cortes reconheceram que uma empresa prestando serviços em um determinado país precisa obedecer à legislação desse país, mesmo que sua operação e seus servidores estejam localizados ou sediados em outro país.

Em outro caso envolvendo o Yahoo!, a Suprema Corte da Bélgica confirmou que se uma empresa presta serviços em território belga, ela precisa obedecer à lei local fornecendo todos os dados e documentos controlados por ela.[22] Interessante notar que a decisão não exigiu que a empresa tivesse sede ou subsidiária na Bélgica, mas apenas que ali prestasse serviços – à época, Yahoo! não possuía representantes na Bélgica e foi citada por *e-mail*.

Mais recentemente, a Corte Europeia de Justiça decidiu que um provedor estabelecido em um Estado Membro deve obedecer às diretrizes europeias, independentemente do local físico de seus equipamentos ou do local em que sua operação é mantida.[23] Em 14 de abril de 2016, a União Europeia aprovou como lei pacote de Proteção de Dados – Regulation (EU) 2016/679, conhecido pela sigla General Data Protection Regulation (GDPR) – que segue os mesmos critérios, estabelecendo a jurisdição dos Estados membros quanto à proteção de dados sobre empresas que prestam serviços em seus territórios ou são ali sediadas.[24]

---

20 WIKIPÉDIA. LICRA contre Yahoo! Disponível em: <https://fr.wikipedia.org/wiki/LICRA_contre_Yahoo!>. Acesso em: 3 jul. 2018.

21 Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme (433 F.3ed 1199).

22 GAV LAW – GEERT VAN CALSTER. It's true! Belgian Supreme Court confirms order for Yahoo! to hand over IP-addresses. Disponível em: <https://gavclaw.com/2015/12/07/its-true-belgian-supreme-court-confirms-order-for-yahoo-to-hand-over-ip-addresses/>. Acesso em: 3 jul. 2018.

23 COURT OF JUSTICE OF THE EUROPEAN UNION. An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties. Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf>. Acesso em: 3 jul. 2018.

24 O GDPR entrou em vigor em 25 de maio de 2018. Nos termos do artigo 3º. do Regulamento, as regras ali previstas aplicam-se a empresas europeias, ainda que as atividades de processamento sejam desenvolvidas em outros territórios (controle) e aos dados colhidos na União Europeia referentes a serviços ali prestados, ainda que as empresas estejam sediadas em outros países (critério da

Em resumo, países europeus, há mais de uma década, reconhecem o critério controle/prestação de serviço para a obtenção direta de provas eletrônicas, adotando-o em suas legislações e em decisões judiciais. Se uma empresa presta serviços ou está localizada em determinado país, ela precisa atender às requisições de documentos eletrônicos apresentadas legalmente pelos órgãos de investigação desse país, não importando onde esses documentos estão fisicamente armazenados, se no próprio Estado requisitante ou em outro local. Esse mesmo critério foi adotado pelo Marco Civil da Internet.

A LEGISLAÇÃO BRASILEIRA

O artigo 11 da Lei no. 12.965/2014, Marco Civil da Internet, estabelece que:

> Artigo 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e dos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Análise superficial do dispositivo pode levar à conclusão de que ele apenas reproduz o princípio territorial puro. Se a empresa presta serviços no Brasil, deve adequar-se à legislação brasileira, à legislação local, o que em si não contém nenhuma inovação.

Essa conclusão, porém, é equivocada, pois o dispositivo tem alcance muito maior do que a simples aplicação do princípio territorial. Em verdade, o artigo reflete posicionamento jurisprudencial, inclusive das cortes superiores, de que a empresa que presta serviços no país precisa cumprir a legislação nacional. A norma apenas deixa tal obrigação mais clara, determinando em seu § 2º., que a lei brasileira será aplicada "mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil". Assim, ainda que a operação da empresa ocorra toda no exterior, e ali sejam tomadas as decisões corporativas e mantidos os servidores que coletam e armazenam os dados necessários para a prestação dos serviços, deverá ser observada a legislação brasileira para os dados coletados no Brasil, inclusive quanto às requisições judicias descritas no artigo 10.

---

prestação de serviço). A íntegra do documento pode ser acessada em: EUR-LEX. Document 32016R0679. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC>. Acesso em: 3 jul. 2018.

Nesse contexto, as sucessivas negativas de provedores constituídos sob as leis brasileiras, mas com sede de operação em outros países em fornecer dados diretamente às autoridades brasileiras carecem de completo fundamento, quer na legislação nacional, quer na legislação internacional. Cada vez mais é irrelevante onde os dados são armazenados, restando apenas a questão de quem controla esses dados e onde o serviço é prestado.

Imperioso concluir, dessa forma, que a legislação brasileira, ainda que preservando certos aspectos do princípio territorial, também adotou o critério controle e nisso está em absoluta harmonia com a legislação europeia, em vigor – GDPR – e proposta – E-Evidence –, com a nova legislação norte-americana sancionada em março de 2018,[25] e com o Direito Internacional. Terá jurisdição para requisitar dados diretamente o Estado em que a empresa que controla os dados presta serviços, independentemente do local físico em que mantidos seus equipamentos e armazenados os documentos. A regra é controle, não localização.

E A PRIVACIDADE?

Questão frequente quando se debate o acesso transfronteiriço a dados e provas eletrônicas é a proteção da privacidade. O argumento é simples: permitir que qualquer país possa ter acesso a dados armazenados independentemente da localização física dos documentos pode abrir as portas para violações. O pensamento é: e se um país que não observa regras básicas do Estado Democrático de Direito exigir a entrega de documentos a empresa sediada ou mantida em país onde essas regras são seguidas, a empresa é obrigada a fornecê-los?

A adoção do critério controle conduz à resposta afirmativa: desde que preenchidos os requisitos básicos, a empresa deverá fornecer os dados. Isso, evidentemente, provoca inúmeras reações, pois parece violar nossas convicções mais íntimas sobre a aplicação e o respeito aos Direitos Humanos. Como podemos permitir uma violação a princípios que elegemos seguir em nosso próprio território? Entretanto, há mais camadas nessa discussão.

25 O CLOUD Act, além de outras disposições, introduziu o § 2713, que determina que provedores de comunicação eletrônica ou serviço informatizado remoto devem atender às ordens legalmente expedidas pelas autoridades norte-americanas referentes a dados sob seu controle, independente da localização. *In verbis*: CONGRESS.GOV. H.R.4943 - CLOUD Act. Disponível em: <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>. Acesso em: 3 jul. 2018. "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States".

Em primeiro lugar é importante lembrar que nem sempre o país que requisita as informações protege a privacidade de forma menos adequada, ou menos abrangente, do que aquele onde sediada a empresa que controla os dados. Um exemplo claro é a legislação brasileira. O artigo 22 do Marco Civil da Internet, estabelece que o acesso a dados de registro de conexão, incluindo aí dados de IP, depende de ordem judicial baseada em fundados indícios da ocorrência do ilícito e motivada com indicação da utilidade dos registros para fins de investigação. Os mesmos dados básicos de conexão, ou *subscriber information*, como registro de logs de acesso a IP, segundo a legislação norte-americana,[26] dependem apenas de requisição de autoridade – *subpoena* –, seja ela policial ou do Ministério Público, sendo desnecessário o controle judicial.

Em segundo lugar, deve-se ter em mente que as empresas prestadoras de serviços não são as guardiãs da proteção do direito à privacidade. Muito pelo contrário. Em muitas ocasiões, elas são as principais responsáveis por violações e abusos. Empresas visam lucro e, por vezes, na busca de seus objetivos, deixam de lado a proteção integral da intimidade, ainda que não a violem diretamente.[27] E não há nada de errado nisso. Entretanto, é sempre necessário ver com ceticismo a defesa incondicional do direito à privacidade por empresas privadas. Enquanto essa defesa atender aos seus próprios objetivos, as empresas serão aliadas; quando deixar de existir essa similaridade, a situação será outra. O melhor defensor do direito à privacidade é seu titular.

Em terceiro lugar, a entrada em vigor do GDPR, que prevê expressamente ampla aplicação da legislação e da jurisdição de países europeus sobre a proteção de dados para serviços prestados em território europeu, trouxe mudanças significativas na forma como os dados são tratados mesmo em países fora do bloco. Os efeitos completos da efetiva implementação das regras ainda precisarão ser estudados, mas parece desde já evidente que as empresas que prestam serviços globalmente acabarão seguindo as diretrizes europeias no resto do mundo. Isso demonstra que há uma certa convergência no Direito Internacional para aceitar os critérios de controle e prestação de serviços para a definição de jurisdição, tanto para proteção quanto para fornecimento de dados às autoridades.

---

26 18 U.S.C. § 2703(c)(2).

27 Os casos recentes envolvendo a rede social *Facebook*, a empresa *Cambridge Analytica* e as eleições norte-americanas, são apenas um exemplo de muitos. STATT, Nick. Federal investigators want to know if Facebook lied about Cambridge Analytica. Disponível em: <https://www.theverge.com/2018/7/2/17528610/federal-investigation-facebook-cambridge-analytica-doj-fbi-sec>. Acesso em: 3 jul. 2018.

Apesar dessas nuances, as preocupações são válidas. No entanto, elas podem ser amenizadas com o estabelecimento de limites para a obtenção das provas. A já citada *Guidance Note #10* traz alguns parâmetros que têm sido aceitos como norteadores do acesso transfronteiriço a dados. Um Estado poderá exigir esses dados desde que a empresa controladora preste serviços em seu território de algum modo direcionado a seus habitantes, o que se justifica porque a empresa, nesse caso, tem que atender às exigências do local onde executa o serviço, em situação análoga, por exemplo, a de um banco com matriz em outo país mas que, nem por isso, deixa de se submeter às autoridades reguladoras do local onde presta o serviço. Disposição semelhante está contida na proposta da Comissão Europeia sobre E-Evidence e de forma mais ampla, como já citado, no próprio GDPR.

Esses limites já encontram respaldo na legislação brasileira, no artigo 11 da Lei 12.965/2014 e nas regras de competência do Código Penal e do Código de Processo Penal. A possibilidade de acesso transfronteiriço a provas, assim, não significa violação indiscriminada de direitos, mas preservação da capacidade de investigação e de responsabilização de delitos cometidos em determinado território.

CONCLUSÃO: O FUTURO DO ACESSO A DADOS

O problema do acesso direto a dados e à prova eletrônica é urgente e afeta não apenas os crimes propriamente considerados cibernéticos, como a persecução penal de crimes comuns, mas com provas armazenadas em sistemas informáticos. O critério *controle*, aliado ao local da prestação de serviço, não é a única solução para esse problema, mas tem sido a mais adotado por legislações em todo o mundo.

Existem duas razões principais para a adoção do critério controle/local de prestação de serviço. A primeira delas é a realidade da prova eletrônica.

Dados e documentos eletrônicos são, por essência, *móveis*. Eles podem ser armazenados em qualquer lugar e também podem ser movimentados para qualquer lugar, a qualquer tempo, em questão de minutos, com um único clique. Eles podem ser movidos para o território de um Estado observador de obrigações internacionais, para *Sealand*[28] ou para o alto

28 WIKIPÉDIA. Principality of Sealand. Disponível em: <https://en.wikipedia.org/wiki/Principality_of_Sealand>. Acesso em: 3 jul. 2018.

mar.[29] Com frequência, é impossível determinar onde os dados estão fisicamente localizados – servidores que utilizam redes de anonimato como TOR 2 e i2p, por exemplo, ou nos casos de Content Delivery Networks –, ou mesmo autenticar a localização declarada – nem todos os servidores de aplicativos são transparentes quanto ao local de sua operação. A lei não pode ignorar a realidade e o único critério disponível hoje é controle.

Em segundo lugar, o critério controle/prestação de serviço preserva a territorialidade e a soberania dos Estados. Uma empresa não pode ser constituída, manter escritórios ou subsidiárias, ou prestar serviços em um país, dirigidos especificamente a seus residentes, sem se submeter à lei local. Do contrário, empresas não apenas poderiam escolher a jurisdição, como também a lei que as regula, escolhendo aquela que mais lhes favorece, não necessariamente aquela que melhor protege seus consumidores e usuários. Se é inconcebível que uma empresa possa prestar qualquer tipo de serviço físico sem obedecer à lei local, o mesmo é válido para empresas de internet. O modelo de negócios possui peculiaridades, mas não demanda tratamento preferencial.

De outro lado, a aplicação do critério controle com o norte definido pelo *Guidance Note #10* e com as regras previstas na proposta de E-Evidence, inclusive quanto à solução de conflito de normas, pode auxiliar na preservação do direito à privacidade. Restringe-se o acesso às situações em que o prestador de serviços direciona sua atividade aos habitantes do Estado requisitante e estes, cientes de sua própria legislação, também estarão cientes de que as empresas que lhes prestam serviços poderão ser compelidas a fornecer dados, conforme as regras locais. Esse critério dá segurança ao usuário, que não precisará se preocupar com a legislação de outros países para descobrir se seus dados estão ou não protegidos.

O atual quadro da legislação internacional apresenta desafios e o critério controle pode gerar distorções. Entretanto, ele é hoje o principal instrumento aceito internacionalmente e que, na prática, se mostra mais adequado às peculiaridades da prova eletrônica.

29 HRUSKA, Joel. Under the Sea: Microsoft testing underwater data centers. Extreme Tech, 1 fev. 2016. Disponível em: <http://www.extremetech.com/extreme/222251-under-the-sea-microsoft-testing-underwater-data-centers>. Acesso em: 3 jul. 2018.

REFERÊNCIAS

CONGRESS.GOV. H.R.4943 - CLOUD Act. Disponível em: <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>. Acesso em: 3 jul. 2018.

COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 185. Disponível em: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=VsTdZN6J>. Acesso em: 3 jul. 2018.

COUNCIL OF EUROPE. CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa428>. Acesso em: 3 jul. 2018.

COUNCIL OF EUROPE. T-CY Guidance Note #10. Production orders for subscriber information. (Article 18 Budapest Convention). Disponível em: <https://rm.coe.int/16806f943e>. Acesso em: 3 jul. 2018.

COURT OF JUSTICE OF THE EUROPEAN UNION. An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties. Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf>. Acesso em: 3 jul. 2018.

CYBERCRIME CONVENTION COMMITTEE. Transborder access and jurisdiction: What are the options? Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8>. Acesso em: 3 jul. 2018.

DEPARTMENT OF JUSTICE. Case 14-2985, Document 286-1, 07/14/2016, 1815361, Page1 of 43. Disponível em: <https://www.justice.gov/archives/opa/blog-entry/file/937006/download>. Acesso em: 3 jul. 2018.

EUR-LEX. Document 32016R0679. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC >. Acesso em: 3 jul. 2018.

EUR-LEX. Document 52018PC0225. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN>. Acesso em: 3 jul. 2018.

EUROPEAN COMMISSION. E-evidence - cross-border access to electronic evidence. Disponível em: <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en>. Acesso em 3 jul. 2018.

GAV LAW – GEERT VAN CALSTER. It's true! Belgian Supreme Court confirms order for Yahoo! to hand over IP-addresses. Disponível em: <https://gavclaw.com/2015/12/07/its-true-belgian-supreme-court-confirms-order-for-yahoo-to--hand-over-ip-addresses/>. Acesso em: 3 jul. 2018.

HOGAN LOVELLS. Hogan Lovells White Paper - Government access to Data in the Cloud. Disponível em: <https://www.hoganlovells.com/en/publications/hogan-lovells-white-paper-government-access-to-data-in-the-cloud>. Acesso em: 3 jul. 2018.

HRUSKA, Joel. Under the Sea: Microsoft testing underwater data centers. Extreme Tech, 1 fev. 2016. Disponível em: <http://www.extremetech.com/extreme/222251-under-the-sea-microsoft-testing-underwater-data-centers>. Acesso em: 3 jul. 2018.

KERR, Orin. 2nd Circuit denies rehearing in Microsoft Ireland case by an evenly divided vote. The Washington Post, 24 jan. 2017. Disponível em: <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/01/24/2nd-circuit-denies-rehearing-in-microsoft-ireland-case-by-an-evenly-divided-vote/?utm_term=.678da86781c8>. Acesso em: 3 jul. 2018.

STATT, Nick. Federal investigators want to know if Facebook lied about Cambridge Analytica. Disponível em: <https://www.theverge.com/2018/7/2/17528610/federal-investigation-facebook-cambridge-analytica-doj-fbi-sec>. Acesso em: 3 jul. 2018.

WIKIPEDIA. Content delivery network. Disponível em:<https://en.wikipedia.org/wiki/Content_delivery_network>. Acesso em: 3 jul. 2018.

WIKIPÉDIA. LICRA contre Yahoo! Disponível em: <https://fr.wikipedia.org/wiki/LICRA_contre_Yahoo!>. Acesso em: 3 jul. 2018.

WIKIPÉDIA. Principality of Sealand. Disponível em: <https://en.wikipedia.org/wiki/Principality_of_Sealand>. Acesso em: 3 jul. 2018.

IV

NEUTRALIDADE DE REDE: ACESSO, AUTONOMIA E INOVAÇÃO

A NEUTRALIDADE DA REDE: NORMA FUNDAMENTAL PARA A PROTEÇÃO DA EXPRESSÃO E DO EMPREENDEDORISMO NA INTERNET[1]

LUCA BELLI

INTRODUÇÃO

Durante os últimos quinze anos de debate sobre neutralidade da rede (NR)[2] (LEMLEY, M.; LESSIG, L., 2000; WU, T., 2003) este princípio tem sido profundamente analisado em todo o mundo, desencadeando debates intensos e polarizando as opiniões de múltiplos atores tanto no Brasil como ao nível internacional. Apesar da existência de várias definições da NR, cabe destacar que todas as formulações convergem na consideração da NR como um princípio de não discriminação cujo objetivo é preservar uma Internet aberta e de finalidade geral, facilitando a participação ativa do usuário bem como o pleno gozo dos direitos fundamentais de todos os internautas. Como argumentarei neste artigo, a NR não simplesmente baseada em direitos fundamentais existentes, mas, além disso, torna-se uma verdadeira norma de direito internacional a fim cujo papel é a garantia da liberdade de expressão e de inovação na era da Internet. Neste sentido, a NR tem sido consagrada em diversos instrumentos normativos ao nível nacional bem como internacional.

---

1 Este capítulo foi submetido em junho de 2017. Uma análise mais atualizada das práticas de Zero Rating no Brasil foi publicada pelo autor em: OBSERVATÓRIO DO MARCO CIVIL DA INTERNET. Neutralidade de rede e ordem econômica. Disponível em: <http://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economica/>. Acesso em: 20 dez. 2018. Mais informações sobre Zero Rating, coordenado pelo autor confira em: ZERO RATING. Disponível em:<www.zerorating.info>. Acesso em: 12 nov. 2017.

2 O debate sobre as práticas discriminatórias das operadoras foi aberto para os professores Mark Lemley e Lawrence Lessig em 2000. Todavia, o conceito de neutralidade da rede foi criado pelo professor Tim Wu em 2003.

No Brasil, a NR se encontra explicitamente protegida pela Lei 12.965/2014, mais conhecida como o Marco Civil da Internet (MCI), que regula o uso da Internet no Brasil, estabelecendo princípios e regras fundamentais, entre as quais figura com prominência a NR. Nomeadamente, após ter reconhecido a neutralidade como um dos princípios que disciplinam o uso da Internet no Brasil no artigo 3°, o MCI torna o princípio da NR em uma obrigação do provedor de acesso à Internet, afirmando no artigo 9° – Da Neutralidade da Rede – que:

> O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

Como destacarei na segunda parte desse artigo, o debate sobre a NR influenciou fortemente a elaboração do MCI e do decreto n°8771 de 2016 que regulamenta o MCI. Particularmente, o debate voltou a ser extremamente inflamado no momento da discussão da (in)compatibilidade entre o tratamento não discriminatório e as práticas de patrocínio de aplicativos, conhecidas como *zero-rating* (ZR), baseadas no patrocínio do acesso a determinadas aplicações cuja consumação de dados não é descontada das franquias mensais dos usuários (BELLI, 2016). Além de permitir aos cidadãos e aos *policy-makers* brasileiros de recoltar as informações essenciais para formar a sua própria opinião sobre o assunto, os debates públicos sobre MCI e NR foram particularmente úteis a fim de identificar com clareza os interesses em jogo, evidenciando uma clara oposição entre, de um lado, as operadoras e uns produtores de equipamentos cujo interesse é prevalentemente em oposição à NR, e de outro lado a maioria dos sujeitos interessados, em favor da definição de garantias solidas de NR (BRITO CRUZ; MARCHESAN; SANTOS, 2015).

O propósito do presente artigo é contextualizar o debate sobre a NR a fim de explicar o raciocínio, a necessidade e a utilidade das políticas públicas e das regulações recentemente desenvolvidas ao nível global bem como no Brasil. *In primis,* o artigo examinará os fundamentos da NR, destacando que as bases conceptuais da NR podem encontrar-se nas normas de direito internacional sobre a proteção dos direitos humanos (BELLI, 2016). Em consequência, fornecerei uma visão geral da evolução do debate a fim de ressaltar uma migração intercontinental das discussões e da elaboração de políticas e regulações de NR. *In secundis*, a análise se concertará em torno da disciplina brasileira da NR (DEL CAMPO, 2017). Analisando o MCI e sua função de lei principiológica apta a promover o pleno exercício da cidadania e o acesso universal e, mais geralmente, os direitos fundamentais do indivíduo, destacarei que o mesmo MCI

considera a neutralidade da rede como um de seus pilares fundamentais que permitem a realização dos objetivos constitucionais supracitados. Particularmente, a Constituição Brasileira de 1988, nos incisos IV e IX do artigo 5º dispõe que "é livre a manifestação do pensamento, sendo vedado o anonimato" e que "é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença". Como ressaltarei na primeira seção desse artigo, o objetivo do princípio de NR é a preservação do paradigma aberto e distribuído que permitiu à Internet de expandir as fronteiras da liberdade na produção, difusão e recepção de informações e ideias, revolucionando os espaços e as dinâmicas de colaboração e troca de conhecimentos. Tal paradigma é totalmente diferente do paradigma centralizado e hierarquicamente estruturado que caracteriza a mídia tradicional. Então, o objetivo precípuo da NR é evitar que a Internet seja centralizada e transformada em uma mídia tradicional em razão das práticas implementadas pelas operadoras.

Por último, analisarei brevemente o assunto espinhoso do ZR, destacando que a maioria dos planos de ZR oferecidos até então no Brasil tendem a reduzir a abertura da Internet, já que restringem *de facto* o uso da Internet a um número limitado de aplicações patrocinadas. Este tipo de restrição é particularmente relevante para os indivíduos cuja capacidade econômica é mais limitada e, consequentemente, cuja possibilidade de comprar acesso irrestrito à Internet se torna mais difícil. Além disso, destacarei que a combinação de uma franquia limitada de dados – elemento de escassez essencial a fim de manter o patrocínio conveniente pelos consumidores – e de serviços patrocinados pode transformar a Internet em uma rede cujo objetivo é predefinido pelas operadoras. Ao invés de manter a qualidade essencial da Internet como rede de finalidade geral, que cada usuário é livre de utilizar de qualquer maneira, a combinação de franquias limitadas e serviços patrocinados torna os usuários em meros consumidores de aplicativos patrocinados pré-selecionados para terceiros. Tal paradigma é susceptível de aniquilar a peculiar característica dos internautas como "prosumidores", sendo simultaneamente consumidores e produtores de informação, ideias e inovação.

ELEMENTOS DE CONVERGÊNCIAS NO DEBATE SOBRE A NEUTRALIDADE DA REDE

Por mais que tenham sido propostas diversas nuances da NR, a maioria dos atores concordam com a sua essência, definindo-a como "o princípio segundo o qual todo o tráfego da internet deve ser tratado, sem discriminação, restrição ou interferência não razoável, independentemente de seu

emissor, receptor, tipo, conteúdo, dispositivo, serviço ou aplicação".[3] No entanto, existe um grande debate sobre a execução concreta do princípio, alimentando controvérsias em relação ao que deveria ser considerada uma discriminação "razoável" do tráfego Internet. Neste sentido, as controvérsias sobre a NR se concentram no grau de liberdade que os operadores de redes devem ter para implementar as técnicas de gestão do tráfego de Internet (GTI), que podem "discriminar" em favor ou contra conteúdo ou aplicativos específicos que transitem em suas redes eletrônicas. Embora possa parecer um problema puramente técnico, a definição das práticas de GTI acarreta grandes implicações sociais, jurídicas e econômicas. Na realidade, a implementação de um tratamento diferenciado mediante técnicas de GTI abusivas pode limitar excessivamente a liberdade de expressão ou a privacidade dos usuários ou reduzir a concorrência, quando tais medidas não sejam necessárias e proporcionais para o cumprimento de um objetivo legítimo (BELLI; VAN BERGEN, 2013).[4]

O debate sobre a neutralidade da rede tornou-se especialmente relevante, já que as técnicas de GTI podem não apenas ser utilizadas para um propósito legítimo, mas também para prejudicar os serviços concorrentes, bloqueando-os ou degradando-os indevidamente, ou para favorecer a parceiros comerciais através de priorização.[5] Tais limitações indevidas são possíveis diante da ausência de políticas de neutralidade de rede e já foram demonstradas em uma variedade de contextos nacionais, como nos

---

3 Internet Governance Forum (IGF), "Policy Statement on Network Neutrality", resultados do XV Fórum das Nações Unidas sobre Governança da Internet, novembro, 2015, § 1. INTERNET GOVERNANCE FORUM. Disponível em: <http://bit.ly/2qbKqDX>. Acesso em: 12 nov. 2017.

4 Além de Federal Communications Commission (FCC). Report and Order on Remand, Declaratory Ruling, and Order on the Matter of Protecting and Promoting the Open Internet. GN Docket No. 14-28. 2015; e Conselho da Europa (CoE), Recomendação CM/Rec 1 do Comitê de Ministros aos Estados Membros sobre a Proteção e Promoção do Direito à Liberdade de Expressão e do Direito à Intimidade Respeito da Neutralidade da Rede, janeiro, 2016. COUNCIL OF EUROPE. Recommendation CM/Rec (2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality. Disponível em: <http://bit.ly/2f8FlWS>. Acesso em: 20 dez. 2018.

5 Veja Body of European Regulators for Electronic Communications (BEREC), "A View of Traffic Management and other Practices Resulting in Restrictions to the Open Internet in Europe", In.: Findings from BEREC's and the European Commission's Joint Investigation, *BoR* (12) 30, 29 de maio de 2012; e FCC, supra nota 7.

Estados Unidos,[6] Chile[7] ou na União Europeia,[8] impulsando a criação de marcos para a neutralidade da rede.

É importante mencionar que a GTI tem um papel fundamental para garantir o correto funcionamento das redes eletrônicas, por exemplo, ao preservar a segurança e integridade das redes. No entanto, é possível que os operadores usem as técnicas de GTI em má fé para favorecer ou prejudicar aplicativos e conteúdo específicos, baseados em considerações meramente comerciais. De fato, nos últimos quinze anos foram desenvolvidas técnicas de GTI que permitem a identificação e discriminação de aplicações e conteúdo específicos, que podem ser utilizadas para obstruir a difusão e o uso de aplicativos que estão em concorrência direta com os serviços oferecidos pelas operadoras, tais como aplicativos de *Voice over IP* como Skype que competem diretamente com ligações e mensagens, ou as aplicações que competem com os parceiros comerciais dos operadores. Neste sentido, o fenômeno crescente da integração vertical (BELLI L.; DE FILIPPI P. (2015)[9] entre os operadores de redes e os provedores de conteúdo e aplicações (PCA) oferece incentivos concretos para as operadoras privilegiar o tráfego dos parceiros comerciais, mediante a priorização paga,[10] o bloqueio ou a degradação[11] dos serviços concorrentes. Assim, embora as várias técnicas de GTI possam oferecer benefícios, vale

---

6 Federal Communications Commission (FCC), Madison River Communications, LLC and affiliated companies, Acct. Nº FRN: 0004334082, Washington D.C., 2005. Disponível em: <http://bit.ly/2f8Dul1>; Federal Communications Commission (FCC), "Commission Orders Comcast to End Discriminatory Network Management Practices", FCC News Media Information 202/418-0500, 1º de agosto de 2008. Disponível em: <http://bit.ly/2cpWlsb>. Acesso em: 12 nov. 2017.

7 Tribunal de Defesa da Livre Concorrência (TDLC), "Voissnet vs. CTC", sentença 45, outubro de 2006.

8 BEREC, supra nota 8.

9 A integração vertical é o processo de agregação de dois ou mais entidades, consideradas como elos de uma cadeia de valor. A integração vertical entre provedoras de acesso à Internet e provedores de conteúdo ou aplicativo tem gerado preocupações na medida em que as operadoras verticalmente integradas poderiam privilegiar o tráfego dos provedores integrados. Ver também BEREC, supra nota 8; FCC, supra nota 7.

10 A priorização paga faz referência à prática de outorgar um tratamento preferencial ao fluxo de dados dos parceiros comerciais dos operadores. Esta prática tem sido criticada por seu potencial de criar "vias rápidas" e "rotas sujas" na Internet, favorecendo os sócios comerciais e prejudicando aqueles serviços que carecem da capacidade financeira necessária para pagar por prioridade.

11 O objetivo desta prática é de limitar especificamente as velocidades de upload e download de determinados tipos de fluxo de dados.

ressaltar que a GTI também pode ser utilizada com propósitos abusivos que só beneficiam um espectro muito limitado dos atores da Internet, ou seja, os operadores e seus sócios comerciais.

As práticas indevidas de GTI podem trazer consequências nefastas não apenas para a livre concorrência, mas também para a liberdade dos usuários de buscar, transmitir e receber informações sem interferência, princípio que se encontra garantido não somente pelo direito internacional, mas também pela maioria das Constituições em vigor. Todavia, cabe ressaltar que o tratamento não discriminatório imposto pela NR possui exceções, da mesma medida em quem a liberdade de expressão, apesar de ser um direito fundamental, pode ser sujeita à restrições. Embora seja certo que a gestão do tráfego discriminatório tem seus benefícios quando é necessária e proporcional para o cumprimento de propósitos legítimos,[12] o problema é até que ponto possam-se considerar as práticas de gestão de tráfego como legítimas, necessárias e proporcionais.

Neste sentido, cabe mencionar que, embora existam pontos de vista divergentes em relação à GTI, em geral, os atores concordam que a gestão de tráfego discriminatória pode ser considerada razoável sempre e quando seja necessária e proporcional para o cumprimento de alguns propósitos específicos. Particularmente, a GTI é geralmente considerada como razoável para fins de segurança e integridade da rede – por exemplo, para lidar com o uso malicioso da Internet, como o *spam* ou os ataques cibernéticos – ou para priorizar os serviços de emergência, em caso de força maior, ou quando a priorização de protocolos específicos (BASTIAN *et al*., 2010)[13] torna-se necessária a fim de mitigar os efeitos do congestionamento (FRIEDEN, 2014).[14]

12 BEREC, *supra* nota 4; FCC, *supra* nota 3; IGF, *supra* nota 2.

13 A expressão "protocolo específico" descreve uma técnica de GTI que se dirige a uma classe de aplicações que se baseam-se na exploração do mesmo protocolo, tal como os aplicativos de voz sobre IP. A diferença da GTI que discrimina aplicações específicas, a GTI de "protocolos específicos" aponta a toda uma classe de aplicações que exploram o mesmo protocolo. A GTI de "protocolo específico" se opõe à GTI independente de protocolo, dita *"protocol agnostic"* que não se dirige ou afeta a nenhuma classe específica de aplicações.

14 Cabe destacar que a identificação da existência de congestionamento nas redes não é tão simples como poderia parecer. Na realidade, resulta particularmente difícil identificar de modo objetivo a verdadeira causa do congestionamento e, como afirma Frieden, "a verdadeira causa do congestionamento (…) permanece indescritível. Os provedores de conteúdo especulam se as operadoras causam o congestionamento deliberadamente, ao negar-se a otimizar a capacidade da rede [e as] operadoras negam este cenário e afirmam que a congestão seja causada para circunstâncias como o clima, férias em casa e a decisão dos distribuidores de conteúdo, como Netflix, de lançar novas temporadas".

Além disso, o uso de redes de distribuição de conteúdo (PALLIS; VAKALI, 2016)[15] – CDN, segundo sua sigla em inglês –, geralmente, se considera compatível com a NR, já que tais redes melhoram o rendimento dos aplicativos e diminuem o congestionamento sem necessidade de implementar um tratamento discriminatório.[16]

Como foi evidenciado nesta seção, as técnicas de GTI podem ser empregadas para garantir o correto funcionamento da Internet, mas também para favorecer ou degradar conteúdo ou aplicativos específicos, ante ao total desconhecimento dos usuários finais. Neste sentido, várias empresas de Internet têm destacado que, além de estar motivadas a discriminar o tráfego dos competidores, as operadoras de redes verticalmente integradas têm a capacidade para ocultar suas ações.[17] Assim, é particularmente importante ressaltar a relevância da transparência no gerenciamento do trafego Internet, além da necessidade, da proporcionalidade e da legitimidade das medidas de gerenciamento.

UMA GESTÃO DE TRÁFEGO DE INTERNET CONFORME AOS DIREITOS HUMANOS

A GTI discriminatória pode ser utilizada para fins anticoncorrenciais, mas também pode minar a liberdade de expressão dos usuários. A visão tradicional da liberdade de expressão como direito fundamental implicante uma obrigação negativa do Estado, ou seja, implica o dever de abstenção do Estado, que não pode impedir nem coibir a manifestação de opiniões e ideias. Tal visão necessita ser complementada com uma visão da liberdade

15 As CDN são redes que atuam como intermediários entre a fonte de um provedor de aplicações e a operadora, com o objetivo de acelerar a transmissão dos dados. As CDN exploram práticas de hospedagem local e de cópia dos dados fornecido para um provedor especifico a fim que, quando o usuário necessita de acessar os dados, a CDN intercepta seu pedido e envia os dados desde o servidor de hospedagem mais próximo do usuário em vez de enviá-los desde a fonte remota. Assim, as CDN melhoram o rendimento encurtando a distância total que os dados devem percorrer para chegar a seu destino.

16 BEREC, *supra* nota 4; FCC, *supra* nota 3.

17 Internet Association. (2014) Comments of the Internet Association in response to the Federal Communications Commission's ("Commission" or "FCC") May 15, 2014 Notice of Proposed Rulemaking ("NPRM" or "Notice"), GN Docket No. 14-28. INTERNET ASSOCIATION. Before the FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554. Disponível em: <http://internetassociation.org/wp-content/uploads/2014/07/Comments.pdf>. Acesso em: 12 nov. 2017.

de expressão que implica uma obrigação positiva do Estado de permitir a livre procura, recepção e difusão de informações e ideias, protegendo os indivíduos de "qualquer ato perpetrado para pessoas ou entidades privadas".[18] Neste sentido, no âmbito internacional, os Estados possuem a obrigação negativa de não interferir no direito das pessoas de buscar, transmitir e receber informações e ideias livremente, e também possuem a obrigação positiva de proteger as pessoas dos efeitos adversos que as empresas privadas e outros indivíduos podem produzir em suas liberdades.

Tal visão é corroborada pela a jurisprudência da Corte Interamericana de Direitos Humanos (Corte IDH) e o Tribunal Europeu de Direitos Humanos (TEDH), que interpretam a liberdade de expressão como fundamento do tratamento não discriminatório da informação e das ideias. Assim, a Corte IDH estabelece que "a igualdade deve regular o fluxo da informação" e enfatiza que o Estado possui a obrigação positiva de "estender as regras de igualdade ao maior grau possível, para permitir a participação das distintas informações no debate público, impulsionando o pluralismo informativo".[19] Por outro lado, o TEDH tem expressado continuamente que a liberdade de expressão "se aplica não apenas ao conteúdo da informação, mas também ao meio de disseminação, já que qualquer restrição imposta necessariamente interferirá com o direito de receber ou transmitir informação".[20] Tais considerações também tem sido reiteradas pelos relatores especiais

---

18 Ver: Comitê de Direitos Humanos das Nações Unidas, "A natureza da obrigação jurídica geral imposta aos Estados membros no Pacto", Observação geral No. 31, Reunião No. 2187, 29 de março, 2004. Ver: <http://www.unhcr.org/4963237716.pdf>; Conselho da Europa. (2014). Recommendation CM/Rec (2014) 6 of the Committee of Ministers to member States on a guide to human rights for Internet users. Conselho da Europa. (2014). The Rule of Law on the Internet and in the Wider Digital World. Issue paper published by the Council of Europe Commissioner for Human Rights; Tribunal Europeu de Direitos Humanos, *"López Ostra v. Spain",* Sentença Nº 16798/90, §44-58, 9 de dezembro de 1994; Tribunal Europeu de Direitos Humanos, "*Khurshid Mustafa and Tarzibachi v. Sweden",* Judgment Nº 23883/06, 16 de dezembro de 2008.

19 Corte IDH, *"Kimel vs. Argentina",* sentença de 2 de maio de 2008, Fondo, reparações e custas, Serie C, No. 177, § 57; Corte IDH, *"Fontevecchia y D'Amico vs. Argentina",* sentença de 29 de novembro de 2011, Fondo, reparaciones y costas, Serie C Nº. 238, § 45.

20 Tribunal Europeu de Direitos Humanos, (TEDH). EUROPEAN COURT OF HUMAN RIGHTS. "Autronic AG v. Switzerland", 22 Mai 1990. Sentença Nº 12726/87. Disponível em: <http://hudoc.echr.coe.int/eng?i=001-57630>. Acesso em: 21 dez. 2018; TEDH (2012).. EUROPEAN COURT OF HUMAN RIGHTS. "Ahmet Yıldırım v. Turkey". Sentença Nº. 3111/10. Disponível em: <http://hudoc.echr.coe.int/fre?i=001-115705>. Acesso em: 21 dez. 2018.

para liberdade de expressão da ONU, da OEA da OSCE e da CADHP, que já enfatizaram que "o tratamento dos dados e o tráfego de internet não devem ser objeto de nenhum tipo de discriminação em função de fatores como dispositivos, conteúdos, autor, origem e/ou destino do material, serviço ou aplicação" (LARUE; MIJATOVIC; MARINO; TLAKULA, 2011).

Em razão da jurisprudência e dos relatórios mencionados no parágrafo precedente, os governos europeus têm consagrado a NR em uma Recomendação do Comitê de Ministros[21] do Conselho da Europa que explicita a natureza de norma internacional de direitos humanos da NR. De fato, os 47 membros do Conselho da Europa retiraram o compromisso com a NR, já abertamente previsto na Declaração do Comitê de Ministros sobre a Neutralidade da Rede de 2010.[22] Tais compromissos surgem a partir da observação de que o acesso não discriminatório e a circulação de conteúdo, aplicações e serviços não apenas facilitam o livre intercâmbio de informação, mas também contribui para reduzir as barreiras para ingressar no mercado de criatividade e inovação, de fato maximizando o interesse público. Neste sentido, é importante reiterar que, no ambiente *on-line*, a liberdade de receber e transmitir ideias significa a liberdade de acessar e difundir inovação, contribuindo ativamente na evolução da Internet. Como destaquei precedentemente, os usuários de Internet se caracterizam por serem "prosumidores", sendo não apenas consumidores de informação, mas também são produtores de inovações potencialmente disruptivas. Assim, ao reduzir a possibilidade de os operadores de interferir na liberdade de expressão dos usuários, a NR quer preservar a capacidade dos usuários a serem criadores e desenvolvedores da inovação e oferecerem novas aplicações e serviços potencialmente disruptivos, competindo livremente com os atores de mercado já estabelecidos.

---

21 Conselho da Europa. (2016). Recomendação CM/Rec (2016) 1 do Comitê de Ministros aos Estados Membros, sobre a proteção e promoção do direito à liberdade de expressão e o direito à vida privada, em relação à neutralidade de rede.Conselho da Europa. (2016).

No original: "Recommendation CM/Rec (2016) 1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality".

22 Conselho da Europa. (2010). Declaration of the Committee of Ministers on Network Neutrality. Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies. Ver: <http://bit.ly/2hAI4dx>. Acesso em: 12 nov. 2017.

Neste sentido, é muito importante destacar que parece errado afirmar que as políticas de NR estejam em conflito com os interesses do setor privado, segundo argumentam alguns opositores da NR.[23] Ao contrário, vale ressaltar que os opositores da NR se concentram particularmente no setor das telecomunicações que, mesmo sendo um componente importante do setor privado não é sinônimo de setor privado. E compreensível que uns operadores oponham à NR, afirmando que a regulação da NR impediria a implementação de novos modelos comerciais, como a "priorização paga" (WU; YOO, 2007). Todavia, em geral, um amplo espectro de atores comerciais, tais que provedores de conteúdo e aplicações e os inovadores, respaldam as políticas de NR sem as quais as operadoras assumiriam uma posição de controladores das redes. Assim, as empresas incipientes ou *startups* bem como as empresas já estabelecidas no mercado tem exigido a proteção do princípio de NR e coalizara-se para suportar o princípio de não discriminação nos diversos países onde políticas de NR foram debatidas.[24]

DISCRIMINAÇÃO INDEVIDA OU RESPOSTA À EVOLUÇÃO DOS PADRÕES DE CONSUMO?

Devido à evolução dos padrões de consumo da internet (OU, 2008),[25] em particular a difusão de vídeo e jogos *on-line*, as operadoras têm afirmado sua vontade de usar a GTI para diferenciar o tráfego (GROSSMAN, 2002;

---

23 Ver http: <//bit.ly/2qp06Xr>. Acesso em: 12 nov. 2017.

24 Por exemplo, na UE, as *startups* estabeleceram a iniciativa *"start-ups for net neutrality"*, também replicada no Brasil. Ver: ENGINE. STARTUPS FOR NET NEUTRALITY. Disponível em: <http://www.engine.is/startups-for-net-neutrality>. Acesso em: 12 nov. 2017; e NEUTRALIDADE NO MARCO CIVIL. Disponível em: <http://www.startupspelaneutralidadedarede.com/>. Acesso em: 12 nov. 2017. Na Índia quase 700 fundadores de startups solicitaram ao primeiro ministro Modi que defendesse a neutralidade da rede. Ver: GADGETS NOW. Nearly 700 startup founders urge PM Modi to defend net neutrality. <http://timesofindia.indiatimes.com/tech/tech-news/Nearly-700-startup-founders-urge-PM-Modi-to-defend-net-neutrality/articleshow/50729785.cms>. Acesso em: 12 nov. 2017.

25 Enquanto na década de 1990 o tráfego da internet consistia, majoritariamente, em intercâmbio de correio eletrônico, os anos 2000 testemunharam a difusão de aplicações de *peer-to-peer* que geraram um maior consumo de internet banda larga, enquanto a difusão de voz sobre IP, de streaming de video e dos jogos com múltiplos jogadores conectados, generalizaram o uso de aplicações sensíveis à latência.

BAKER; POLK; M. DOLLY, 2010; ROSEN, *et al*, 2011)[26] e propor esquemas de pagamento de prioridade, para apoiar o investimento (FELTEN, 2013)[27] que permitiria a expansão da capacidade da rede (BELLO; JUNG, 2015). O crescimento recente do *streaming* de vídeo tem exigido esforços econômicos para gerenciar a crescente demanda de tráfego (OECD, 2014), pressionando, assim, os operadores a propor um uso extensivo da GTI para diferenciar os níveis de qualidade e de preço a fim de maximizar os recursos necessários para suportar os investimentos. Neste sentido, várias operadoras sugeriram a necessidade de tarifas adicionais, além das tarifas de acesso à Internet já existentes, dado que, os esquemas de pagamento de prioridade, permitiriam de obter receitas adicionais que poderia ser investida na melhoria da rede. Embora seja verdade que as políticas de NR impedem os operadores de obter as receitas adicionais que seriam determinadas para o pagamento de prioridade, parece pouco realista dizer que tais receitas adicionais levariam automaticamente a um maior investimento em infraestrutura, ou supor que os operadores investiriam mais em infraestrutura diante da ausência de disposições de NR. Nesta perspectiva, cabe ressaltar que a existência de maior lucro não implica maiores investimentos. Assim, apesar do lucro líquido ter crescido 179%[28] durante o primeiro trimestre de 2016, a Telefônica Brasil diminuiu os

26 A diferenciação do tráfego se baseia no uso de qualquer técnica de GTI "que classifique e aplique um tratamento potencialmente diferente a dois ou mais fluxos de tráfego que disputam recursos em uma rede (entenda-se por fluxo um grupo de pacotes que compartilham um conjunto de propriedades em comum)." BITAG. (2015). "Differentiated Treatment of Internet Traffic." Ver: BROADBAND INTERNET TECHNICAL ADVISORY GROUP. Differentiated Treatment of Internet Traffic. Disponível em: <http://www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf>. Acesso em: 12 nov. 2017. A diferenciação se baseia na exploração de múltiplas classes de tráfego, que podem ter distintos níveis de prioridade e podem ser implementadas utilizando os protocolos de serviços diferenciados (DissServ), serviços integrados (IntServ) ou *multiprotocol label switching* (comutação de etiquetas multiprotocolo).

27 É importante mencionar que as operadoras não são os únicos atores econômicos que enfrentam custos e investimentos relevantes. Neste sentido, não se deve considerar que os PCA se aproveitam abusivamente da infraestrutura dos operadores, uma vez que enfrentam significativos custos recorrentes e consideráveis investimentos para aproximar o tráfego tanto quanto seja possível dos usuários finais.

28 Cf.: FÓRUM VIVO. Telefônica insistirá na franquia em banda larga fixa. Disponível em: <http://vivo.tl/2eVKTGF>. Acesso em: 12 nov. 2017.

seus investimentos[29] e apoiou abertamente a introdução de franquias de dados dentro de redes fixas no Brasil, considerando as franquias como uma medida necessária para estimular o investimento.[30]

Além disso, ao analisar a necessidade dos modelos de pagamento de prioridade para financiar os investimentos em redes, é importante destacar que os usuários já pagam pelo acesso à Internet e legitimamente esperam a possibilidade de acessar e receber o conteúdo e as aplicações pelas quais pagam o acesso. A razão pela qual os usuários compram acesso à Internet é a possibilidade de acessar, criar e compartilhar qualquer tipo de conteúdo e aplicações de sua escolha, que são a verdadeira *raison d'être* da Internet (CLARK; BLUMENTHAL, 2011). Neste sentido, a NR se propõe a evitar que as operadoras imponham um duplo preço na Internet, aplicando uma tarifa adicional que favoreça os serviços verticalmente integrados pela operadora e desfavoreça o acesso à conteúdo e aplicativos que não gozam de uma relação comercial com os operadores (ECONOMIDES; TÅG, 2012). Deste modo, basear a discriminação de conteúdo e aplicações em critérios puramente comerciais põe em perigo os fundamentos conceptuais da Internet, é dizer, prover uma plataforma aberta de uso geral para a comunicação e a inovação. Este último aspecto resulta de grande importância porque o GTI não discriminatório permite a todos os usuários o pleno gozo da qualidade de prosumidores e principalmente, porque a maioria dos atores dentro do ecossistema da Internet não são operadores de redes, mas serviços *on-line* – com ou sem fins de lucro –, *startups* ou empresas comuns que tem presença na Internet. Com a exceção dos maiores *players* do mercado, a maioria dos atores da Internet não teria capacidade financeira para pagar esquemas de priorização, ou patrocinar o acesso ao próprio serviço por meio de *zero-rating*, como veremos no item seguinte. Por isso, os defensores da NR têm se unido, exigindo sólidas garantias contra tratamento discriminatório. Neste sentido, em vários países, as *startups*, empresas e gigantes tecnológicos tem respaldado abertamente o conceito de que "preservar a neutralidade da rede garantirá que a Internet se mantenha como um motor para o crescimento econômico, a inovação e os valores democráticos".[31]

---

29 Cf.: BUCCO, Rafael. LUCRO DA TELEFÔNICA BRASIL CRESCE 179% NO PRIMEIRO TRIMESTRE. Disponível em: <http://bit.ly/2evInbv>. Acesso em: 12 nov. 2017.

30 Ver: HIRATA, Lucas. Para presidente da Telefônica, é 'injusto' usar menos dados pelo mesmo preço. Disponível em: <http://bit.ly/2p2H2cL>. Acesso em: 12 nov. 2017.

31 Internet Association, *supra* nota 20.

Muitas das preocupações que surgiram na última década nos debates sobre a neutralidade da rede e GTI discriminatória, voltam a ressurgir ultimamente em relação ao fenômeno do ZR. De fato, as políticas de NR foram adaptadas com o fim de evitar que as decisões dos operadores gerassem um desequilíbrio no ecossistema Internet, colocando em risco o pleno gozo dos direitos dos usuários e limitando a abertura da Internet. Por essa razão, podemos constatar uma justaposição quase perfeita entre o debate sobre NR contra discriminação e o debate sobre NR contra ZR. Na verdade, os oponentes do ZR coincidem em grande medida com os oponentes da discriminação de trafego, enquanto que os que suportam a liberdade de gestão de trafego e as práticas de ZR são geralmente operadoras juntas com um grupo muito limitado de *stakeholders* (BRITO CRUZ; MARCHESAN; SANTOS, 2015). Na próxima seção discutirei brevemente a disciplina da NR no MCI a e, subsequentemente, estudarei a compatibilidade dos modelos de ZR com a NR avelhando alguns dos custos e benefícios de tais práticas.

A REGULAÇÃO DA NEUTRALIDADE DA REDE E DO ZERO-RATING NO BRASIL

Apesar de sua categoria de lei ordinária, o MCI tem sido considerado como a "Constituição da Internet do Brasil" (CGI.br, 2014),[32] uma vez que define os elementos fundacionais da disciplina da Internet na União, como também sua clara intenção de proteger os direitos e liberdades fundamentais *on-line*. Cabe destacar, também, que o ex-presidente Luiz Inácio Lula da Silva promoveu o MCI com o compromisso de desenvolver um "marco de direitos civis para a internet" (COELHO, 2009) e recebeu um forte respaldo da ex-presidente Dilma Rousseff que, em resposta às revelações por parte do informante Edward Snowden, turbinou o processo de finalização do MCI a fim de consagrar fortes garantias dos direitos humanos no ambiente *on-line*. Portanto, o MCI foi o resultado da combinação de democracia participativa e a firme vontade política de proteger os direitos dos usuários. Neste sentido, o relator do MCI na Câmara dos Deputados, o Deputado Alessando Moron, argumentou que a neutralidade da rede é um direito fundamental e a pedra angular da democracia, que permite aos

32 O MCI é considerado o ícone internacional da democracia participativa devido ao processo de consulta on-line que levou à sua criação. O processo de abertura e colaboração que conduziu a criação do MCI se iniciou e se orquestrou conjuntamente com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas junto com o Ministério da Justiça do Brasil.

indivíduos ter acesso a uma pluralidade de fontes de informação.[33] Deste modo, a consagração da NR na legislação brasileira marca o entendimento do legislador de que o tratamento não discriminatório do tráfego de Internet tornou-se um requisito prévio fundamental para alcançar democracias que funcionem corretamente, impulsionadas pela pluralidade de informações, ideias, opiniões e pela inovação irrestrita.

A EVOLUÇÃO DA NEUTRALIDADE DA REDE NO BRASIL

É importante destacar que a NR é defendida no Brasil desde 2009, quando o Comitê Gestor de Internet do Brasil (CGI.br) incorporou-a em seu Decálogo de princípios fundamentais da governança da internet (CGI.br, 2009). Nomeadamente, a prescrição do Decálogo, segundo a qual "filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento" (CGI.br, 2009), foi reformulada repetidas vezes durante o processo de elaboração do MCI (RAMOS, 2015), até ser aprovada sua versão final em abril de 2014. Finalmente, a NR se consagrou no MCI que incluiu explicitamente a neutralidade da rede entre os princípios que definem "a disciplina do uso da internet no Brasil",[34] junto com direitos fundamentais tais como a privacidade e a liberdade de expressão, destacando a função instrumental destes princípios "a fim de promover (i) o direito de todos de acessar a internet; (ii) o acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; (iii) a inovação e o estímulo à ampla difusão das novas tecnologias e modelos de uso e acesso".[35] Assim, o MCI atribui à neutralidade da rede uma posição primária, colocando-a entre os princípios constitucionais, tais como a proteção dos direitos humanos e a promoção da inovação, a fim de destacar o rol crucial da neutralidade da rede para promover um ambiente sustentável de internet.

O legislador brasileiro considerou que a neutralidade da rede é necessária para evitar o tipo de controle que potencialmente poderia limitar a capacidade dos usuários de receber e transmitir informação e ideia, incluída sua capacidade de compartilhar inovação. Neste sentido, o MCI impõe

33 Cf.: MOLON DEFENDE NEUTRALIDADE DA REDE E CRITICA QUALIDADE DA INTERNET BRASILEIRA EM CONFERÊNCIA INTERNACIONAL DA FGV-RIO. MOLON Deputado Federal, 11 jun. 2015. Disponível em:Disponível em: <http://bit.ly/2fQtApt>. Acesso em: 12 nov. 2017.

34 Cf.: Marco Civil, art 2º.

35 Ibid, art 4º.

o "dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação."[36] De maneira importante, o tratamento não discriminatório que contempla o princípio da neutralidade da rede permite que os usuários se tornem desenvolvedores ativos da inovação e produtores de conteúdo além de serem meros consumidores, provocando, assim, um círculo virtuoso de inovação (WILLIAMSON; BLACK; PUNTON, 2011), e criando um campo de jogo equitativo para os empreendedores e para as empresas a fim de que lancem produtos e serviços inovadores.

Por esses motivos, o MCI escolheu proteger firmemente a NR, permitindo aos operadores administrar de forma discriminatória o tráfego de internet somente quando tal administração seja "essencial para a adequada provisão dos serviços e aplicações – ou para a – priorização dos serviços de emergência".[37] Mais ainda, enquanto o MCI promove "a liberdade dos modelos de negócios"[38] na Internet, especifica claramente que tal liberdade não poderá superar a NR, declarando que a oferta comercial não poderá "entrar em conflito com os outros princípios estabelecidos nesta lei". Como tal, em seu artigo 9º, o MCI sugere que devem ser proibidas as práticas fundadas em um tratamento diferenciado. A despeito do fato que o ZR se baseie em uma evidente diferenciação de preço, a decorrência do período entre a aprovação do MCI e a elaboração e aprovação do decreto de regulamentação do MCI, ofereceu às operadoras uma janela de tempo suficiente para começaram a oferecer planos de ZR no mercado brasileiro, aproveitando da incerteza jurídica para argumentar que as práticas de ZR não contradizem a normativa sobre NR.

O *ZERO-RATING*

Em geral, a expressão ZR descreve as práticas comerciais nas quais os operadores, ou um terceiro, patrocinam o consumo de dados relacionado com uma seleção limitada de aplicativos, que podem ser acessados por usuários de redes móveis, sem incorrer em gastos por consumo de dados (BELLI, 2016). Assim, o consumo de dados dos serviços de ZR não está incluído na capacidade de dados dos usuários. Geralmente, tais práticas se baseiam na discriminação positiva de aplicações específicas e tem sido propostas em países desenvolvidos bem como em países em via de desen-

36 Cf.: Marco Civil, art 9º.

37 Ibid, art 9º.

38 Ibid art. 3º, VIII.

volvimento, gerando uma nova onda de debates sobre NR. Cabe destacar que existem várias formas de ZR que podem ser classificadas em:

I. subsidio de aplicativos;

II. patrocínio de aplicativos;

III. plataformas de ZR;

VI. patrocínio não-discriminatório de dados;

V. e tele-serviços públicos patrocinados (BELLI, 2017).

A maioria dos esquemas de ZR visam atingir dois objetivos que podem ser considerados fundamentais desde a perspectiva dos operadores como das grandes empresas de Internet, isto é, atrair assinantes das redes da concorrência e obter novos clientes. Todavia, cabe destacar que subsistem importantes diferencias entre os elementos da taxonomia, baseada em qual entidade patrocina qual serviço.

Tabela 1 – Taxonomia de modelos de *zero-rating*

Tipo de ZR	Quem é o patrocinador?	Qual serviço é patrocinado?
Subsidio de aplicativos	Operadoras	Acesso a aplicativos selecionados pelas operadoras
Patrocínio de aplicativos	Provedores de conteúdo ou aplicativos	Acesso a aplicativos patrocinados pelos provedores
Plataformas de ZR	Potencialmente qualquer tipo de entidade	Acesso a aplicativos patrocinados pelos provedores ou que respeitem os requisitos técnicos impostos pelo patrocinador
Patrocínio não-discriminatório de dados	Potencialmente qualquer tipo de entidade	Os dados patrocinados podem ser utilizados discricionariamente pelo usuário
Tele-serviços públicos patrocinados	Poderes públicos ou operadoras	Acesso a aplicativos de tele-serviços públicos

Fonte: Elaborado pelo autor.

Os modelos apresentados na tabela acima apresentam diferencias conceptuais que devem ser analisadas a fim de definir a compatibilidade ou não com a racionalidade da NR. Os reguladores Europeus, reunidos no BEREC – o órgão dos reguladores das comunicações eletrônicas na Europa –, elaboraram critérios particularmente uteis a fim de efetuar avaliar a compatibilidade dos vários modelos de ZR com o princípio de NR.[39]

39 Ver BEREC (30 de Agosto 2016). BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. BoR (16) 127.

Nomeadamente, as linhas diretrizes elaboradas pelo BEREC esclarecem que "41. Uma oferta de *zero rating* em que todos os aplicativos são bloqueados – ou degradados – uma vez que o limite de dados é atingido, exceto para o(s) aplicativo(s) subsidiados, violaria a neutralidade da rede [...]" (BEREC, 2016).

Além disso, as diretrizes evidenciam a existência de práticas de zero rating com efeitos anticoncorrenciais, apontando que tais práticas deveriam ser evitadas. Nomeadamente, o BEREC afirma que:

> 42. O provedor de acesso pode aplicar ou oferecer zero rating para toda uma categoria de aplicativos (por exemplo, todos os aplicativos de vídeo ou de transmissão de música) ou apenas para determinadas aplicações (por exemplo, seus próprios serviços, um aplicativo de mídia social específico, o vídeo ou música mais popular aplicativos). No último caso, um usuário final não está impedido de usar outras aplicações de música. No entanto, a ausência de preço aplicada ao tráfego de dados da aplicação de música com zero rating (e o fato de que o tráfego de dados da aplicação de música com zero rating não seja incluído nas franquias de dados do provedor) cria um incentivo econômico para que o usuário use essa aplicação de música em vez dos concorrentes. Os efeitos da prática do zero rating aplicada a uma aplicação específica são mais susceptíveis de 'prejudicar a essência dos direitos dos usuários finais' ou levar a circunstâncias em que 'a escolha dos usuários finais seja materialmente reduzida na prática' do que quando o zero rating é aplicado a uma categoria completa de aplicativos. (BEREC, 2016)

Todavia, tais critérios não deveriam ser necessários no âmbito brasileiro já que, entre o final de 2014 e o início de 2016, o Ministério da Justiça do Brasil organizou uma consulta destinada a elaborar o decreto de regulamentação do MCI e fornecer indicações sobre a compatibilidade de práticas de patrocínio com o princípio de NR.

Cabe destacar mais uma vez que, bem como em outros países, no Brasil os participantes da consulta pública forneceram respostas bastante polarizadas a respeito do ZR, mostrando uma marcada divisão entre, por um lado, os operadores e os fabricantes de equipamentos que respaldaram fortemente a adoção de modelos de ZR, enquanto a maioria dos demais consultados argumentaram que o ZR deveria ser considerado incompatível com as disposições da NR (BRITO CRUZ; MARCHESAN; SANTOS, 2015). Os apoiadores do ZR declararam as práticas são susceptíveis de avantajar os consumidores, fornecendo um acesso gratuito a serviços selecionado e permitindo que os consumidores que não possuem recursos possam acessar a certos serviços que, de outro modo, deveriam renunciar. Por outro lado, os detratores do ZR declararam que, a longo prazo, os benefícios potenciais do ZR aparecerão à custa do desenvolvimento do ecossistema digital brasileiro e da liberdade de informação e opinião dos cidadãos do Brasil.

Neste sentido, vale a pena meditar que, apesar do ZR poder ser considerado um modelo de negócios legítimo, o raciocínio do subsidio e do patrocínio de aplicativos é direcionar o consumidor para um leque de serviços limitados, cuja base de usuários e cujo poder de barganha já alcançam um tamanho suficiente para ser aprovados pelas operadoras. Assim podemos apontar que a maioria dos planos de ZR existentes se propõe a orientar os usuários a serviços menos custosos no lugar de deixar o usuário completamente livre de escolher os serviços mais úteis ou mais inovadores. Tal padrão pode criar, assim, muros que delimitariam os usuários de poucos recursos para que só utilizassem serviços subsidiados e tivessem acesso a bolhas de informação predefinidas pelos operadores ou outros patrocinadores. Todavia, é importante recordar que o artigo 2º do MCI exige a firme proteção da pluralidade e da abertura, e o artigo 3º prevê explicitamente "a liberdade dos modelos de negócios" a condição que sejam respeitados os "outros princípios estabelecidos nesta lei", tais como a NR. Á luz de tais considerações o decreto 8.771/2016[40] foi elaborado e forneceu umas indicações mais solidas a respeito das circunstâncias nas quais os modelos de ZR devem ser considerados como incompatíveis com as disposições sobre NR. Assim, o artigo 9º do decreto 8.771/2016 proíbe todas as práticas que:

> I - comprometam o caráter público e irrestrito do acesso à internet e os fundamentos, os princípios e os objetivos do uso da internet no País;
> II - priorizem pacotes de dados em razão de arranjos comerciais; ou
> III - privilegiem aplicações ofertadas pelo próprio responsável pela transmissão, pela comutação ou pelo roteamento ou por empresas integrantes de seu grupo econômico.

No entanto, é importante destacar que, até agora, as operadoras brasileiras têm rejeitado a incompatibilidade do ZR e da NR, incluindo serviços subsidiados em uma grande variedade de contratos de acesso móvel. Um exemplo particularmente flagrante é oferecido pela operadora Claro, que além de subsidiar acesso a WhatsApp, subsidia os próprios serviços de vídeo e de música.

40 Cf.: BRASIL. Decreto nº 8.771, 11 de maio de 2016. Disponível em: <http://bit.ly/1TRNpKo>. Acesso em: 12 nov. 2017.

Figura 1 – Exemplo de prática de zero-rating não compatível com o artigo 9º do decreto 8.771/2016

Fonte: Simulador *on-line* de planos da Operadora Claro.[41]

É importante também reiterar que, no Brasil bem como em outros países da América Latina, apenas aplicações bem estabelecidas são incluídas nos planos de ZR. A saber, Facebook, Twitter, Whatsapp e, mais raramente, Deezer, são geralmente os únicos aplicativos subsidiados pelas operadoras. Deste modo, o panorama brasileiro exemplifica de maneira contundente as críticas segundo as quais os planos de ZR consolidariam os serviços bem estabelecidos em vez de promover a concorrência, o surgimento e a difusão de novos aplicativos e o pluralismo da mídia. Na verdade, como demonstra o exemplo brasileiro, apenas os serviços que já estão em posição dominante são suficientemente atrativos e possuem o poder de negociação necessário para encerrar acordos de ZR. Mais ainda, tal cenário confirma as críticas segundo as quais os planos de ZR teriam o potencial de transformar os usuários ativos de internet em consumidores passivos de aplicações, impulsionando uma evolução da Internet desde uma rede de uso geral e geradora de aplicativos inovadores a uma rede estanque cujo uso seria predefinido pelas operadoras, ao estilo de sistemas predecessores da Internet como o Minitel (BELLI, 2016).[42]

41 Ver: CLARO. Disponível em: <http://www.claro.com.br/simulador-planos/simular/#pos>. Acesso em: 12 nov. 2017.

Ainda que as práticas de ZR possam ser consideradas como medidas eficientes de prestação de serviços patrocinados, parece inquestionável que essas práticas se baseiam na discriminação positiva dos serviços subsidiados e/ou patrocinados, com o objetivo de tornar os usuários em simples consumidores de serviços específicos no lugar de prosumidores da Internet. Tal evolução parece estar em claro conflito com o artigo 3º do MCI, que estabelece "a preservação e garantia da neutralidade da rede" assim como "a preservação da natureza participativa da rede" como princípios fundamentais da disciplina da internet no Brasil. Mais ainda, ao promover o uso de apenas aplicações bem estabelecidas o dos seus próprios aplicativos, os atuais planos de ZR não parecem ser compatíveis com o respeito e a promoção da "livre iniciativa, a livre concorrência, […] a pluralidade e diversidade" que estão explicitamente consagrados pelo artigo 2º do MCI. Portanto, parece desejável que ação fiscalizadora tripartite, estabelecida pelos artigos 17-20 do decreto 8.771/2016 – segundo o qual a Anatel, a Secretaria Nacional do Consumidor e o Sistema Brasileiro de Defesa da Concorrência atuam de forma colaborativa, consideradas as diretrizes do CGI.br – esclarecesse em qual medida as práticas de ZR existentes no Brasil possam ser consideradas como compatíveis com as disposições do MCI anteriormente mencionadas e bem como com o artigo 10 do decreto 8.771/2016, segundo o qual

> As ofertas comerciais e os modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa, compreendida como um meio para a promoção do desenvolvimento humano, econômico, social e cultural, contribuindo para a construção de uma sociedade inclusiva e não discriminatória.

Neste sentido, a elaboração das tão atendidas "diretrizes do CGI.br", mencionadas pelo artigo 20 do decreto 8.771/2016, representa uma importante etapa a fim de esclarecer o assunto.

42 A rede Minitel era um sistema fechado, popular especialmente na França durante a década de 1990, no âmbito do qual apenas a operadora podia decidir quais serviços estariam disponíveis para os usuários, ao tempo que o regulador das telecomunicações tenha o poder de aprovar ou rejeitar qualquer serviço de forma unilateral. A natureza desse sistema de uso predefinido é antitética à natureza aberta e de uso geral da Internet.

CONCLUSÃO

O raciocínio da NR é manter a Internet como um sistema aberto e distribuído, cuja evolução pode ser moldada diretamente pelos usuários, que participam livremente em qualidade de prosumidores. Como mencionado neste artigo, várias técnicas de GTI e vários planos de ZR são susceptíveis de alterar a natureza da Internet e infringir a NR. Além disso, cabe destacar que, apesar de alguns modelos de ZR poderem ser utilizados como soluções temporais para permitir que os indivíduos não conectados possam se comunicar, é importante advertir que existem soluções que podem preservar a natureza da Internet – e os benefícios que decorrem de tal natureza – de maneira mais sustentável. Em especial, as políticas públicas deveriam promover a conectividade plena, outorgando aos indivíduos o poder de criar e de compartilhar inovação, sendo prosumidores ativos em vez de consumidores passivos. Neste sentido, como já destaquei em várias ocasiões,[43] os formuladores de políticas deveriam avaliar os custos e benefícios de ZR e também considerar soluções alternativas, a fim de empoeirar os indivíduos, tais como redes comunitárias (BELLI, 2016; VARIG, 2015; DE FILIPPI; TRÉGUER, 2015). As redes comunitárias já se encontram presentes em vários países desenvolvidos e em vias de desenvolvimento e, diferente dos esquemas de ZR, se baseiam no empoderamento individual mediante a criação de infraestruturas pelos usuários mesmos.

A característica mais comum das redes comunitárias é o uso das tecnologias de *networking* pela e para a comunidade local que define, implementa e administra a rede comunitária através de recursos compartilhados e esforços coordenados. Essa abordagem não é meramente teórica, mas demonstra a capacidade de produzir benefícios concretos e distribuídos. Alguns exemplos de destaque incluem a rede Guifi.net[44] com seus mais de 33.000 participantes espalhados em toda a região de Catalunha, Espanha, e as redes comunitárias criadas pela associação argentina AlterMundi,[45] e

43 Vejam-se, por exemplo, o workshop do IGF 2015 sobre "Community Networks: a Revolutionary Paradigm", disponível em: <http://bit.ly/2pIIN2w>, e a Conferência Internacional sobre conectividade sustentável, organizada pela FGV Direito Rio, em abril 2016, disponível em: <http://bit.ly/2pIA7Jw>.

44 Cf.: GUIFI.NET. Disponível em: <http://guifi.net/en/node/38392>. Acesso em: 12 nov. 2017.

45 Cf.: ALTER MUNDI. Redes comunitarias de Internet. <http://docs.altermundi.net/RedComunitaria/>. Acesso em: 12 nov. 2017.

a *Digital Empowerment Foundation*[46] na Índia. O objetivo principal de tais redes é empoderar as comunidades através das tecnologias, permitindo aos participantes desenvolver e administrar a infraestrutura como um recurso comum. O que é mais importante, as redes comunitárias permitem oferecer e receber qualquer tipo de serviço de modo não discriminatório e sem inspeção ou modificação dos fluxos de dados dentro da rede para além do estritamente necessário para seu funcionamento (ECHÁNIZ, 2015). Como tais, as redes comunitárias não são apenas compatíveis com os fundamentos da NR, mas também promovem o empoderamento pleno do usuário, em especial porque estão dirigidas à população que não se encontra conectada. A rigor da verdade, as redes comunitárias se baseiam no uso de modelos de implantação fácil, que os indivíduos que carecem de conhecimento técnico podem reproduzir e explorar oportunamente.

Assim, as redes comunitárias parecem oferecer uma resposta muito concreta à busca de inclusão digital, dado que não apenas contam com o potencial de criar infraestrutura desde os extremos, mas também de estimular a alfabetização digital, o empoderamento comunitário e a criação de conteúdo e serviços locais. Em uma era em que os governos são frequentemente criticados pela falta de visão política e por priorizarem os interesses de atores privados bem estabelecidos, a promoção de uma conectividade sustentável através de abordagens que empoderem os usuários, tais como redes comunitárias, seria uma escolha inteligente para promover "a livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença".

REFERÊNCIAS

ALTER MUNDI. Redes comunitarias de Internet. <http://docs.altermundi.net/RedComunitaria/>. Acesso em: 12 nov. 2017.

BAKER F.; POLK J. Polk; M. DOLLY, M. A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic. Request for Comments: 5865. 2010. Disponível em: <https://tools.ietf.org/html/rfc5865>. Acesso em: 12 nov. 2017.

BASTIAN *et al*. Comcast's Protocol-Agnostic Congestion Management System. RFC 6057. 2010. Disponível em: <https://tools.ietf.org/html/rfc6057>. Acesso em: 12 nov. 2017.

BELLI, L. (Ed.) Net Neutrality Reloaded: Zero Rating, Specialised Service, Ad Blocking and Traffic Management. Annual Report of the UN IGF Dynamic Coalition on

46 Cf.: WIRELESS FOR COMMUNITIES. Disponível em: <http://wforc.in/>. Acesso em: 12 nov. 2017.

Network Neutrality. Rio de Janeiro: FGV Direito Rio, 2016. Disponível em: <http://bit.ly/2oTtlgK>. Acesso em: 12 nov. 2017.

BELLI, L. Net Neutrality, Zero Rating and the Minitelisation of the Internet. *Journal of Cyber Policy,* Londres, Routledge n. 1, v. 2, 2017.

BELLI, L. (Ed.) Community Connectivity: Building the Internet from Scratch**.** Relatório anual da Coalizão Dinâmica sobre Conectividade Comunitária da IGF. FGV Editora, 2016. Disponível em: <http://bit.ly/2qzVPO6>. Acesso em: 12 nov. 2017.

BELLI, L.; DE FILIPPI P. Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet. Springer, 2015. Disponível em: <http://www.springer.com/us/book/9783319264240>. Acesso em: 12 nov. 2017.

BELLI, L.; VAN BERGEN, M. Protecting Human Rights through Network Neutrality: Furthering Internet Users' Interest, Modernising Human Rights and Safeguarding the Open Internet, Conselho da Europa, CDMSI, Estrasburgo, dezembro 2013, Misc. 19. Disponível em: <http://bit.ly/2fMPiKB>. Acesso em: 12 nov. 2017.

BELLO, P.; JUNG, J. Net Neutrality: Reflections on the Current Debate, GCIG Paper, n. 13, CIGI y Chatham House, Mayo de 2015. Disponível em: <http://bit.ly/2g9YewV>. Acesso em: 12 nov. 2017.

BEREC**.** BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. BoR, n. 16, v. 127, 2016**.**

BRASIL. Decreto nº 8.771, 11 de maio de 2016. Disponível em: <http://bit.ly/1TR-NpKo>. Acesso em: 12 nov. 2017.

BRITO CRUZ, F., MARCHEZAN J.; SANTOS M. O que está em jogo na regulamentação do Marco Civil da Internet? Relatório final sobre o debate público, patrocinado pelo Ministério da Justiça na regulação da lei 12.965/2014. 2015. Disponível em: <http://bit.ly/1NGFwnf>. Acesso em: 12 nov. 2017.

BROADBAND INTERNET TECHNICAL ADVISORY GROUP. Differentiated Treatment of Internet Traffic. Disponível em: <http://www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf>. Acesso em: 12 nov. 2017.

BUCCO, Rafael. LUCRO DA TELEFÔNICA BRASIL CRESCE 179% NO PRIMEIRO TRIMESTRE. Disponível em: <http://bit.ly/2evInbv>. Acesso em: 12 nov. 2017.

CGI.br. Princípios para a governança e o uso da Internet no Brasil, 2009. Disponível em: <http://www.cgi.br/resolucoes/documento/2009/003>. Acesso em: 12 nov. 2017.

CGI.br. Um pouco sobre o Marco Civil da Internet, 20 de abril de 2014. Disponível em: <http://bit.ly/2fQpL3E>. Acesso em: 12 nov. 2017.

CLARK, D.; BLUMENTHAL, M. The End-to-end Argument and Application Design: the Role of Trust. *Federal Communications Law Journal*, v. 63, n. 2, Article 3, 2011. Disponível em: <http://bit.ly/2fR3ODW>. Acesso em: 12 nov. 2017.

CLARO. Disponível em: <http://www.claro.com.br/simulador-planos/simular/#pos>. Acesso em: 12 nov. 2017.

COELHO, Mário. Lula quer regular a internet. Congresso em Foco, 24 nov. 2009. Disponível em: <http://bit.ly/2eVJ2l3>. Acesso em: 12 nov. 2017.

COUNCIL OF EUROPE. Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality. Disponível em: <http://bit.ly/2f8FlWS>. Acesso em: 20 dez. 2018.

DE FILIPPI, P.; TRÉGUER, F., Wireless Community Networks: Towards a Public Policy for the Network Commons?. In.: BELLI L.; DE FILIPPI P. (2015). *Net Neutrality Compendium:* Human Rights, Free Competition and the Future of the Internet. Springer. [s.d.]. Disponível em: <http://www.springer.com/us/book/9783319264240>. Acesso em: 12 nov. 2017.

DEL CAMPO, A. *Hacia una Internet libre de censura II:* Perspectivas en América Latina. Ciudad Autónoma de Buenos Aires: Universidad de Palermo, 2017.

ECHÁNIZ, Nicolás. Community Networks: Internet from the First Mile. FRIDA: 10 Years Contributing to Development in Latin America and the Caribbean, FRIDA Program, LACNIC, outubro de 2015. Disponível em: <http://bit.ly/1Nt5aKr>. Acesso em: 12 nov. 2017.

ECONOMIDES, N.; TÅG, J. Network Neutrality on the Internet: a Two-sided Market Analysis. *Information Economics and Policy Journal*, v. 24, p. 91-104, fev. 2012. Disponível em: <http://bit.ly/1NCEDyX>. Acesso em: 12 nov. 2017.

ENGINE. STARTUPS FOR NET NEUTRALITY. Disponível em: <http://www.engine.is/startups-for-net-neutrality>. Acesso em: 12 nov. 2017.

EUROPEAN COURT OF HUMAN RIGHTS. "Ahmet Yıldırım v. Turkey". Sentença Nº. 3111/10. Disponível em: <http://hudoc.echr.coe.int/fre?i=001-115705>. Acesso em: 21 dez. 2018.

EUROPEAN COURT OF HUMAN RIGHTS. "Autronic AG v. Switzerland", 22 Mai 1990. Sentença Nº 12726/87. Disponível em: <http://hudoc.echr.coe.int/eng?i=001-57630>. Acesso em: 21 dez. 2018.

FELTEN, B. There's No Economic Imperative to Reconsider an Open Internet, 3 de abril de 2013. Disponível em: <http://bit.ly/2ga5dGb>. Acesso em: 12 nov. 2017.

FÓRUM VIVO. Telefônica insistirá na franquia em banda larga fixa. Disponível em: <http://vivo.tl/2eVKTGF>. Acesso em: 12 nov. 2017.

FRIEDEN, Rob. Net Bias and the Treatment of 'Mission-Critical' Bits. Paper Conferencia TPRC, 24 mar. 2014. Disponível em: <http://bit.ly/2eXhbRE>. Acesso em: 12 nov. 2017.

GADGETS NOW. Nearly 700 startup founders urge PM Modi to defend net neutrality. <http://timesofindia.indiatimes.com/tech/tech-news/Nearly-700-startup-founder

s-urge-PM-Modi-to-defend-net-neutrality/articleshow/50729785.cms>. Acesso em: 12 nov. 2017.

GROSSMAN, D. New Terminology and Clarifications for Diffserv. Request for Comments: 3260. April 2002. Disponível em: <https://tools.ietf.org/html/rfc3260>. Acesso em: 12 nov. 2017.

GUIFI.NET. Disponível em: <http://guifi.net/en/node/38392>. Acesso em: 12 nov. 2017.

HIRATA, Lucas. Para presidente da Telefônica, é 'injusto' usar menos dados pelo mesmo preço. Disponível em: <http://bit.ly/2p2H2cL>. Acesso em: 12 nov. 2017.

INTERNET ASSOCIATION. Before the FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554.Disponível em: <http://internetassociation.org/wp-content/uploads/2014/07/Comments.pdf>. Acesso em: 12 nov. 2017.

INTERNET GOVERNANCE FORUM (IGF). Policy Statement on Network Neutrality, resultados do XV Fórum das Nações Unidas sobre Governança da Internet, novembro, 2015, § 1. Disponível em: <http://bit.ly/2qbKqDX>. Acesso em: 12 nov. 2017.

INTERNET GOVERNANCE FORUM. Disponível em: <http://bit.ly/2qbKqDX>. Acesso em: 12 nov. 2017.

LARUE, Frank (UN); MIJATOVIC Dunja (OSCE); MARINO Catalina Botero (OEA); TLAKULA Faith Pansy (CADHP). Declaração conjunta para liberdade de expressão e internet do relator especial, junho de 2011. Disponível em: <http://bit.ly/1wnId8U>. Acesso em: 12 nov. 2017.

LEMLEY, M.; LESSIG, L. The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era. *UCLA Law Review*, n. 48, v. 925, 2000.

MOLON DEFENDE NEUTRALIDADE DA REDE E CRITICA QUALIDADE DA INTERNET BRASILEIRA EM CONFERÊNCIA INTERNACIONAL DA FGV-RIO. MOLON Deputado Federal, 11 jun. 2015. Disponível em: Disponível em: <http://bit.ly/2fQtApt>. Acesso em: 12 nov. 2017.

NEUTRALIDADE NO MARCO CIVIL. Disponível em: <http://www.startupspelaneutralidadedarede.com/>. >. Acesso em: 12 nov. 2017.

OBSERVATÓRIO DO MARCO CIVIL DA INTERNET. Neutralidade de rede e ordem econômica. Disponível em: <http://www.omci.org.br/jurisprudencia/207/neutralidade-de-rede-e-ordem-economica/>. Acesso em: 20 dez. 2018.

OECD. "The Development of Fixed Broadband Networks". *OECD Digital Economy Papers*, n. 239, 2014.

OU, G. Managing Broadband Networks: a Policymaker's Guide. *The Information Technology and Innovation Foundation (ITIF)*, 2008. Disponível em: <http://bit.ly/1Fz48ui>. Acesso em: 12 nov. 2017.

PALLIS, G.; VAKALI, A. Insight and Perspectives for Content Delivery Networks. *Communications of the ACM*, v. 49, n. 1, 2016. Disponível em: <http://bit.ly/2f-Nh5us>. Acesso em: 12 nov. 2017.

RAMOS, P. H. S. Arquitetura da rede e regulação: a neutralidade da rede no Brasil. Fundação Getúlio Vargas, Escola de Direito, São Paulo, 2015. Disponível em: <http://bit.ly/2fPID1c>. Acesso em: 12 nov. 2017.

ROSEN, E. *et al*. Multiprotocol Label Switching Architecture. Request for Comments: 3031. 2001. Disponível em: <https://tools.ietf.org/html/rfc3031>. Acesso em: 12 nov. 2017.

VARIG, R. at al. Guifi.net, una infraestructura de red colaborativa. Competer Networks, 2015. Disponível em: <http://people.ac.upc.edu/leandro/pubs/crowds-guifi-en.pdf>. Acesso em: 12 nov. 2017.

WILLIAMSON, Brian; BLACK, David; PUNTON, Thomas. The Open Internet. A Platform for Growth", um relatório para a BBC, Blinkbox, Channel 4, Skype e Yahoo! Plum Consulting, outubro de 2011. Disponível em: <http://bit.ly/2fV-t61F>. Acesso em: 12 nov. 2017.

WIRELESS FOR COMMUNITIES. Disponível em: <http://wforc.in/>. Acesso em: 12 nov. 2017.

WU, T. Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law*, 2, 141, 2003.

WU, T.; YOO, C. Keeping Internet neutral? Tim Wu and Christofer Yoo Debate. *Federal Communications Law Journal*, v. 59, n. 3, 2007. Disponível em: <http://bit.ly/2gdkmWW>. Acesso em: 12 nov. 2017.

ZERO RATING. Disponível em:<www.zerorating.info>. Acesso em: 12 nov. 2017.

CONVERGÊNCIA, CONECTIVIDADE COMUNITÁRIA E A QUESTÃO DO ESPECTRO

DIEGO VICENTIN

Recentemente minha atenção foi chamada para o item 51 da consulta da Anatel sobre a agenda regulatória 2017-2018. Ele trata da regulamentação do Licensed Assisted Access (LAA), um padrão da família 3GPP que irá disputar espaço com o Wi-Fi no espectro "aberto" – não-licenciado. A descrição oficial do item 51 é a seguinte: "Elaborar regulamentação que permita o uso da faixa de 5GHz por operadoras de forma compartilhada no espaço e no tempo com tecnologias WI-FI".[1]

Mesmo que o item 51 não esteja entre os mais urgentes da agenda, ele se relaciona com a infraestrutura a partir da qual vamos – enquanto consumidores – nos conectar à Internet no futuro próximo. A introdução do LAA é um sinal da convergência entre redes "móveis" – celulares – e "sem fios" (WLAN). Convergência que é ao mesmo tempo técnica, política e de mercado e que, portanto, não acontece sem tensões e conflitos. Por exemplo, entre padrões e famílias tecnológicas distintas: de um lado LTE-LAA e 3GPP[2] e, de outro, WiFi e IEEE 802.[3] De uma perspectiva ampla, trata-se da encruzilhada entre as telecomunicações e a computação

1 AGÊNCIA NACIONAL D TELECOMUNICAÇÕES. CONSULTA PÚBLICA Nº 1. Disponível em: <https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C1982&Tipo=1&Opcao=andamento>. Acesso em: 16 jun. 2017.

2 3GPP (3rd Generation Partnership Project) é a associação responsável por definir os padrões básicos de funcionamento da tecnologia LTE (4G) de redes celulares. Ver: BERTENYI, Balazs. RAN adjusts schedule for 2nd wave of 5G specifications. Disponível em: <http://www.3gpp.org/>. Acesso em: 16 jun. 2017.

3 O grupo IEEE 802 é o responsável por definir padrões básicos de funcionamento de redes locais (LAN) e metropolitanas (MAN) como Wi-Fi (802.11), Ethernet (802.3), Bluetooth (802.15) e WiMAX (802.16). Ver: IEEE 802 LAN/MAN STANDARDS COMMITTEE. Get 802 standards. Disponível em:<http://www.ieee802.org/>. Acesso em: 16 jun. 2017.

em rede que tornou-se objeto da pesquisa de doutorado que finalizei em 2016 (VICENTIN, 2016).[4]

Passei algum tempo acompanhando as atividades do grupo IEEE 802, que se reúne a cada dois meses para decidir os princípios básicos de funcionamento de tecnologias como o Wi-Fi (802.11), a Ethernet (802.3) e o Bluetooth (802.15). Do ponto de vista técnico a padronização deve garantir interoperabilidade entre diferentes aparelhos e fabricantes; trata-se de decidir as regras básicas de funcionamento de uma tecnologia. Mas, em reuniões como as do grupo 802, ao contrário do que se poderia imaginar, a técnica não é o plano de realidade mais evidente. Na verdade, são resolvidas ali sobretudo as tensões de mercado, principalmente na disputa por patentes essenciais (Vicentin, 2015). Em campo, ouvi muitas vezes que é com a padronização técnica que se cria o mercado.

De fato, não seria exagero dizer que o grupo IEEE 802 criou o mercado de computação em "redes locais" (Local Area Networks, LANs). Tanto o padrão Ethernet (802.3) quanto o Wi-Fi (802.11) tornaram-se hegemônicos mundialmente. Aquilo que as operadoras de rede celular temiam de certo modo aconteceu: o Wi-Fi tornou-se a primeira opção no tráfego de dados por interface aérea na "última milha".[5] Mas esse temor fazia sentido apenas quando os mercados de provimento de Internet por cabo/Wi-Fi e de "Internet móvel" (celular) eram distintos. Hoje, grandes conglomerados dominam praticamente toda infraestrutura de conexão.[6] É de se esperar, portanto, que as sinergias entre redes distintas dessa infraestrutura sejam exploradas na medida em que tais redes passam a ser propriedade de um mesmo grupo econômico. De início, as operadoras de rede celular integraram as redes Wi-Fi à sua arquitetura numa prática

4 Pesquisa de doutorado realizada no Instituto de Filosofia e Ciências Humanas da UNICAMP, com financiamento da FAPESP.

5 A "última milha" é o termo genérico (porque não corresponde à distância assinalada) usado para designar o meio físico (cabo ou interface de rádio) que conecta diretamente o usuário final à rede.

6 Existe amplo material sobre a concentração de mercado nas telecomunicações, entre as publicações mais recentes. Ver:

OBSERVATORIO. Concentração das telecomunicações no Brasil e as ameaças de desregulação do setor. Disponível em: <http://www.observacom.org/concentracao-das-telecomunicacoes-no-brasil-e-as-ameacas-de-desregulacao-do-setor/>. Acesso em: 23 abr. 2017.

conhecida como *offloading,*[7] especialmente em áreas densas e/ou ambientes fechados – centros comerciais, estádios, etc. – onde as redes 3G e 4G não dão conta da demanda por tráfego. Mas a integração/convergência entre redes "móveis" e "sem fios" não vai parar por aí, e a introdução do LAA é sinal claro disso.

Até aqui, o tráfego desviado da rede celular por Wi-Fi *offloading* não é descontado do limite de franquia que normalmente se aplica aos planos de "Internet móvel", mas, isso torna-se uma possibilidade real com a introdução do LAA no mercado, já que essa tecnologia vai garantir aos operadores de rede maior controle sobre o fluxo que atravessa uma ou outra rede. Não é por menos que as Teles[8] estejam forçando a possibilidade de cobrança de franquia nos serviços de "Internet fixa";[9] elas querem unificar essas duas infraestruturas também no que diz respeito ao modelo de cobrança, controlando e taxando o fluxo de dados – seu volume – e não apenas o acesso à rede – a conexão. Trata-se de implementar um novo regime de escassez que, se concretizado, terá efeitos negativos aumentando as barreiras de entrada na cultura digital e diminuindo a capacidade de protagonismo do usuário final.[10] Seria mais um passo na direção da concentração de poder sobre a infraestrutura de rede que dá corpo ao funcionamento da Internet.

---

7 WIKIPEDIA. Mobile data offloading. Disponível em: <https://en.wikipedia.org/wiki/Mobile_data_offloading>. Acesso em: 23 abr. 2017.

8 O termo "Tele" é utilizado comumente, no Brasil, para se referir às grandes empresas operadoras de rede, concessionárias do ramo das telecomunicações.

9 Sobre a cobrança de franquia, ver: OBSERVATORIO. Reflexões a cerca da adoção da franquia da dados na internet fixa. Disponível em: <http://observatoriodainternet.br/post/reflexoes-a-cerca-da-adocao-da-franquia-da-dados-na-internet-fixa>. Acesso em: 23 abr. 2017.

10 Para um exemplo simples das implicações do limite de franquia para a cidadania e acesso à informação, ver: REDDIT. As novas franquias de dados impostas pelas operadoras impedem o trabalho de pesquisadores independentes. Exemplo: o vazamento da Mossack Fonseca. Disponível em: <https://www.reddit.com/r/brasil/comments/4db26p/as_novas_franquias_de_dados_impostas_pelas/>. Acesso em: 23 abr. 2017.

A QUESTÃO DO ESPECTRO

Ainda que as redes WLAN e celular compartilhem alguns princípios de funcionamento, existe uma diferença significativa entre ambas em relação ao modo de ocupação do espectro eletromagnético.[11] É de conhecimento geral que as redes celulares funcionam a partir da utilização exclusiva do espectro, em que as empresas adquirem – por valores bilionários – o direito de ocupar determinadas faixas de frequência numa determinada região por determinado período de tempo. Essa perspectiva, que tornou-se dominante ao longo do século XX, supõe que a interferência é algo essencialmente negativo e que o uso exclusivo do espectro eletromagnético é o remédio mais eficaz para evitá-la.

No final do século XX, no entanto, a tendência de fechamento do espectro sofreu uma pequena inversão a partir da abertura de uma faixa de frequências para uso não-licenciado para fins médicos, científicos e industriais – bandas ISM. A medida foi adotada globalmente com nuances regulatórias entre países distintos, mas, de todo modo, isso inaugurou um modelo alternativo de regulação do espectro que permitiu o surgimento de uma série de inovações técnicas – Wi-Fi e Bluetooth são bons exemplos, além de uma série incontável de aparelhos médico-hospitalares. Assim, esse pequeno trecho do espectro – que sofreu acréscimos ao longo dos anos – passou a ser qualificado como "aberto", "compartilhado" ou "não-licenciado" – *unlicensed* ou *license-exempt*, em inglês.

Qualquer definição do espectro não-licenciado deve operar na junção do dispositivo regulatório e do aparato técnico que lhe dá corpo. Uma definição mínima pode se manter presa ao fato de que estamos tratando de uma parcela do espectro de radiofrequências cujo uso não requer licença, desde que os equipamentos operando nessa(s) faixa(s) estejam de acordo com as normas estabelecidas pelo órgão regulador responsável. Ou seja, não é preciso cadastramento ou autorização prévia para utilização do espectro "aberto": as normas de regulação recaem sobre a configuração dos aparelhos que operam nessa(s) faixa(s). Desse modo, não é possível separar as faixas hoje chamadas "não-licenciadas" dos objetos técnicos que nelas

11 O espectro eletromagnético é o conjunto de todas as possíveis frequências de radiação eletromagnética. Trata-se de uma grandeza que se propaga no espaço em formato de onda e a partir de uma perturbação inicial. As ondas de rádio formam o subconjunto das ondas eletromagnéticas que tornou-se absolutamente central para o funcionamento da infraestrutura contemporânea de informação e comunicação. As ondas de rádio são aquelas que cobrem o espectro eletromagnético no intervalo entre 3Hz e 3000 GHz (3THz).

operam. Tais objetos são formalmente reconhecidos como "equipamentos de radiação restrita";[12] o termo se estende sobre um grupo bastante heterogêneo que inclui desde aparelhos auditivos até roteadores Wi-Fi.

Justamente porque o uso do "espectro aberto" não se dá nos termos de uso exclusivo, aparelhos que funcionem nessa faixa precisam aceitar interferência de outros que estejam ocupando o mesmo espaço – terreno e espectral. Assim, foi preciso desenvolver protocolos que garantissem a coexistência nesse(s) espaço(s). O Listen Before Talk (LBT) é o protocolo adotado pelo Wi-Fi, sua vantagem mais evidente é a de que não requer controle centralizado de rede para a coordenação do acesso ao espectro, diferentemente do que acontece nas redes celulares. Assim, boa parte do embate entre as famílias IEEE 802 e 3GPP está relacionado à definição do protocolo que vai permitir a "coexistência justa" entre Wi-Fi, LTE-LAA e LTE-U. Esse último é certamente o mais agressivo combatente nessa disputa, na medida em que pretende adotar o protocolo Duty Cycle,[13] que deve colocar em desvantagem os aparelhos baseados em LBT no que diz respeito ao acesso ao espectro, prejudicando seu funcionamento.

Quero chamar atenção para o fato de que, com a introdução do LAA e do LTE-U, corremos o risco de que o espectro "aberto" ou não-licenciado seja subjugado ao modelo de escassez do espectro fechado, de licenciamento exclusivo. O próprio nome Licensed Assisted Access subentende que o espectro "aberto" servirá de válvula de escape para o tráfego excedente no espectro "fechado". As operadoras de rede celular vão fazer uso do primeiro sobretudo na função de *downlink*, e para dar conta do crescimento da utilização de *streaming* de vídeo e outras aplicações de alta demanda – por tráfego. Basicamente pretendem ocupar o espectro não-licenciado e monetizá-lo distribuindo conteúdo na direção dos usuários finais. Ainda não há consenso[14] sobre o modo como isso vai influenciar o "ecossistema" já instalado da família Wi-Fi, especialmente para redes

12 Atualmente os "aparelhos de radiação restrita são regulados pela resolução 506 de 2008 da ANATEL. Disponível em:

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Resolução nº 506, de 1º de julho de 2008. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2008/104-resolucao-506>. Acesso em: 23 abr. 2017.

13 Ver: WIKIPEDIA. Duty cycle. Disponível em: <https://en.wikipedia.org/wiki/Duty_cycle>. Acesso em: 23 abr. 2017.

14 Debate recente com representantes da indústria e da sociedade civil sobre os critérios de coexistência entre LTE e Wi-Fi. Cf.: NEW AMERICA. Wi-Fi and Unlicensed LTE. Disponível em: <https://www.newamerica.org/oti/events/wi-fi-and-unlicensed-lte/>. Acesso em: 23 abr. 2017.

municipais e comunitárias que se fiam nessa tecnologia. Para além do *streaming*, há o crescimento potencial da "internet das coisas" que deve alavancar ainda mais a demanda por tráfego na interface aérea. É preciso estar atento e defender que o espectro não-licenciado mantenha-se como bem de interesse público e compartilhado, e a faixa do 5GHz – até aqui, a menos ocupadas do espectro "aberto" – não seja apropriada completamente pelo interesse privado das grandes operadoras de rede.

REDES COMUNITÁRIAS E APROPRIAÇÃO

> Tem havido desequilíbrios extraordinários de poder ao longo da história. Eu não sou comunista, mas anteriormente houve gerações de pensadores quem defenderam a necessidade de se apropriar dos meios de produção como forma de enfrentar desigualdades no acesso à riqueza. Estamos nos aproximando rapidamente do ponto em que temos que nos apropriar dos meios de nossa comunicação. (SNOWDEN, 2016)

O excerto acima foi extraído de uma fala de Edward Snowden por videoconferência para uma plateia em Berlim.[15] Podemos levantar a hipótese de que a apropriação a que se refere Snowden está acontecendo em pequena escala, no plano local, por iniciativas as quais se convencionou chamar "redes comunitárias". De modo geral, o termo se refere a comunidades que decidiram implementar sua própria infraestrutura de informação e comunicação por razões que vão desde o simples desejo por uma conexão à Internet – que tenha qualidade satisfatória e preço acessível – até motivações tecnopolíticas mais refinadas, de grupos que pretendem exercer algum grau de autonomia sobre os meios através dos quais se comunicam, ou seja, sobre seu próprio sistema de informação.

Claro que o termo "rede comunitária" tem múltiplos sentidos que excedem o encontro computação-comunidade. De todo modo, mesmo dentro desse viés específico, as redes comunitárias são muito diferentes entre si e não necessariamente se destinam a prover acesso à Internet. Já é bastante conhecido o caso das redes de telefonia celular autogeridas que funcionam no território indígena de Oaxaca, no México. As ligações à longa distância são concretizadas por VOIP[16] e requerem o pagamento de pequenas taxas

15 Logan CIJ Symposium, 11-12 de Março de 2016. Cf.: YOUTUBE. LoganCIJ16: Edward Snowden addresses the audience. Disponível em: <https://www.youtube.com/watch?v=OVn55kIzJeA&list=PLS_7b8Iu1oBGXgCt1y3-i8lUD4gFI2u7S>. Acesso em: 23 abr. 2017.

16 *Voice over Internet Protocol*. Cf.: TELECO. Voz sobre IP I: Comutação de Circuito e de Pacote. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoipconv/pagina_3.asp>. Acesso em: 23 abr. 2017.

dos usuários, as ligações locais, no entanto, são livres de cobrança. A rede foi instalada com apoio da associação Rhizomatica e funciona gerida por associações locais. Um aspecto importante do ponto de vista de política pública para o qual quero chamar atenção é o de que tais redes conseguiram uma licença social para o uso do espectro nas frequências da telefonia celular – que normalmente exigem pagamento e licença. Mas, nesse caso, como em outros, a ação tecnopolítica vem antes da autorização legal.[17]

No Brasil os exemplos de redes comunitárias estão se multiplicando. Um dos casos mais significativos e longevos é o da Rede Mocambos, que promove diversas formas de conexão entre territórios quilombola no Brasil. A rede mantém um sistema de compartilhamento de arquivos e conteúdo cultural – Baobáxia –, que foi descrito como uma "rede federada eventualmente conectada" (Tozzi, 2010). Mais recentemente, merece destaque a fundação da Cooperativa Laboratório de Redes Livres (CooLab)[18] que surge com intuito de promover a expansão das redes comunitárias oferecendo capacitação técnica e meios de financiamento para compra e instalação da infraestrutura de rede. A Coolab advém do acúmulo e da troca de experiência entre realizadores de projetos que foram realizados ao longo da última década, e que vão desde a criação provedores comunitários de Internet até a instalação de uma rede de radiofonia numa reserva extrativista no estado Acre, passando ainda pela rede Wi-Fi da "Casa dos Meninos" no Jd. São Luiz, em São Paulo.

A lista de redes comunitárias é extensa, heterogênea e atravessa países dos cinco continentes. A proposta aqui não é entrar em detalhes sobre o modo de organização e funcionamento das redes comunitárias, ou mesmo empreender algum tipo de taxonomia.[19] O que me interessa é indicar que as redes comunitárias desdobram o problema da relação entre tecnologia e política porque potencialmente concretizam uma resistência local, comunitária, frente aos grupos que controlam nossos meios de informação e comunicação em escala global. Trata-se da possibilidade de exercer poder local sobre a infraestrutura de rede que é usualmente caracterizada como "última milha". Isso implica a potencial adoção de tecnologias livres,

17 As redes foram instaladas e entraram em operação e subsequentemente conseguiram licença para uso do espectro. Ver: RHIZOMATICA. Disponível em: <http://rhizomatica.org>. Acesso em: 23 abr. 2017.

18 Ver: COOLAB. Disponível em: <http://www.coolab.org/>. Acesso em: 23 abr. 2017.

19 Cf.: BELLI, Luca (Ed.). COMMUNITY CONNECTIVITY: BUILDING THE INTERNET FROM SCRATCH. Disponível em: <http://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/community_connectivity_-_building_the_internet_from_scratch_0.pdf>. Acesso em: 23 abr. 2017.

minoritárias em relação aos padrões utilizados pelo mercado e, portanto, que resultam em modos de operação – de funcionamento – que diferem das redes comerciais em vários aspectos.

REDES COMUNITÁRIAS, GOVERNANÇA E O "ESPECTRO ABERTO"

O tema das redes comunitárias vem recebendo atenção crescente, inclusive de organizações que desempenham papel relevante como mecanismos de tomada de decisão que modulam o funcionamento da Internet. Parte dessa atenção vem acompanhada da expectativa de que as próprias comunidades desenvolvam a capacidade de fazer avançar a expansão da Internet para localidades que não despertam suficiente interesse de mercado. Desse modo, as redes comunitárias são colocadas numa chave específica – e de certo modo restritiva – que advoga pela "conectividade". Essa expectativa estimula a formalização da existência das redes comunitárias, abrindo espaço para o debate regulatório e de políticas públicas.

No plano internacional, houve o surgimento de uma "coalizão dinâmica" que se dedica à conectividade comunitária no bojo do Internet Governance Forum (IGF).[20] O Dynamic Coalition on Community Connectivity (DC3)[21] é uma coalizão multissetorial que pretende definir um conjunto de "melhores práticas" para o funcionamento e a organização das redes comunitárias, bem como fazer recomendações de políticas que favoreçam o desenvolvimento dessas redes. O grupo reúne voluntários de vários países, em sua maioria membros da sociedade civil organizada e pesquisadores diretamente envolvidos com a implementação e manutenção de redes comunitárias.

---

20 O Fórum de Governança da Internet (IGF, em inglês) foi instituído pela ONU em 2005 no contexto da Cúpula Mundial da Sociedade da Informação (World Summit on Information Society, WSIS). Trata-se de uma reunião anual, com representação multissetorial, que promove debates sobre temas sensíveis à governança da Internet visando promover recomendações sobre seu modo de funcionamento e gestão. Apesar da visibilidade que o fórum adquiriu e de sua importância como meio de pautar a agenda da governança da Internet, suas recomendações não têm poder normativo. Ver: MUELLER, 2010; ROSA; VICENTIN, 2016.

21 The Internet Governance Forum (IGF), Dynamic Coalition on Community Connectivity (DC3). Ver: THE INTERNET GOVERNANCE FORUM. Dynamic Coalition on Community Connectivity (DC3). Disponível em: <https://www.intgovforum.org/cms/175-igf-2015/3014-dynamic-coalition-on-community-connectivity-dc3>. Acesso em: 23 abr. 2017.

Por ocasião do IGF de 2016, em Guadalajara, México, a coalizão apresentou sua "declaração sobre conectividade comunitária".[22] O documento institui princípios e definições para redes comunitárias e indica que estas são caracterizadas por seis "pontos". O primeiro deles (a) diz respeito à apropriação comunitária: "a infraestrutura de rede é de propriedade da comunidade em que é implementada". Em seguida o documento institui que tal infraestrutura deve ser (b) "governada e operada pela comunidade" o que pressupõe que (c) "os detalhes de implementação da rede são públicos e acessíveis a todos" e que (d) "qualquer um está autorizado a estender a rede, desde que esteja de acordo com seus princípios e seu *design*". Por fim, a rede (e) "deve oferecer reciprocidade" em acordos de *free peering* e (f) "considerar questões de segurança e privacidade no design e na operação da rede".

Ainda que as redes comunitárias possam carregar de maneira mais explícita a bandeira da conectividade, da expansão dos meios de informação e comunicação, sua potência mais liberadora está na apropriação local da infraestrutura. Trata-se de um princípio definidor das redes comunitária e, por isso, ele abre a série de seis "pontos" elencados pelo DC3. A apropriação da infraestrutura de rede passa pela afirmação do direito de uma comunidade em construir seus próprios meios de comunicação, seja quando não há interesse de mercado ou mesmo quando o mercado não dá conta dos anseios de uma dada comunidade, por exemplo, no que diz respeito à qualidade do serviço, segurança da informação ou proteção da privacidade. Mas, para garantir que esse direito se afirme na prática, e a despeito de toda diversidade que guardam entre si, as redes comunitárias precisam defender seu acesso a recursos que são básicos para sua operação. Nesse espírito, redes comunitárias da Europa recentemente elaboraram em conjunto uma carta aberta endereçada a formuladores de políticas públicas da União Europeia.

A carta destaca o descaso com o qual as demandas das redes comunitárias vêm sendo tratadas e faz uma série de recomendações que diz respeito à regulação de suas atividades dentro do quadro do "Código Europeu de Comunicações Eletrônicas".[23] Redes comunitárias do mundo todo contribuíram e endossaram a carta que, entre suas recomendações,

22 Ver: THE INTERNET GOVERNANCE FORUM. OUTCOME DOCUMENT ON COMMUNITY CONNECTIVITY. Disponível em: <http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3737/174>. Acesso em: 23 abr. 2017.

23 Ver: EUROPEAN ECONOMIC AND SOCIAL COMMITTEE. European Electronic Communications Code. Disponível em: <http://www.eesc.europa.eu/?i=portal.en.ten-opinions.40540>. Acesso em: 23 abr. 2017.

inclui "expandir o espectro comum" (*expanding the spectrum commons*). Basicamente isso diz respeito ao que venho chamando aqui de espectro não-licenciado ou "aberto". A carta advoga pela expansão desse modelo de compartilhamento para outras frequências do espectro, inclusive com características de propagação que favoreçam o estabelecimento de *links* em longa distância – e assim possam ser utilizados na função de *backbone*. Além disso, a carta ainda nota que a entrada do LTE no espectro não-licenciado pode representar uma ameaça ao funcionamento das redes que funcionam com tecnologia Wi-Fi. Com isso, voltamos ao assunto que abre esse pequeno texto para encerrá-lo.

Aqui, defendi brevemente que a operação do padrão LTE no espectro aberto – em suas variantes LTE-U ou LAA – é um sinal da convergência entre redes "móveis" (celulares) e "sem fios" (WLAN). Numa perspectiva ampla, trata-se da encruzilhada entre telecomunicações e computação em rede. Tal convergência é simultaneamente técnica, política e de mercado e não acontece sem tensões e conflitos. Em meios aos conflitos, julgo que o risco mais urgente – e que deve ser levado em conta na regulamentação do LAA pela Anatel – se refere ao uso intensivo do "espectro aberto" pelas grandes operadoras de rede, que devem transformá-lo num bem escasso sobretudo em áreas com alta densidade de usuários. A ocupação do espectro aberto corre o risco de ser feita mormente com a distribuição de conteúdo via *streaming* para usuários finais, que serão encaixados na velha chave do "consumo". Com isso, o espectro aberto se submete ao espectro fechado funcionando em sua assistência. As redes comunitárias tem razão em se preocupar, pois aquilo que chamam de *spectrum commons* corre o risco de ser apropriado e monetizado pelas grandes operadoras de rede.

REFERÊNCIAS

AGÊNCIA NACIONAL D TELECOMUNICAÇÕES. CONSULTA PÚBLICA Nº 1. Disponível em: <https://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C1982&Tipo=1&Opcao=andamento>. Acesso em: 16 jun. 2017.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Resolução nº 506, de 1º de julho de 2008. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2008/104-resolucao-506>. Acesso em: 23 abr. 2017.

BELLI, Luca (Ed.). COMMUNITY CONNECTIVITY: BUILDING THE INTERNET FROM SCRATCH. Disponível em: <http://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/community_connectivity_-_building_the_internet_from_scratch_0.pdf>. Acesso em: 23 abr. 2017.

BERTENYI, Balazs. RAN adjusts schedule for 2nd wave of 5G specifications. Disponível em: <http://www.3gpp.org/>. Acesso em: 16 jun. 2017.

COOLAB. Disponível em: <http://www.coolab.org/>. Acesso em: 23 abr. 2017.

EUROPEAN ECONOMIC AND SOCIAL COMMITTEE. European Electronic Communications Code. Disponível em: <http://www.eesc.europa.eu/?i=portal.en.ten-opinions.40540>. Acesso em: 23 abr. 2017.

IEEE 802 LAN/MAN STANDARDS COMMITTEE. Get 802 standards. Disponível em:<http://www.ieee802.org/>. Acesso em: 16 jun. 2017.

MUELLER, Milton L. 2010. Networks and States: The Global Politics of Internet Governance. Cambridge: The MIT Press, [s.d.].

NAVARRO, L.; FREITAG, F.; BAIG, R.; ROCA, R. A commons oriented framework for Community Networks. In: Belli, Luca (Ed.). 2016. Community Connectivity: Building the Internet from Scratch. Rio de Janeiro: FGV Direito Rio. Disponível em: <http://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/community_connectivity_-_building_the_internet_from_scratch_0.pdf>. Acesso em: 16 jun. 2017.

NEW AMERICA. Wi-Fi and Unlicensed LTE. Disponível em: <https://www.newamerica.org/oti/events/wi-fi-and-unlicensed-lte/>. Acesso em: 23 abr. 2017.

OBSERVATORIO. Concentração das telecomunicações no Brasil e as ameaças de desregulação do setor. Disponível em: <http://www.observacom.org/concentracao-das-telecomunicacoes-no-brasil-e-as-ameacas-de-desregulacao-do-setor/>. Acesso em: 23 abr. 2017.

OBSERVATORIO. Reflexões a cerca da adoção da franquia da dados na internet fixa. Disponível em: <http://observatoriodainternet.br/post/reflexoes-a-cerca-da-adocao-da-franquia-da-dados-na-internet-fixa>. Acesso em: 23 abr. 2017.

REDDIT. As novas franquias de dados impostas pelas operadoras impedem o trabalho de pesquisadores independentes. Exemplo: o vazamento da Mossack Fonseca. Disponível em: <https://www.reddit.com/r/brasil/comments/4db26p/as_novas_franquias_de_dados_impostas_pelas/>. Acesso em: 23 abr. 2017.

RHIZOMATICA. Disponível em: <http://rhizomatica.org>. Acesso em: 23 abr. 2017.

ROSA, Fernanda R.; VICENTIN, Diego. Governança da Internet e suas implicações para políticas públicas. *Critical Reviews on Latin America Research (CROLAR)*, v. 5, p. 67-77, 2016.

TELECO. Voz sobre IP I: Comutação de Circuito e de Pacote. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoipconv/pagina_3.asp>. Acesso em: 23 abr. 2017.

THE INTERNET GOVERNANCE FORUM. Dynamic Coalition on Community Connectivity (DC3). Disponível em: <https://www.intgovforum.org/cms/175-igf-2015/3014-dynamic-coalition-on-community-connectivity-dc3>. Acesso em: 23 abr. 2017.

THE INTERNET GOVERNANCE FORUM. OUTCOME DOCUMENT ON COMMUNITY CONNECTIVITY. Disponível em: <http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3737/174>. Acesso em: 23 abr. 2017.

TOZZI, Vicenzo. Redes federadas eventualmente conectadas. Arquitetura e protótipo para a rede Mocambos. 2010. Trabalho de conclusão de curso – Universita degli Studi di Firenze, Florença, 2010. Disponível em: <http://www.mocambos.net/w/images/b/b3/Mono_RFEC_RedeMocambos_VT.pdf>. Acesso em: 26 mar. 2016.

VICENTIN, Diego. 2015. O que é razoável na relação entre padrões e patentes? Inovação – Revista Eletrônica de PD&I. ISSN: 2359-4691. Disponível em: <http://www.inovacao.unicamp.br/artigo/o-que-e-razoavel-na-relacao-entre-padroes-e-patentes/>. Acesso em: 26 mar. 2016.

VICENTIN, Diego. 2017. Tecnopolítica e padronização: uma experiência etnográfica no grupo IEEE 802. In: KREMER, Pablo; VESSURI, Hebe; GILBERT, Jorge (Orgs.). *Ciencia, tecnología y sociedad. Nuevas miradas desde America Latina.* Valparaíso: Ed. Universidad de Valparaíso, 2017.

VICENTIN, Diego. *A reticulação da banda larga móvel:* definindo padrões, informando a rede. 2016. Tese (Doutorado) – Universidade Estadual de Campinas, Instituto de Filosofia e Ciências Humanas, Campinas, 2016.

WIKIPEDIA. Duty cycle. Disponível em: <https://en.wikipedia.org/wiki/Duty_cycle>. Acesso em: 23 abr. 2017.

WIKIPEDIA. Mobile data offloading. Disponível em: <https://en.wikipedia.org/wiki/Mobile_data_offloading>. Acesso em: 23 abr. 2017.

YOUTUBE. LoganCIJ16: Edward Snowden addresses the audience. Disponível em: <https://www.youtube.com/watch?v=OVn55kIzJeA&list=PLS_7b8Iu1oBGXgC-t1y3-i8lUD4gFI2u7S>. Acesso em: 23 abr. 2017.

DA TEORIA À PRÁTICA: A FISCALIZAÇÃO E APLICAÇÃO DA NEUTRALIDADE DA REDE NO BRASIL

PEDRO HENRIQUE SOARES RAMOS
ANDRESSA BIZUTTI ANDRADE

INTRODUÇÃO

Este ensaio procura mapear quais as ferramentas institucionais e regulatórias existentes no Brasil, previstas no Decreto nº 8.771/16 ou não, que podem promover a fiscalização da observância da regra da neutralidade da rede por provedores de acesso, com o objetivo de avaliar se essas ferramentas são ou não suficientes para garantir a aplicação da regra de neutralidade da rede prevista na lei 12.965/14 – "Marco Civil da Internet". Por meio deste trabalho, busca-se fornecer subsídios para que pesquisadores, aplicadores e fiscalizadores de infrações relacionadas ao cumprimento da regra da neutralidade da rede possam compreender com clareza as competências de cada uma das instituições envolvidas no *enforcement* de tal princípio.

A primeira parte traz uma breve descrição do que é a neutralidade da rede, como esse princípio de arquitetura da rede foi regulado por meio do Marco Civil da Internet, bem como uma introdução sobre o Decreto nº 8.771/16, decreto regulamentador do Marco Civil da Internet. A segunda parte apresenta um mapeamento do papel dos principais atores direta ou indiretamente envolvidos na fiscalização e aplicação da regra de neutralidade da rede, relacionando suas funções institucionais com a base legal correspondente. A terceira parte traz um mapa das principais ferramentas decorrentes do ordenamento brasileiro à disposição de usuários para fiscalizarem e exigirem a aplicação da regra de neutralidade da rede por parte de provedores de acesso. A quarta parte traz a conclusão desse trabalho, avaliando se as ferramentas anteriormente mapeadas são ou não suficientes para garantir a efetividade da regra da neutralidade da rede no Brasil e, ao final, a quinta parte contém a bibliografia utilizada ao longo deste estudo.

NEUTRALIDADE DA REDE

A neutralidade da rede é um princípio de arquitetura de rede que endereça aos provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de forma isonômica, não os discriminando em razão de seu conteúdo, origem ou destino. As primeiras formulações a respeito do tema surgiram no início dos anos 2000 (LESSIG, 2001, WU 2002), período em que a expansão da banda larga e a emergência de novas gerações de internet móvel aumentaram o número de dispositivos conectados em um ritmo muito maior do que a expansão física das redes de telecomunicação disponíveis, surgindo evidências de que provedores de acesso estariam discriminando tráfego de aplicações que pudessem ser danosas a seus interesses comerciais – como, por exemplo, aplicações VoIP que competem com serviços de telefonia tradicional.

Ainda que acadêmicos não se afluam em uma única definição sobre a neutralidade, podemos identificar uma série de elementos constitutivos do princípio da neutralidade e que estão presentes nos principais trabalhos a respeito do tema:

I. o princípio da neutralidade da rede impõe a provedores de acesso a obrigação de não bloquear o acesso de usuários a determinados sites e aplicações, sendo também vedado aos provedores de acesso arbitrariamente reduzir a velocidade ou dificultar o acesso entre aplicações idênticas ou similares;

II. a neutralidade da rede impede a cobrança diferenciada para acesso a conteúdos e aplicações específicas, sendo livre a cobrança de tarifas diferenciadas conforme a velocidade de acesso ou volume de banda utilizada; e

III. os provedores de acesso devem manter práticas transparentes e razoáveis a respeito de seus padrões técnicos de gerenciamento de tráfego.

Em 23 de abril de 2014, o Marco Civil da Internet foi sancionado pela então Presidenta Dilma Rousseff, passando a ser a Lei Federal n. 12.965/2014, entrando em vigor dois meses após sua publicação. Por meio do artigo 9º, o Marco Civil da Internet buscou estabelecer um regime de neutralidade da rede *ex ante,* estabelecendo uma regra geral de não discriminação – tal escolha do Marco Civil da Internet mostra-se, inclusive, alinhada com alguns dos mais completos regimes de neutralidade de rede em vigor no mundo. Ao mesmo tempo, a regulação brasileira da neutralidade da rede prevê também a possibilidade de discriminações por requisitos técnicos indispensáveis e em caso de serviços de emergência, estabelecendo regras

de validade para avaliar se essas exceções estão sendo aplicadas de maneira isonômica e proporcional.[1]

Em 11 de maio de 2016, a Presidenta Dilma Rouseff, publicou o Decreto nº 8.771/16, o decreto regulamentador do Marco Civil da Internet. Tal Decreto, expedido pelo Poder Executivo, tem como objetivo regular a aplicação da referida lei.

O Decreto nº 8.771/16 dispõe sobre:

I. as hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego;

II. procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações;

III. medidas de transparência na requisição de dados cadastrais pela administração pública; e

---

1 Art. 9.º do Marco Civil da Internet – O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1.º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da internet e a Agência Nacional de Telecomunicações, Council of Europe.

Council of Europe.

somente poderá decorrer de:

I – requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II – priorização a serviços de emergência

§ 2.º Na hipótese de discriminação ou degradação do tráfego prevista no § 1.º, o responsável mencionado no *caput* deve:

I – abster-se de causar dano aos usuários, na forma do art. 927 do Código Civil;

II – agir com proporcionalidade, transparência e isonomia;

III – informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV – oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3.º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

IV. parâmetros para fiscalização e apuração de infrações contidas no Marco Civil da Internet.[2]

Para o presente estudo, importa analisarmos o item iv supracitado, isto é, os dispositivos do Decreto que tratam da competência para fiscalização da aplicação dos preceitos do Marco Civil da Internet e, mais especificamente, do princípio da neutralidade da rede. Nos próximos itens deste artigo, iremos analisar cada um desses dispositivos, bem como iremos trazer outros exemplos de instituições que apesar de não previstas no Decreto regulamentador também podem atuar como garantidoras da aplicação da neutralidade da rede pelos atores responsáveis.

QUEM FISCALIZA E APLICA A NEUTRALIDADE DA REDE NO BRASIL?

Ao longo da redação do Decreto nº 8.771/16, podemos localizar dispositivos relevantes ao presente estudo, referentes à competência de diferentes atores acerca da fiscalização do cumprimento das regras dispostas no Marco Civil da Internet. Estes são os artigos 5º, §2º; 6º; 17; 18; 19; 20; 21.[3]

---

2 Art. 1º do Decreto nº 8.771/16 – Este Decreto trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indica procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações contidas na Lei nº 12.965, de 23 de abril de 2014.

3 Art. 5º, §2º do Decreto nº 8.771/16 – A Agência Nacional de Telecomunicações – Anatel atuará na fiscalização e na apuração de infrações quanto aos requisitos técnicos elencados neste artigo, consideradas as diretrizes estabelecidas pelo Comitê Gestor da Internet – CGI.br;

Art. 6º do Decreto nº 8.771/16 – Para a adequada prestação de serviços e aplicações na internet, é permitido o gerenciamento de redes com o objetivo de preservar sua estabilidade, segurança e funcionalidade, utilizando-se apenas de medidas técnicas compatíveis com os padrões internacionais, desenvolvidos para o bom funcionamento da internet, e observados os parâmetros regulatórios expedidos pela Anatel e consideradas as diretrizes estabelecidas pelo CGI.br;

Art. 17 do Decreto nº 8.771/16 - A Anatel atuará na regulação, na fiscalização e na apuração de infrações, nos termos da Lei nº 9.472, de 16 de julho de 1997;

Art. 18 do Decreto nº 8.771/16 – A Secretaria Nacional do Consumidor atuará na fiscalização e na apuração de infrações, nos termos da Lei nº 8.078, de 11 de setembro de 1990;

Verificamos que tais disposições fazem menção à quatro instituições relacionadas à aplicação das regras previstas no Marco Civil da Internet: Anatel, CGI.br, CADE – atuando de acordo com o Sistema Brasileiro de Defesa à Concorrência – e a Secretaria Nacional do Consumidor (Senacom). Além disso, segundo o artigo 20 do Decreto, os órgãos devem atuar de forma colaborativa, consideradas as diretrizes do CGI.br, o que significa que todos devem desenvolver conjuntamente ações para garantir a aplicação e fiscalização do princípio da neutralidade da rede.

A seguir iremos analisar as competências de todos esses atores. De qualquer forma, cabe desde já destacar que tais disposições do Decreto regulamentador, ao nosso ver, não são de forma alguma taxativas e, sim, exemplificativas, o que significa que outras instituições podem – e devem – atuar também na fiscalização e aplicação da neutralidade da rede no Brasil. Assim, pelo nosso levantamento, pelo menos outras três instituições possuem importância relevante no *enforcement* da neutralidade da rede: as Fundações Procon, o Ministério Público e, por último, o Poder Judiciário. Esses atores estão também dotados de uma série de ferramentas para exercer essas funções, conforme veremos a seguir.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL)

A Anatel foi criada pela Lei Federal n. 9.472/97 – Lei Geral de Telecomunicações (LGT). O seu papel como agência atuante na aplicação e fiscalização do princípio da neutralidade da rede está expresso nos artigos 5º, §2º, 6º e 17 do Decreto nº 8.771/16. Somado a esses, temos também as competências elencadas no art. 19 da Lei Geral de Telecomunicações que se mostram aplicáveis à efetivação e fiscalização da neutralidade da rede:

Art. 19 do Decreto nº 8.771/16 – A apuração de infrações à ordem econômica ficará a cargo do Sistema Brasileiro de Defesa da Concorrência, nos termos da Lei nº 12.529, de 30 de novembro de 2011;

Art. 20 do Decreto nº 8.771/16 – Os órgãos e as entidades da administração pública federal com competências específicas quanto aos assuntos relacionados a este Decreto atuarão de forma colaborativa, consideradas as diretrizes do CGI.br, e deverão zelar pelo cumprimento da legislação brasileira, inclusive quanto à aplicação das sanções cabíveis, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, nos termos do art. 11 da Lei nº 12.965, de 2014;

Art. 21 do Decreto nº 8.771/16 – A apuração de infrações à Lei nº 12.965, de 2014, e a este Decreto atenderá aos procedimentos internos de cada um dos órgãos fiscalizatórios e poderá ser iniciada de ofício ou mediante requerimento de qualquer interessado.

> Art. 19. À Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente: […] XVI – deliberar na esfera administrativa quanto à interpretação da legislação de telecomunicações e sobre os casos omissos; XVII – compor administrativamente conflitos de interesses entre prestadoras de serviço de telecomunicações; XVIII – reprimir infrações dos direitos dos usuários; XIX – exercer, relativamente às telecomunicações, as competências legais em matéria de controle, prevenção e repressão das infrações da ordem econômica, ressalvadas as pertencentes ao Conselho Administrativo de Defesa Econômica – CADE.

Além das competências supra citadas, como forma de fiscalizar a aplicação do princípio da neutralidade da rede, a Resolução n. 612 da Anatel – que estabelece seu Regimento -=– prevê ao menos dois institutos que podem ser utilizados para averiguação e *enforcement* das regras previstas no Marco Civil da Internet: o Procedimento Administrativo para Averiguação de Denúncia (PAVD), etapa preliminar para investigação da existência de indícios ou fatos que comprovam o fato denunciado e o Procedimento para Apuração de Descumprimento de Obrigações (PADO), cujo julgamento pode aplicar uma das sanções previstas na Lei Geral de Telecomunicações – advertência, multa, suspensão temporária, caducidade ou declaração de inidoneidade. Tanto o PAVD quanto o PADO podem ser iniciados de ofício pela agência ou por quaisquer terceiros interessados (arts. 105 e 80, respectivamente da Resolução n. 162 da Anatel).

SECRETARIA NACIONAL DO CONSUMIDOR (SENACOM)

A Senacom foi criada pelo Decreto nº 7.738, de 28 de maio de 2012. Suas atribuições estão presentes no artigo 3º do Decreto nº 2.181/97.

Em linhas gerais, a Senacom, representa os interesses dos consumidores brasileiros e faz parte do Sistema Nacional de Defesa do Consumidor. Tal órgão possui como atribuições, segundo seu próprio site, "(i) garantir a proteção e exercício dos direitos dos consumidores; (ii) promover a harmonização nas relações de consumo; e (iii) incentivar a integração e a atuação conjunta dos membros da SNDC", entre outros.[4]

Como órgão destinado à proteção dos consumidores, voltado à análise de questões que possuem repercussão nacional e interesse geral, sua atuação na aplicação e fiscalização da neutralidade da rede se mostra relevante.

4 Ver: MINISTÉRIO DA JUSTIÇA. O que é Senacon. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/o-que-e-senacon>. Acesso em: 29 abr. 2017.

A Senacom, segundo o artigo 18 do Decreto nº 8.771/16, é um órgão com competência expressa de fiscalização de infrações envolvendo o Marco Civil da Internet e, portanto, a neutralidade da rede. Além dessa disposição, as competências de tal órgão previstas no artigo 3º do Decreto nº 2.181/97, de uma forma ou outra, auxiliam o *enforcement* das regras do Marco Civil da Internet, seja por meio de conscientização dos consumidores acerca do seu significado e dos mecanismos para garantir sua correta aplicação, ou por meio da aplicação de sanções diretas em casos de violação à neutralidade da rede quando o lesado for o usuário final de internet. Ressaltamos a seguir as principais competências da Senacom que se relacionam ao presente estudo:

> (i) planejamento, coordenação e execução da política nacional de proteção e defesa do consumidor (art. 3º, I), na qual, por exemplo, pode ser inserido um programa para conscientização acerca da neutralidade da rede;
>
> (ii) informação e conscientização dos consumidores (art. 3º,II e III), o que pode ser aplicado à neutralidade da rede;
>
> (iii) solicitar à polícia judiciária a instauração de inquérito para apuração de delito contra consumidores, representação ao Ministério Público e levar ao conhecimento dos órgãos competentes as infrações de ordem administrativa que violarem os interesses difusos, coletivos ou individuais dos consumidores (art. 3, V, VI e VII);
>
> (iv) fiscalizar e aplicar as sanções administrativas na Lei nº 8.078, de 1990[5] e em outras normas pertinentes à defesa do consumidor.

Tais competências se mostram de grande importância para que os consumidores tenham ciência do que é a neutralidade da rede, bem como sua importância para que, consequentemente, saibam quais são seus direitos perante às empresas de telecomunicações. Além disso, a Senacom se mostra relevante também para efetivar o *enforcement* da neutralidade da rede, por meio de fiscalização e aplicação de sanções cabíveis.

CONSELHO ADMINISTRATIVO DE DEFESA DA CONCORRÊNCIA (CADE)

De acordo com seu *site*, o CADE é uma autarquia federal, com o objetivo principal de "zelar pela livre concorrência no mercado", responsável por investigar e decidir sobre a matéria concorrencial e "fomentar a cultura

5 Código de Defesa do Consumidor.

da livre concorrência".[6] As atribuições do CADE estão previstas na Lei nº 12.529/2011, lei esta que estruturou o Sistema Brasileiro de Defesa da Concorrência. De acordo com o *site* do CADE, a entidade exerce três funções principais, conforme análise das disposições do referido texto legal:[7]

> (i) preventiva: analisar e posteriormente decidir sobre as fusões, aquisições de controle, incorporações e outros atos de concentração econômica entre grandes empresas que podem colocar em risco a livre concorrência (art. 9º incisos I, X);
>
> (ii) repressiva: investigar (competência da Super Intendência-Geral do Cade) e posteriormente julgar, por meio do Plenário do Tribunal Administrativo de Defesa Econômica, cartéis e outras condutas nocivas à livre concorrência, aplicando sanções, caso necessário; (art. 9º, incisos I, II, III, IV, V, VI, VII, VIII, XVIII, XIX, Art. 13, incisos III, IV e V);
>
> (iii) educacional: instruir o público em geral sobre condutas que possam prejudicar a livre concorrência (art. 9º, incisos I, XIV, art. 13, incisos XIV, XV, art. 19, IV).

O CADE, segundo o artigo 19 do Decreto nº 8.771/2016, é responsável por apurar infrações à ordem econômica relacionadas ao Marco Civil da Internet e referido Decreto. Esse órgão como entidade garantidora da aplicação da regra da neutralidade da rede atua, portanto, como fiscalizadora de possíveis infrações à ordem econômica cometidas pelos provedores de acesso, e, também, analisando operações societárias que poderiam, de alguma forma, prejudicar a correta aplicação do referido princípio.

O Regimento Interno do CADE (Resolução nº 15, de 25 de maio de 2016) prevê como ocorrerão os procedimentos administrativos, as investigações, as aplicações de sanções e multas em casos de descumprimento. A Lei 12.529/11 estabeleceu, principalmente em seus artigos 9º e 13, diversos mecanismos para que as decisões do CADE sejam de fato cumpridas sendo que estes, aliados às disposições Regimento Interno, permitem o *enforcement* das regras do Marco Civil da Internet, na perspectiva da defesa da ordem econômica.

---

6 CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. O Cade. Disponível em: <http://www.cade.gov.br/acesso-a-informacao/institucional>. Acesso em: 29 abr. 2017.

7 CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. Competências. Disponível em: <http://www.cade.gov.br/acesso-a-informacao/institucional/copy_of_competencias>. Acesso em: 29 abr. 2017.

Por fim, a supracitada lei, também prevê a atuação do CADE em conjunto com outros órgãos, Poder Judiciário, e entidades para assegurar a plena atuação do órgão, no âmbito das suas atribuições. Tal previsão se mostra relevante para a aplicação e fiscalização da neutralidade da rede, pois é de grande importância a atuação conjunta de diversos órgãos para buscar a efetividade de tal regra.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.BR)

O CGI.br foi instituído por meio do Decreto nº 4.829/03. Em linhas gerais, o Comitê tem a "atribuição de estabelecer diretrizes estratégicas relacionados ao uso e desenvolvimento da Internet no Brasil e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP (Internet Protocol) e administração pertinente ao Domínio de Primeiro Nível 'br'".[8] O Comitê também atua na promoção de estudos, procedimentos para a segurança da internet e programas de pesquisa e desenvolvimento com o intuito de garantir a manutenção do nível de qualidade técnica e inovação no uso da internet.

O CGI.br, conforme artigo 2º do Decreto nº 4.829/03, é um comitê multissetorial, com

I. representantes do Ministério da Ciência e Tecnologia, Casa Civil da Presidência da República, Ministério das Comunicações, Ministério da Defesa, Ministério do Desenvolvimento, Indústria e Comércio Exterior, Ministério do Planejamento, Orçamento e Gestão, Agência Nacional de Telecomunicações, Conselho Nacional de Desenvolvimento Científico e Tecnológico;

II. representante do Fórum Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia;

III. representante de notório saber em assuntos de internet;

IV. quatro representantes do setor empresarial, nos segmentos de provedores de acesso e conteúdo da internet, provedores de infraestrutura de telecomunicações, indústria de bens de informática, de bens de telecomunicações e de software e setor empresarial usuário;

V. quatro representantes do terceiro setor;

VI. três representantes da comunidade científica tecnológica.

8 Ver: CGI.BR. Sobre. Disponível em: <https://www.cgi.br/sobre/>. Acesso em: 29 abr. 2017.

O CGI.br aparece em quatro artigos do Decreto nº 8.771/2016 como órgão consultivo, no qual seus estudos e diretrizes devem ser utilizados pelos órgãos fiscalizadores (artigos 5º,§2º, 6º, 13, §1º[9] e 20). O papel do CGI.br, portanto, não é de fiscalização ou aplicação da neutralidade da rede, mas sim de fornecimento de embasamento técnico para que os devidos órgãos tenham conhecimento suficiente para atuar na aplicação e fiscalização de tal princípio.

Este papel é de grande importância. A neutralidade da rede é um tema pouco difundido e que requer conhecimento técnico específico para ser integralmente compreendido, sendo que o entendimento por completo de tal princípio é essencial para que a aplicação e fiscalização deste seja efetiva. Assim, o CGI.br, como órgão especializado, tem a função de garantir que os outros órgãos compreendam a presente temática para garantir uma atuação eficiente destes em relação à neutralidade da rede.[10]

Por fim, destacam-se as capacidades indutora e articuladora do CGI.br. A primeira é a capacidade técnica e legitimidade institucional para realização de estudos e pesquisas para atores do mercado e órgãos fiscalizadores, em relação às melhores práticas, nacionais e internacionais, relacionadas à neutralidade da rede e suas exceções. Já a capacidade articuladora relaciona-se ao papel multissetorial do CGI.br, permitindo sua articulação em diferentes setores e instituições. Tais capacidades estão diretamente relacionadas a sua função de criador de diretrizes para a correta aplicação e fiscalização do princípio da neutralidade da rede.

---

9 Art. 13, §1º do Decreto 8.771/2016 – Cabe ao CGI.br promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificados e o porte dos provedores de conexão e de aplicação.

10 No mesmo sentido, as competências da CGI.br estabelecidas ao longo do artigo 1º do Decreto 4.829/03 se mostram relevantes: estabelecimento de diretrizes estratégicas para o desenvolvimento da internet (art. 1º, I); realização programas de pesquisa e desenvolvimento relacionado à internet (art. 1º, III); promoção de estudos e recomendações de procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de internet (art. 1º, IV); articulação de ações relativas à proposição de normas e procedimentos relativos à regulamentação das atividades inerentes à internet (art. 1º, V); adoção de procedimentos administrativos e operacionais necessários para que a gestão da internet se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da internet, podendo celebrar acordo, convênio, ajustes ou instrumento congênere (art. 1º, VII); deliberar sobre quaisquer questões a ele encaminhadas, relativamente aos serviços de internet (art. 1º VIII).

FUNDAÇÕES PROCON

As Fundações Procon são órgãos estaduais ou municipais de proteção e defesa do consumidor que atuam na execução da "Política Nacional de Defesa do Consumidor". Tais órgãos não estão previstos expressamente no Decreto nº 8.771/16 como atuantes da aplicação e fiscalização do Marco Civil da Internet, mas suas competências regulamentais se mostram relevantes para o *enforcement* da neutralidade da rede, razão pela qual tais instituições merecem ser estudas no presente artigo.

Como podem ser municipais ou estaduais, cada munícipio e/ou estado possuem a própria legislação acerca do funcionamento do seu próprio Procon. Porém, o Decreto nº 2.181/97 estabelece, em seu artigo 4º, quais as atividades que devem ser exercidas por tais órgãos.

Segundo os termos do artigo supracitado, as atividades dos Procons são aquelas presentes no artigo 4º e nos incisos II a XII do artigo 3º. Por atuar perante o mercado consumidor, as competências dos Procons estão diretamente conectadas às competências da Senacon.

A principal diferença de atuação da Senacom em relação aos Procons, é que enquanto a primeira instituição se volta à análise de questões que possuem repercussão nacional e interesse geral, os Procons prestam atendimento e auxílio direto ao consumidor (Art. 4º, II do Decreto nº 2.181/97). Isso não significa, porém, que os Procons não tenham atuação genérica, ou que a Senacon não possa prestar auxílio direto ao consumidor. Significa apenas que os focos de ambas instituições são diferentes, o que faz sentido, levando em consideração que o Senacom é um órgão do governo federal, enquanto as Fundações Procon atuam de forma localizada, mais próximas das demandas dos consumidores.

Diante de tais atribuições do Procon, sua atuação como entidade envolvida na aplicação e fiscalização das regras previstas no Marco Civil da Internet nos parece importante. Trata-se de instituição próxima ao consumidor, que poderá, diretamente, receber reclamações e denúncias e fazer o intermédio entre ele e as empresas, bem como fiscalizar a atuação dos provedores de acesso, e aplicar sanções por possíveis violações.

MINISTÉRIO PÚBLICO

O Ministério Público é instituição prevista constitucionalmente (Art. 127 da Constituição Federal), considerado essencial à função jurisdicional do Estado, com a competência de defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis e no controle

externo da atividade policial. Na legislação infraconstitucional, é previsto na Lei Complementar nº 75/1993, que trata especificamente do Ministério Público da União, bem como na Lei nº 8.625/1993.

O artigo 25 da Lei nº 8.625/93, na alínea a do inciso IV, dispõe que o Ministério Público poderá promover inquérito civil e ação civil pública, a fim de proteger, prevenir e reparar danos causados ao consumidor. Isto significa que essa instituição pode investigar provedores de acesso que, por ventura, descumpram a regra de neutralidade da rede, por meio de inquérito civil, para posteriormente, se for o caso, propor ação civil pública contra tal provedor. Para instruir o inquérito civil, o Ministério Público pode atuar em conjunto com outros órgãos e entidades, públicas ou privadas (art. 26, I, b, c), requerendo informações e esclarecimentos.

Diferentemente de outros órgãos aqui citados, o Ministério Público não tem competência para aplicar multas ou sanções por descumprimento da legislação ou por ações que gerem prejuízos ao consumidor. De outro lado, tal órgão pode estabelecer acordos para cessação de condutas – os chamados Termos de Ajustamento de Conduta – caso verifique alguma ação irregular por determinado provedor de acesso, no qual esse, extrajudicialmente, assina documento em que, dentre outras estipulações, se compromete a cessar a conduta ilegal.

Além disso, como parte legítima a propor ações civil públicas a fim de proteger os interesses consumeristas, o Ministério Público aparece como uma importante instituição fiscalizadora das regras do Marco Civil da Internet que pode atuar judicialmente para garantir o *enforcement* do princípio da neutralidade da rede, caso verifique seu descumprimento.

JUDICIÁRIO

Independentemente de todas as entidades aqui citadas, o Poder Judiciário é a última instância de controle da aplicação e fiscalização da regra da neutralidade da rede.

Apesar de necessitar que algum agente proponha ação a fim de discutir a regularidade dos serviços prestados pelo provedor de acesso, o que for decidido no judiciário prevalecerá. Assim, órgãos de *enforcement* das regras do Marco Civil da Internet que possuem processos administrativos internos, com possível efeito sancionador, como Anatel, Cade, Senacon e Procons, podem ver suas decisões reformadas totalmente na via judicial, caso seja auferida eventual ilegalidade.

Isso, de forma alguma, deslegitima a atuação dessas entidades aqui citadas, uma vez que o Poder Judiciário sozinho não tem competência para agir sem que alguma parte apresente a devida demanda. Assim, o Poder Judiciário não consegue sozinho garantir a aplicação e fiscalização da neutralidade da rede, sendo necessária a atuação das outras instituições que foram analisadas durante este estudo.

AVALIAÇÃO DOS PAPÉIS IDENTIFICADOS

A partir do mapeamento realizado supra, podemos identificar que há pelo menos três tipos de competências legislativas atribuídas aos atores supra elencados, e que são relevantes para o *enforcement* da neutralidade da rede. Em primeiro lugar, identifica-se a função de articulação, em que os atores são dotados de competências para, em conjunto com outros atores, propor modelos de fiscalização e aplicação. Segundo, identifica-se uma função de defesa de direitos difusos, em que os atores possuem competência para defender grupos de interesse para que direitos estabelecidos em lei possam ser, de fato, gozados pela sociedade. Finalmente, temos uma função de aplicação de sanções, em que os atores são dotados de competência para o controle de comportamento social por meio do estabelecimento de sanções pelo descumprimento das regras estabelecidas pelo Marco Civil da Internet.

A seguir, apresentamos uma representação gráfica de tais funções e quais instituições atuam em cada uma das esferas:

Figura 1 - Representação Funcional das Instituições Fiscalizadoras da Neutralidade da Rede

Fonte: Elaboração dos autores.

FERRAMENTAS PARA FISCALIZAÇÃO E APLICAÇÃO

Nesta parte do presente artigo traremos um mapa das principais ferramentas, decorrentes do ordenamento brasileiro, à disposição de usuários para fiscalizarem e exigirem a aplicação da regra de neutralidade da rede por parte de provedores de acesso.

INVERSÃO DO ÔNUS DA PROVA (CDC)

O Código de Defesa do Consumidor, em seu artigo 6º, inciso VIII, no capítulo acerca dos direitos básicos do consumidor, garante ao consumidor a inversão do ônus da prova, a seu favor, quando as alegações deste forem verossímeis ou quando ele for hipossuficiente.

No caso da aplicação da neutralidade da rede, a inversão do ônus da prova parece ter um papel fundamental. Basicamente, transfere aos provedores de acesso a obrigação de provarem que estão entregando o serviço contratado pelo consumidor devidamente, seguindo os preceitos do Marco Civil da Internet, ao invés de determinar que o próprio consumidor prove que o serviço não está sendo prestado de forma correta, o que lhe imporia notórias dificuldades, diante da sua clara hipossuficiência técnica.

Assim, em caso de dúvida fundamentada, pelo consumidor, de que seu provedor de acesso não está cumprindo com o que ora foi contratado, ele poderá acionar o Poder Judiciário e requerer que o próprio provedor de acesso prove que está prestando devidamente seus serviços. Trata-se, portanto, de forte ferramenta para que o consumidor possa fiscalizar e exigir a correta aplicação da regra da neutralidade da rede, via judiciário.

DIREITO DE INFORMAÇÃO

Previsto tanto no Código de Defesa do Consumidor (art. 6º, III), como no Marco Civil da Internet (art.7, VI), o direito de informação garante ao consumidor e usuário da internet informações claras e completas acerca dos serviços por ele contratados.

Trata-se de importante ferramenta para conscientização do consumidor acerca da neutralidade da rede, pois fornece ao usuário de internet acesso a maiores subsídios para compreender o que tal regra significa, e, consequentemente, fiscalizar a devida aplicação da regra da neutralidade.

Caso o usuário de internet, consumidor, desconfie que o serviço contratado não está sendo entregue da forma devida pelo provedor de acesso, e não consiga tal informação perante a empresa prestadora do serviço, poderá acionar o Poder Judiciário, utilizando o direito à inversão do ônus da prova, mencionado supra e requerer que as empresas de telecomunicação comprovem o cumprimento de suas obrigações legais.

DIREITOS PREVISTOS NO REGULAMENTO GERAL DE DIREITOS DO CONSUMIDOR DE SERVIÇOS DE TELECOMUNICAÇÕES

Além do *site* da Anatel possuir uma seção inteira dedicada apenas aos consumidores, a Anatel aprovou, em 7 de março de 2014, a Resolução nº 632 que aprovou o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações.

Ao longo dos incisos do artigo 3º do Regulamento, são listados diversos direitos do consumidor de serviços de telecomunicações que devem ser respeitados pelos provedores de acesso. Para o *enforcement* da regra de neutralidade da rede, importante destacar os incisos IV, IX, X e XI.

Primeiramente, o inciso IV dispõe acerca do direito de informação, já tratado no item supra, mas especificamente sobre o setor de telecomunicações. O inciso IX trata do direito à resposta eficiente e tempestiva, pela prestadora de serviços de telecomunicações às reclamações dos usuários, solicitações de serviços e pedidos de informação. Já o inciso X determina que é direito do consumidor o encaminhamento de reclamações ou representações contra a prestadora, junto à Anatel ou aos organismos de defesa do consumidor. Por último, o inciso XI prevê, como direito do consumidor, a reparação pelos danos causados pela violação dos seus direitos.

A partir da análise destes quatro incisos verificamos que eles se comunicam e se completam. Ao consumidor é dado o direito à informação completa acerca dos serviços prestados pelos provedores de acesso, mas caso ele necessite de informações complementares, pode requerer diretamente à prestadora e ela terá a obrigação de conceder tais informações de forma eficiente e tempestiva. Caso o consumidor não se veja satisfeito, poderá realizar uma reclamação direta perante à Anatel ou aos órgãos de defesa do consumidor – Senacom e Procon – e, por fim, poderá ser ressarcido pelos danos sofridos, caso cabível.

Assim, caso o consumidor duvide da correta aplicação dos dispositivos do Marco Civil da Internet poderá, antes de discutir a questão diretamente diante do Poder Judiciário, tentar solucionar a situação tanto perante à própria empresa prestadora dos serviços, como junto à Anatel ou órgãos de defesa do consumidor – que foram tratados na segunda parte 2 deste artigo.

CONCLUSÃO

Os mapeamentos realizados supra parecem-nos apontar para as seguintes conclusões:

I. parece-nos que há mecanismos legais bem desenvolvidos, em especial no que se refere às atribuições dos órgãos responsáveis pela articulação, defesa de direitos difusos e aplicação de sanções em caso de descumprimento da neutralidade da rede. Assim, entendemos que as ferramentas, se devidamente aplicadas, são suficientes para garantir o *enforcement* da neutralidade da rede;

II. com exceção do CGI.br, observa-se que os atores responsáveis legalmente pela aplicação e fiscalização da neutralidade da rede possuem competência genérica e nenhum deles parece ter desenvolvido, ainda, um corpo de conhecimento técnico suficiente para entender com clareza suas funções institucionais. Assim, não se verifica ações estruturadas por estes órgãos para garantir a efetividade da neutralidade da rede no Brasil; e

III. apesar do Poder Judiciário ser uma solução, o acesso a este ainda é uma barreira para consumidores, por conta dos custos envolvidos e a demora na resposta às demandas apresentadas, o que acaba por desestimular que consumidores busquem direitos legalmente garantidos. Assim, realização de reclamações perante a Anatel e órgãos de proteção aos consumidores nos parecem mais efetivas e céleres.

Como encaminhamento para futuros estudos, sugere-se que se investigue como os atores institucionais envolvidos com a aplicação possam desenvolver grupos de trabalho específicos para aumentar a efetividade e fiscalização da neutralidade da rede, bem como criar ferramentas que possam permitir a maior transparência de práticas de gerenciamento de tráfego.

REFERÊNCIAS

CADE. COMPETÊNCIAS. Disponível em: <http://www.cade.gov.br/acesso-a-informacao/institucional/copy_of_competencias>. Acesso em: 29 abr. 2017.

CADE. O CADE. Disponível em: <http://www.cade.gov.br/acesso-a-informacao/institucional>. Acesso em: 29 abr. 2017.

CGI.br. Sobre o CGI.br. Disponível em: <https://www.cgi.br/sobre/>. Acesso em: 29 abr. 2017.

CGI.BR. Sobre. Disponível em: <https://www.cgi.br/sobre/>. Acesso em: 29 abr. 2017.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. Competências. Disponível em: <http://www.cade.gov.br/acesso-a-informacao/institucional/copy_of_competencias>. Acesso em: 29 abr. 2017.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. O Cade. Disponível em: <http://www.cade.gov.br/acesso-a-informacao/institucional>. Acesso em: 29 abr. 2017.

LESSIG, L. The Internet Under Siege. *Foreign Policy*, 2001.

MINISTÉRIO DA JUSTIÇA. O que é Senacon. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/o-que-e-senacon>. Acesso em: 29 abr. 2017.

RAMOS, P. H .S. *Arquitetura da rede e desenvolvimento:* a regulação da neutralidade da rede no Brasil. São Paulo: Fundação Getúlio Vargas, 2015.

SENACON. O que é Senacom. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/o-que-e-senacon>. Acesso em: 29 abr. 2017.

WU, T. *A Proposal for Network Neutrality.* Charlottesville: University of Virginia, 2002.

FERRAMENTAS AUXILIARES PARA MEDIÇÃO DA NEUTRALIDADE DA REDE PELOS USUÁRIOS

NATHALIA SAUTCHUK PATRÍCIO

INTRODUÇÃO

Uma rede neutra é aquela em que não há o favorecimento de uma aplicação em detrimento de outra (WU, 2013). A neutralidade da rede pode ser melhor definida como um princípio de projeto de redes. A ideia é a de que uma rede de informação pública útil aspira tratar todos os conteúdos, *sites* e plataformas de forma igual (WU, [s.d.]). Isso significa, por exemplo, que um pacote transportando conteúdos de uma ligação por voz não pode ser transmitido mais lentamente que um pacote de mesmo tamanho contendo informações de um *e-mail*. Nos estudos de redes de computadores, a neutralidade tem por ancestral o princípio fim a fim. Segundo Kurose e Ross (2013) esse princípio afirma que, visto ser dado certo que certas funcionalidades – detecção de erro, por exemplo – devem ser executadas fim a fim, funções colocadas nos camadas mais baixas da Internet podem ser redundantes ou adicionar pouco valor em comparação ao custo de implementá-las em uma camada mais alta. Ou seja, em uma rede de uso geral, como a Internet, funções específicas das aplicações devem estar nos dispositivos terminais da rede ao invés de nos nós intermediários, como roteadores e repetidores (WU, [s.d.]).

Dentre os temas debatidos no campo da governança da Internet, o conceito de neutralidade da rede tem causado polêmica no Brasil e em outros países e por isso tem cada vez mais atraído a atenção da opinião pública internacional. De um lado, provedores de conteúdo e comunidade técnica defendem o modelo de neutralidade, de outro lado, empresas de telecomunicações vislumbram formas de maximizar seus lucros por meio da cobrança de vias rápidas – *fast lanes*, em inglês – para o tráfego de dados, ou por meio de outros artifícios que beneficiam ou prejudicam certo tipo, origem ou destino de tráfego de dados em detrimento dos demais.

Apesar desse cenário de disputa, a Lei nº 12.965, conhecida como Marco Civil da Internet, está em vigor desde 2014 e garante no Brasil a neutralidade da rede na Internet (BRASIL. Lei 12.965, 2014, Art. 3º, IV). Estão previstos alguns casos em que a discriminação e a degradação de tráfego podem ser executadas pelo provedor de conexão a Internet, porém estes são tratados como uma exceção.

De acordo com Ramneek *et al*. (2015), uma lei aceitável para a neutralidade da rede deve ser uma combinação objetiva de aspectos políticos e técnicos, enquanto leva em consideração o mínimo de requisitos de qualidade de experiência do usuário final. Dentro desse contexto, duas questões são relevantes para este artigo:

I. como fiscalizar ou verificar tecnicamente se a neutralidade da rede tem sido cumprida pelos provedores;

II. a ocorrência de discriminação de tráfego apenas nos casos previstos pelo Marco Civil da Internet.

Se no Brasil não há estudos publicados relativos a esse tema, em outros países a questão da medição da neutralidade da rede é tratada de maneira parcial e fragmentada por meio de um conjunto de iniciativas não coordenadas entre si.

Esse texto está estruturado em quatro seções. Na primeira seção é apresentada um pouco da discussão sobre a neutralidade da rede, inclusive no contexto do Marco Civil da Internet. A segunda seção é dedicada às métricas de rede enquanto a terceira seção apresenta algumas ferramentas que se propõem a medir a neutralidade da rede. Por fim, na seção quatro são apresentadas algumas considerações sobre os desafios para fiscalizar tecnicamente a neutralidade da rede de acordo com o Marco Civil da Internet.

NEUTRALIDADE DA REDE NO CONTEXTO DO MARCO CIVIL DA INTERNET

A neutralidade da rede é um tema que tem sido debatido desde o início dos anos 2000 e continua envolto em muita polêmica. Existem diversas definições para ela, sendo uma dentre elas:

> A neutralidade é um princípio que está no cerne do funcionamento da Internet e estabelece tratamento isonômico ao tráfego de pacotes de dados na Internet, não fazendo distinção de acordo com conteúdo, origem e destino, serviço, terminal ou aplicação, sendo que a Internet apenas transportará os pacotes de dados, deixando para o usuário final as decisões em relação ao tipo de uso que fará e aos dados que acessará. (SANTOS, 2016)

De acordo com Santos (2016), para muitos autores que estudam o assunto, uma Internet neutra garante um ambiente propício às inovações tecnológicas, protege a liberdade de expressão, fomenta oportunidades de desenvolvimento socioeconômico além de facilitar a difusão e compartilhamento de bens culturais.

Porém, a manutenção de uma Internet neutra não é algo simples, uma vez que nesse ecossistema há diversos atores com diferentes interesses em relação ao funcionamento rede.

Ramos (2015) coloca que, no caso dos provedores de conexão a Internet, ao serem impedidos de discriminar conteúdos e aplicações, eles perdem um instrumento de controle de suas redes, o que pode levar a redução de lucros e diminuição do potencial de eficiência de suas redes. Essas perdas podem levar à redução de incentivos para inovação na infraestrutura de telecomunicações e à redução na geração de empregos do setor.

Já para os grandes provedores de aplicações a neutralidade da rede tem um papel dúbio. Com a garantia da neutralidade, eles não precisam negociar condições especiais para o tráfego de seus conteúdos com os provedores de conexão, e assim poderiam investir mais recursos em inovação e geração de empregos. Por outro, a proibição de acordos para priorização de tráfego reduz os instrumentos disponíveis para que eles mantenham sua hegemonia, tendo em vista que pequenos provedores terão condições de oferta semelhantes (RAMOS, 2015).

Segundo Ramos (2015) os pequenos provedores de aplicações são beneficiados pela neutralidade da rede, uma vez que, com o tráfego de seus conteúdos sendo tratados da mesma forma que o dos grandes, há uma redução nas barreiras de entrada no mercado. Eles não vão precisar negociar com provedores de conexão para terem uma oferta de qualidade de seus aplicativos, e a maior diversidade de iniciativas levará a um aumento na inovação como um todo.

Os usuários também se beneficiam com a neutralidade da rede, pois terão acesso a conteúdos mais diversificados, impedindo efeitos de filtro de conteúdo que são hoje aplicados pelos grandes provedores de aplicações. Há um ganho na capacidade de autonomia, já que usuários terão maiores incentivos para também se tornarem provedores de aplicação, bem como ganhos expressivos no campo da liberdade de expressão, uma vez que a neutralidade da rede impediria que provedores de conexão criem bloqueios de conteúdo. Por outro lado, há uma potencial consequência negativa que

é o aumento de custos de acesso para *heavy users*[1] de aplicações específicas (RAMOS, 2015).

Segundo Ramos (2015) um provedor de conexão a Internet pode discriminar um conteúdo ou uma aplicação específica na Internet, violando a neutralidade da rede através da:

- restrição completa de acesso a determinadas aplicações;
- redução da velocidade de acesso a determinadas aplicações ou classe de aplicações;
- aumento da velocidade de acesso a determinadas aplicações específicas;
- cobrança de tarifas adicionais para acesso a determinadas aplicações ou classe de aplicações; e
- redução de tarifas para acesso a determinadas aplicações.

No contexto do Marco Civil da Internet, o artigo 9º diz que "o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação". Apenas há a previsão de discriminação ou degradação do tráfego em casos de requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e priorização de serviços de emergência (BRASIL. Lei 12.965, 2014, Art. 9º, § 1º).

A questão da neutralidade da rede foi regulamentada pelo artigo 5º do Decreto 8.771 (BRASIL, 2016), no qual foram explicitados os requisitos técnicos indispensáveis à prestação adequada dos serviços, sendo aqueles decorrentes de:

I. tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa – *spam* – e controle de ataques de negação de serviço;

II. tratamento de situações excepcionais de congestionamento de redes, tais como rotas alternativas em casos de interrupções da rota principal e em situações de emergência.

1 Algumas empresas de conexão à Internet usam o termo *heavy users* com a intenção de distinguir usuários com "uso aceitável" de banda e outros que fazem um alto uso e, de certa forma, indevido. Esse termo tem sido usado como justificativa para diversas restrições, como a implementação de franquia de dados e *traffic shaping*.

MÉTRICAS DE REDE

Existem diversas métricas que são usadas para mensurar o desempenho de uma rede de computadores, incluindo a Internet. Essas métricas podem ser exploradas para ajudar as autoridades competentes e aos usuários finais na fiscalização da neutralidade da rede de acordo com o Marco Civil da Internet.

Uma das principais métricas é a vazão – em inglês, *throughput* –, podendo ser de dois tipos: instantânea e média. Segundo Kurose e Ross (2013) a vazão instantânea é a taxa – em *bits/s* – em que um dispositivo está recebendo um arquivo em um determinado momento. Já a vazão média consiste na quantidade de *bits* que foram transferidos em uma unidade de tempo. Por exemplo, se o arquivo consistir em F *bits* e a transferência levar T segundos para o dispositivo receber todos os F *bits*, então a vazão média da transferência do arquivo é F/T bits/s (KUROSE e ROSS, 2013). Quando se fala especificamente no protocolo TCP[2] (KUROSE; ROSS, 2013), a RFC[3] 6349 define vazão como a quantidade de dados por unidade de tempo que o TCP transporta quando está em estado de equilíbrio (IETF, 2001).

Existe uma outra métrica similar a vazão, conhecida como *goodput*. Segundo Tanenbaum e Wetherall (2011), *goodput* é a taxa em que pacotes úteis são entregues pela rede. Na RFC 2647, *goodput* é definido como o número de *bits* por unidade de tempo encaminhados para a interface correta de destino de um dispositivo conectado à rede, menos os *bits* perdidos ou retransmitidos (IETF, 1999). Comparando-se *throughput* e *goodput*, pode-se dizer que essas métricas se diferem uma vez que o *goodput* não leva em conta os dados dos protocolos, como os cabeçalhos e a retransmissão de pacotes, enquanto o *throughput* considera tudo isso em sua medição.

Outras duas métricas relevantes para redes em geral são o atraso – ou latência – e a variação de atraso – *jitter*. De acordo com Kurose e Ross (2013), o atraso fim a fim é o acúmulo de atrasos de processamento, transmissão e de formação de filas nos roteadores; atrasos de propagação nos enlaces e atrasos de processamento em sistemas finais. O atraso ou a latência de uma rede é geralmente variável e depende basicamente das condições de carga dos diversos segmentos envolvidos (CARISSIMI *et al.*,

2 TCP (Transmission Control Protocol) é o protocolo encarregado do transporte dos pacotes de dados pelas diferentes rotas da Internet.

3 Um RFC (Request For Comments) pode ser um documento de padronização da Internet, um documento informativo ou um documento de boas práticas. Ele é desenvolvido no âmbito do Internet Engineering Task Force (IETF).

2009). Um componente crucial do atraso fim a fim são os atrasos variáveis de fila que os pacotes sofrem nos roteadores. Por isso, o tempo decorrido entre o momento em que um pacote é gerado na fonte e o momento em que é recebido no destinatário pode variar de pacote para pacote, o que é denominado de variação de atraso (KUROSE; ROSS, 2013).

Outro aspecto importante em uma rede é a questão da perda de pacotes. Kurose e Ross (2013) afirmam que, do ponto de vista de um sistema final, a perda de pacote é vista como um pacote que foi transmitido para o núcleo da rede, mas sem nunca ter emergido dele no destino. As filas dos roteadores são finitas e, portanto, podem estar cheias em um determinado instante de tempo. Se um pacote chegar nessas condições, o roteador o descartará por não ter espaço em memória para armazená-lo. Quanto maior for a intensidade de tráfego, maior será a fração de pacotes perdidos pelo descarte. Sendo assim, o desempenho em um nó da rede não é medido apenas em termos de atraso, mas também da probabilidade de perda de pacotes (KUROSE; ROSS, 2013).

Por fim, outras duas métricas que podem ajudar na análise de uma rede são o tempo de viagem de ida e volta – em inglês *round-trip time* (RTT) – e a taxa de entrega média – em inglês, *packet delivery ratio*. De acordo com Kurose e Ross (2013) o RTT é o tempo que leva para um pequeno pacote viajar do cliente ao servidor e de volta ao cliente, incluindo atrasos de propagação de pacotes, de fila de pacotes em roteadores e comutadores intermediários e de processamento de pacotes. Já a taxa de entrega média é a razão entre a quantidade de pacotes de dados recebidos e a quantidade de pacotes de dados enviados (HARRISMARE, 2011; CHENG *et al.*, 2012).

Quando se pensa em caracterizar o desempenho de uma rede, as métricas apresentadas são importantes. No caso da vazão e da taxa de entrega, quanto maiores forem os seus valores, melhor será o desempenho da rede. Já no caso do atraso fim a fim, quanto menor o valor dele melhor será o desempenho.

Segundo Kurose e Ross (2013) é desejável, para algumas aplicações ter um atraso baixo e uma vazão instantânea acima de algum patamar – por exemplo, superior a 24kbits/s para aplicações de telefonia via Internet, e superior a 256 kbits/s para algumas aplicações de vídeo em tempo real. Já outras aplicações, incluindo as de transferência de arquivo, o atraso não é importante, mas é recomendado ter a vazão mais alta possível (KUROSE; ROSS, 2013).

Kurose e Ross (2013) também afirmam que, para aplicações de áudio interativas em tempo real, como o VoIP, atrasos fim a fim menores do que 150ms não são percebidos pelo ouvido humano; enquanto 150 a 400ms podem ser aceitáveis, apesar de não ideais e os que excedem 400ms atra-

palham seriamente a interatividade. Normalmente, o lado receptor de uma aplicação de telefone por Internet desconsiderará quaisquer pacotes cujos atrasos ultrapassam um determinado patamar, sendo que esses pacotes são efetivamente perdidos (KUROSE; ROSS, 2013).

FERRAMENTAS DISPONÍVEIS PARA MEDIÇÃO DA NEUTRALIDADE DA REDE

De acordo com Miorandi *et al*. (2013), a análise técnica da neutralidade da rede de um provedor em relação a uma aplicação específica requer uma investigação profunda do seu comportamento de comunicação, o que é extremamente complexo. A impossibilidade de se conhecer a arquitetura completa da Internet dificulta essa análise, sendo comum a medição da comunicação entre duas pontas. Há três metodologias de medição que diferem entre si na forma em que os dados são gerados e coletados para análise futura:

- ativa: são gerados pacotes de dados específicos para serem trafegados pela rede do provedor com o objetivo de serem medidos algumas métricas técnicas – como *jitter*, vazão, etc;
- passiva: os pacotes trafegados pela rede do provedor são logados e são extraídos indicadores de desempenho relevantes para serem analisados; e
- híbrida: é a combinação das metodologias ativa e passiva.

As ferramentas existentes para detectar discriminações são tipicamente específicas para uma aplicação ou para um mecanismo específico de discriminação e dependem de testes de medição ativos (MIORANDI *et al*., 2013; RAMNEEK, 2015b).

Existem ferramentas que se propõem a fazer a medição de métricas que podem ser usadas como indicadores da violação da neutralidade da rede. Porém, muitas delas ainda são experimentais, fazendo parte de pesquisas na área de redes. Neste trabalho, foram escolhidas cinco ferramentas com abordagens distintas que podem ser aplicadas na medição da neutralidade de rede para serem analisadas em profundidade.

O Neubot é uma dessas ferramentas que mede vários indicadores de forma ativa, incluindo vazão, atraso, *jitter*, assim como o desempenho de protocolos específicos comumente usados, incluindo o Real-Time Transport Protocol – usado na maioria das aplicações de multimídia na Internet –, o protocolo *peer-to-peer* BitTorrent e o protocolo proprietário *peer-to-peer* do Skype Voice over IP (DE MARTIN; GLORIOSO, 2008). A arquitetura do

Neubot é do tipo cliente-servidor.[4] Usuários voluntários podem instalar em seus computadores uma aplicação cliente *open-source*.[5] A aplicação cliente roda em *background* e automaticamente realiza um conjunto de medidas, periodicamente enviando resultados para um servidor central.

Segundo Ramneek (2015b), o ponto forte do Neubot é o monitoramento contínuo da conexão do usuário final em oposição ao envio de pacotes de sondagem aos provedores. Porém, a variação no desempenho pode resultar de outros fatores como por exemplo o congestionamento da rede, anulando a hipótese de discriminação realizada pelo provedor.

Outra ferramenta de medição ativa é a Glasnost, que detecta diferenciação de tráfego baseado tanto nos parâmetros do cabeçalho do protocolo de transporte (número da porta[6]) (KUROSE; ROSS, 2013) quanto no *payload* do pacote – também conhecido como *Deep Packet Investigation* – (MIORANDI *et al*., 2013). Ela é baseada na arquitetura cliente-servidor. Cada cliente se conecta a um servidor através do navegador *web*, rodando diversos testes. Cada teste mede o caminho entre cliente e servidor gerando *streams* de tráfego no nível da aplicação. A ideia principal da Glasnost é a emulação de dois streams de tráfego transportando dados, idênticos em todos os sentidos, menos na característica suspeita de provocar a discriminação ao longo do caminho. Por exemplo, no caso do teste do protocolo BitTorrent, metade dos fluxos de teste usam a porta 6881, uma porta conhecida por ser usada pelo protocolo BitTorrent, enquanto a outra metade usa uma porta aleatória não associada a nenhum protocolo específico (DISCHINGER *et al*., 2008). Essa ferramenta possui página web em que se podia testá-la diretamente através de um navegador.[7]

---

4 A arquitetura cliente-servidor é aquela em que há dispositivos que disponibilizam conteúdos (servidores) para serem acessados por outros (clientes). Ela se contrapõe à arquitetura *peer-to-peer*, em que um dispositivo pode fazer o papel tanto de cliente quanto de servidor ao mesmo tempo. O BitTorrent utiliza a arquitetura *peer-to-peer*.

5 O guia de instalação do cliente do Neubot pode ser encontrado em: NETWORK MEASUREMENTS FROM THE EDGES. Neubot install guide. Disponível em: <http://neubot.org/neubot-install-guide>. Acesso em: 15 abr. 2017.

6 Cada número de porta é um número de 16 bits na faixa de 0 a 65535. Os números de porta entre 0 e 1023 são denominados números de porta bem conhecidos e são reservados para utilização por protocolos de aplicação bem conhecidos, como HTTP (porta 80) e FTP (porta 21). Quando se desenvolve uma nova aplicação é necessário atribuir a ela um número de porta.

7 Após 8 anos em funcionamento, a ferramenta Glasnost foi descontinuada em 2017, uma vez que foi desenvolvida como Java applet e os navegadores modernos não possuem mais suporte a essa tecnologia. Informações sobre a ferramenta podem ser

Além de mostrar os resultados das medições, a ferramenta Glasnost dava um veredicto sobre a discriminação de pacotes na rede. As mensagens exibidas na interface da ferramenta podem conter basicamente três indicações:

1. não há evidência que o provedor limita o tráfego de *upload/download*;
2. os dados medidos apresentam muito ruído para detectar se o provedor limita o tráfego de *download/upload* e era pedido para que os testes fossem rodados novamente assegurando que não havia outros processos fazendo *download/upload*;
3. o provedor parece limitar o *download/upload*, embora algumas das medições possam ser afetadas por ruído, o que limita a habilidade de detecção pela ferramenta.

A Glasnost também apresentava alguns detalhes do porquê fazia suas avaliações. Por exemplo, no caso de uma possível limitação poderia ser mostrada a seguinte mensagem: "Seu provedor parece permitir uma banda maior para *downloads* usando o protocolo HTTP[8]. Em nossos testes, *downloads* usando fluxos de controle atingiram a taxa de no máximo 226 Kbps enquanto downloads usando HTTP atingiram até 1597 Kbps". No caso em que não parecia haver limitação poderia ser exibida uma mensagem similar a essa: "Não há indicação de que seu provedor limite os *downloads* na porta 8080[9] ou na 57732. Em nossos testes, os *downloads* na porta 8080 atingiram taxas de até 1416 Kbps enquanto os *downloads* pela porta 57732 atingiram taxas de até 1597 Kbps". Além disso, era exibida uma tabela com todos os testes realizados e seus dados individuais.

A ferramenta Glasnost *é* a que fazia um diagnóstico mais interessante do que acontece em uma rede, pois mensurava diversas métricas, de diferentes protocolos. De acordo com Ramneek (2015b), o ponto forte da Glasnost se concentra na sua acurácia e simplicidade de uso. Porém, ela é focada na diferenciação no usuário final e pode não ser capaz de detectar a discriminação entre provedores de conteúdo feitas pelo provedor de conexão.

---

encontradas em: MAX PLANCK INSTITUTE. Glasnost: Test if your ISP is shaping your traffic. Disponível em: <http://broadband.mpi-sws.org/transparency/bttest.php>. Acesso em: 15 abr. 2017.

8 O HTTP (Hypertext Transfer Protocol) é o protocolo para a transferência de hipertexto, que é o texto estruturado que utiliza ligações lógicas (hiperlinks) entre diferentes nós contendo texto (páginas web). Ele é a base para a comunicação de dados da World Wide Web.

9 A porta 8080 é usada tipicamente pelo protocolo HTTPS.

O Network Diagnostic Tool (NDT), por sua vez, é uma ferramenta que mede a vazão do protocolo TCP entre um *software* cliente instalado em um dispositivo de usuário e um servidor. O NDT é atualmente usado pela FCC – sigla para Federal Communications Commission –[10] como seu *software* oficial de medição de banda larga (DOVROLIS *et al.*, 2010). O NDT possui uma página *web* em que pode ser testado diretamente através de um navegador.[11]

A ferramenta NDT tem uma interface de uso bastante fácil por se tratar de um *applet* Java[12] rodando em uma página *web*. Porém, suas métricas são bastante limitadas. As métricas medidas por essa ferramenta de forma isolada não permitem dizer se está ocorrendo uma discriminação de tráfego, pois não compara com outros protocolos ou com o que acontece em outros provedores. Além disso, existem diversas ferramentas semelhantes a ela, podendo-se citar o SIMET aqui no Brasil.[13]

A ferramenta ShaperProbe detecta se um provedor está empregando algum tipo de *traffic shapping*[14] (SANTOS, 2016), através de uma medição ativa dos caminhos de fluxo da rede (RAMNEEK, 2015b). Para isso, ela tenta identificar se o provedor está classificando certos tipos de tráfego como baixa prioridade, fornecendo diferentes níveis de serviço para eles, através de uma técnica conhecida como *token bucket* (MIORANDI *et al.*, 2013). A ferramenta ShaperProbe precisa ser instalada localmente para testes[15].

---

10 A *Federal Communications Commission* é a agência norte americana que regula os serviços de telecomunicações.

11 O teste com a ferramenta NDT pode ser feito diretamente em: MEASUREMENT LAB. NDT (Network Diagnostic Tool). Disponível em:<http://www.measurementlab.net/tools/ndt/>. Acesso em: 15 abr. 2017.

12 *Applet* é um pequeno software que executa uma atividade específica, dentro de um outro programa maior (como por exemplo em uma página web).

13 O SIMET possui três versões: Web, Mobile e Box. Ele mede a vazão, o *jitter*, a latência e a perda de pacotes. Mais informações em: SIMET. Disponível em: <https://simet.nic.br/>. Acesso em: 15 abr. 2017.

14 Traffic shaping é a prática de bloquear/degradar certos "tipos" de tráfego de dados. Foi bastante usada com as redes *peer-to-peer* (P2P), em especial que usavam protocolo BitTorrent.

15 O guia de instalação da ferramenta ShaperProbe pode ser encontrado em: NETINFER. <http://netinfer.net/diffprobe/shaperprobe.html>. Acesso em: 15 abr. 2017.

Ela necessita que o *firewall*[16] da rede esteja com as portas TCP 55000 – saída –, TCP 55005 – saída –, e UDP 55005 – ambas as direções – abertas. Normalmente, os provedores fecham várias portas em conexões residenciais, principalmente para entrada de fluxo de dados por motivos de segurança. Com isso, os testes que usam portas para entrada podem não funcionar nesta ferramenta.

As quatro ferramentas acima descritas usam a plataforma do Measurement Lab, o M-Lab.[17] Ele fornece uma plataforma para desenvolver, testar e implantar novas ferramentas de medição ativa (DOVROLIS *et al.*, 2010). Os servidores do M-Lab estão distribuídos geograficamente em localizações estratégicas ao redor do mundo. Para cada ferramenta são alocados recursos dedicados na plataforma M-Lab para facilitar medições com maior acurácia.

Já como ferramenta de medição passiva há a Network Neutrality Access Observatory (NANO). Esse sistema detecta discriminação de um provedor coletando passivamente os dados de desempenho dos clientes. Os agentes NANO, implantados nos clientes participantes ao longo da Internet, coletam dados de desempenho para serviços selecionados e reportam essas informações para servidores centralizados, que analisam as medidas para estabelecer relações causais entre um provedor e degradações de desempenho (MIORANDI *et al.*, 2013).

Segundo Ramneek (2015b), ela infere a diferenciação, comparando o desempenho alcançado em um provedor específico em comparação a outros provedores, para uma aplicação específica. A inferência produzida pela NANO tem maior acurácia quanto maior o número de fatores são levados em consideração nos testes. Porém, há muitos fatores que podem afetar os resultados e que podem não ser levados em consideração, o que pode levar a um resultado errado em muitos casos. Também, os cálculos são passivos, e podem não fornecer informação em tempo real.

As ferramentas de medição ativa acima expostas se relacionam com as métricas:

16 Firewall é um sistema de segurança de rede que monitora e controla o tráfego de rede. Normalmente, ele protege uma rede interna contra acessos não autorizados vindos da Internet.

17 Informações sobre todas as ferramentas que usam os servidores do M-Lab: MEASUREMENT LAB. Disponível em: <http://www.measurementlab.net/>. Acesso em: 15 abr. 2017.

1. Vazão do protocolo TCP;
2. Vazão do protocolo UDP;
3. Vazão do protocolo BitTorrent;
4. Vazão do protocolo HTTP;
5. (Goodput do protocolo TCP;
6. Goodput do protocolo BitTorrent;
7. Goodput do protocolo HTTP;
8. RTT do protocolo TCP;
9. Latência do protocolo HTTP;
10. Latência do protocolo TCP; e
11. *Jitter* do protocolo TCP.

Na Tabela 1 é possível ver a relação de métricas com cada ferramenta. A ferramenta NANO foi excluída dessa análise por ter sido encontrado que ela trabalha com métricas como o RTT e a vazão, mas sem haver detalhes de quais protocolos são analisados (TARIQ *et al.*, 2008).

Tabela 1: Métricas medidas por cada ferramenta

	Neubot	Glasnost	NDT	ShaperProbe
Vazão do protocolo TCP	Não	Não	Sim	Não
Vazão do protocolo UDP	Não	Não	Não	Sim
Vazão do protocolo BitTorrent	Não	Sim	Não	Não
Vazão do protocolo HTTP	Não	Sim	Não	Não
Goodput do protocolo TCP	Sim	Não	Não	Não
Goodput do protocolo BitTorrent	Sim	Não	Não	Não
Goodput do protocolo HTTP	Sim	Não	Não	Não
RTT do protocolo TCP	Não	Não	Sim	Não
Latência do protocolo HTTP	Sim	Não	Não	Não
Latência do procolo TCP	Sim	Não	Não	Não
Jitter do protocolo TCP	Não	Não	SIm	Não

Fonte: Elaborado pela autora.

No mesmo espírito do que foi apresentado anteriormente, Garret *et al* (2018) apresenta uma descrição aprofundada de dez ferramentas existentes na literatura, analisando como cada solução endereça cada aspecto da detecção da diferenciação de tráfego, quais técnicas são empregadas por cada solução e quais são os tipos de diferenciação detectadas por cada solução.

Setenareski (2017) propôs a criação de um observatório, como instrumento de acompanhamento da Neutralidade da Rede no Brasil, sendo um repositório de ferramentas ou mecanismos computacionais relacionados ao monitoramento do tráfego da Internet, em especial à Neutralidade da Rede; e um fórum de discussão, no qual os usuários possam relatar os resultados encontrados, por meio do uso das ferramentas de monitoramento de tráfego da Internet, e debater estes resultados com outros usuários.

Em Schaurich *et al*. (2018) é proposta uma ferramenta chamada ISPANN, com a qual os países que possuem legislações voltadas a neutralidade da rede podem configurar as regras aplicáveis em seus países, permitindo que a ferramenta audite a rede de um ISP, identificando violações a neutralidade da rede no país em questão. O estudo de caso apresentado compara as legislações dos Estados Unidos, da Europa e do Chile em relação a quatro práticas de violações a neutralidade: bloqueio, discriminação de usuário, discriminação de aplicação/serviço e priorização paga.

Já Rocha (2018) apresenta a criação de um método que identifique a quebra da neutralidade de maneira agnóstica, independentemente do tipo de protocolo, da aplicação, do serviço, do tamanho do pacote ou de qualquer outra informação que o fluxo possuir em um ambiente controlado. O método proposto também é capaz de distinguir entre diferenciação de tráfego e a degradação que ocorre sobre os fluxos.

O Body of European Regulators for Electronic Communications (BEREC) publicou em outubro de 2017 uma especificação para uma ferramenta voltada a medição da neutralidade da rede. Segundo esse documento de especificações, as funções tidas como mandatórias para supervisão e monitoramento da qualidade dos serviços de acesso a Internet são as medidas de velocidade – *downlink* e *uplink* – e as de atraso. Além dessas, são previstas como funções adicionais as medidas de variação de atraso, as de perda de pacote – para *downlink* e *uplink* – e a disponibilidade de conectividade (BEREC, 2017).

Adicionalmente às funções de medição de qualidade dos serviços de acesso a Internet, a especificação do BEREC solicita funções que permitam a revisão dedicada a como os fluxos de dados que aplicativos específicos geram são tratados pelas redes prestadoras de serviço, sendo obrigatórias a verificação do bloqueio de portas no uso dos protocolos TCP e UDP. Ainda são previstas funções adicionais de medição específicas para certas aplicações como (BEREC, 2017):

- DNS: manipulação de requisições específicas de DNS, realizado pela rede subjacente;
- *Proxy*: detectar se há algum intermediário ao longo do caminho da rede que, de uma forma ou de outra, modifique uma requisição;
- *Web*: desempenho de navegação;
- Áudio/Vídeo: detectar se o tratamento de streaming de áudio/vídeo pode afetar o desempenho conforme percebido pelo usuário final;
- VoIP: detectar como o tráfego para ou de tais aplicativos é tratado; e
- *Peer to peer*: esse tipo de comunicação é bloqueada ou está sendo exposta a algum gerenciamento de tráfego.

No primeiro semestre de 2018, o BEREC abriu uma chamada para que instituições ou pessoas físicas se candidatem para o desenvolvimento dessa ferramenta.

DISCUSSÃO E CONSIDERAÇÕES FINAIS

Essa seção explicou diversas métricas que podem ser usadas para verificar o desempenho de uma rede, incluindo a Internet. Além disso, apresentou ferramentas que usam algumas dessas métricas com a finalidade de medir discriminações de rede e, assim, detectar se haveria violação no princípio da neutralidade da rede.

Pode-se perceber que as ferramentas existentes para detectar as discriminações são específicas para uma aplicação, um protocolo ou para um mecanismo específico de discriminação e, na maioria das vezes, dependem de testes de medição ativos. O uso desse tipo de teste nem sempre é ideal, pois gera um maior fluxo de pacotes na rede, sem que esteja de fato transportando alguma informação útil, podendo contribuir em um cenário de congestionamento da rede. Além disso, os provedores de conexão podem descobrir o padrão dos pacotes de testes de medição – por exemplo, pelo IP de destino – e começar a discriminá-los, seja descartando propositadamente, ou até mesmo favorecendo seu caminho para que tenham melhores resultados do que os pacotes úteis. Esse cenário não aconteceria com ferramentas de medição passiva, pois não há pacotes especificamente gerados para esse fim. Por outro lado, como há uma inspeção dos pacotes trafegados pelos usuários, isso pode se transformar em um problema de privacidade. Além disso, ferramentas de medição passiva são difíceis de serem implementadas na prática.

A maioria das ferramentas usam poucas métricas de rede para inferir seus resultados, o que pode torná-las imprecisas. E por fim, as ferramentas não fazem uma comparação entre os resultados de diferentes provedores de conexão, o que poderia ser útil para compreender o comportamento dos pacotes de cada aplicação na rede.

Com o uso de apenas uma dessas ferramentas existentes pouco se pode afirmar sobre a violação da neutralidade da rede de acordo com a definição do Marco Civil da Internet. Um diagnóstico mais completo poderia ser feito através da análise em conjunto das métricas monitoradas pelas várias ferramentas. Mas ainda assim há uma dificuldade em se dizer que elas são suficientes para serem adotadas na fiscalização da neutralidade da rede e que constituem evidências para uma possível ação judicial em caso de violação. Há um desafio ainda em inferir se uma discriminação ocorrida pode estar em conformidade com alguma das exceções regulamentadas através do Decreto.

Verifica-se que há uma necessidade da escolha de métricas de rede que possam ajudar na fiscalização da manutenção da neutralidade da rede, bem como o desenvolvimento de ferramentas que possam monitorá-las e gerar resultados que possam ser usados como provas para ações judiciais no âmbito do Marco Civil da Internet.

REFERÊNCIAS

BEREC. Net neutrality measurement tool specification. Disponível em: < http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7296-net-neutrality-measurement-tool-specification >. 10 Out. 2017.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei n 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Portal da Legislação. Brasília, 11 maio 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 15 abril 2017.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Portal da Legislação. Brasília, 23 abril 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 15 abr. 2017.

CARISSIMI, A. S.; ROCHOL, J.; GRANVILLE, L. Z. *Redes de computadores.* Porto Alegre: Bookman, 2009.

CHENG, Y.; ÇETINKAYA, E. K.; STERBENZ, J. P. G. Dynamic Source Routing (DSR) Protocol Implementation in ns-3. Proceedings of the ICST SIMUTools Workshop on ns-3 (WNS3). Março, 2012. Disponível em: <http://www.ittc.ku.edu/resilinets/papers/Cheng-Cetinkaya-Sterbenz-2012.pdf>. Acesso em: 15 abr. 2017.

DE MARTIN, J. C.; GLORIOSO, A. The Neubot Project: A Collaborative Approach To Measuring Internet Neutrality. IEEE International Symposium on Technology and Society, Fredericton (Canada), 26-28 June 2008.

DISCHINGER, M.; MISLOVE, A.; HAEBERLEN, A.; GUMMADI K. P. Detecting BitTorrent Blocking. Proceedings of the 8th ACM SIGCOMM conference on Internet measurement – IMC'08, October 20–22, 2008, Vouliagmeni, Greece.

DOVROLIS, C.; GUMMADI, K.; KUZMANOVIC, A.; MEINRATH, S. D. Measurement Lab: Overview and an Invitation to the Research Community. *ACM SIGCOMM Computer Communication Review*, v. 40, n. 3, July 2010.

GARRETT, T.; SETENARESKI, L. E.; PERES, L. M.; BONA, L. C. E.; DUARTE, E. P. Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection. *IEEE Communications Surveys & Tutorials,* v. PP, n. 99, mar. 2018.

HARRISMARE. Packet Delivery Ratio, Packet Lost, End to End Delay. 14 julho 2011. Disponível em: <https://harrismare.wordpress.com/2011/07/14/packet-delivery-ratio-packet-lost-end-to-end-delay/>. Acesso em: 15 abr. 2017.

IETF. RFC 2647 - Benchmarking Terminology for Firewall Performance, 1999. Disponível em: <http://tools.ietf.org/html/rfc2647#section-3.17>. Acesso em: 15 abr. 2017.

IETF. RFC 6349 - Framework for TCP Throughput Testing. 2011. Disponível em: <https://tools.ietf.org/html/rfc6349>. Acesso em: 15 abr. 2017.

KUROSE, J.; ROSS, K. W. *Redes de computadores e a internet:* uma abordagem top-down. 6. ed. [S. l.]: Pearson, 2013.

MAX PLANCK INSTITUTE. Glasnost: Test if your ISP is shaping your traffic. Disponível em: <http://broadband.mpi-sws.org/transparency/bttest.php>. Acesso em: 15 abr. 2017.

MEASUREMENT LAB. NDT (Network Diagnostic Tool). Disponível em:<http://www.measurementlab.net/tools/ndt/>. Acesso em: 15 abr. 2017.

MEASUREMENT LAB. Update: Paris Traceroute bug from Early 2018. Disponível em: <http://www.measurementlab.net/>. Acesso em: 15 abr. 2017.

MIORANDI, D.; CARRERAS, I.; GREGORI, E.; GRAHAM, I.; STEWART, J. Measuring Net Neutrality in Mobile Internet: Towards a Crowdsensing-based Citizen Observatory. IEEE International Conference on Communications 2013: IEEE ICC'13 – Workshop on Beyond Social Networks: Collective Awareness.

NETINFER. <http://netinfer.net/diffprobe/shaperprobe.html>. Acesso em: 15 abr. 2017.

NETWORK MEASUREMENTS FROM THE EDGES. Neubot install guide. Disponível em: <http://neubot.org/neubot-install-guide>. Acesso em: 15 abr. 2017.

RAMNEEK; HOSEIN, P.; CHOI, W.; SEOK, W. Disruptive Network Applications and their Impact on Network Neutrality. 17th International Conference on Advanced Communication Technology (ICACT), 2015.

RAMNEEK; HOSEIN, P.; CHOI, W.; SEOK, W. RAMNEEK; HOSEIN, P.; CHOI, W.; SEOK, W. Detecting Network Neutrality Violations through Packet Loss Statistics. 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2015b.

RAMOS, P. H. S. *Arquitetura da rede e regulação:* a neutralidade da rede no Brasil. 2015. 218 f. Dissertação (Mestrado em Direito) – Escola de Direito de São Paulo, Fundação Getúlio Vargas, São Paulo, 2015.

ROCHA, A. M. *Método Agnóstico de Detecção da Quebra da Neutralidade na Internet pelos ISPs*. 2018. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Santa Maria, Santa Maria. 2018.

SANTOS, V. W. O. *Neutralidade da rede e o Marco Civil da Internet no Brasil:* atores, políticas e controvérsias. 2016. Tese (Doutorado em Política Científica e Tecnológica) – Universidade Estadual de Campinas, Campinas, 2016.

SCHAURICH, V. G.; CARVALHO, M.; GRANVILLE, L Z. ISPANN: A policy-based ISP Auditor for Network Neutrality violation detection. 32nd IEEE International Conference on Advanced Information Networking and Applications (AINA 2018), 16-18 May 2018, Krakow, Poland.

SETENARESKI, L. E. *Fiscalização da Neutralidade da Rede e seu Impacto na Evolução da Internet*. 2017. Tese (Doutorado em Informática) – Universidade Federal do Paraná, Curitiba. 2017.

SIMET. Disponível em: <https://simet.nic.br/>. Acesso em: 15 abr. 2017.

TANENBAUM, A. S.; WETHERALL, D. J. *Computer Networks*. 5. ed. [S. l.]: Pearson, 2011.

TARIQ, M. B.; MOTIWALA, M.; FEAMSTER, N. Nano: Network access neutrality observatory. Georgia Institute of Technology, 2008. Disponível em: <http://conferences.sigcomm.org/hotnets/2008/papers/22new.pdf>. Acesso em: 15 abr. 2017.

WU, T. Network Neutrality FAQ. Disponível em: <http://www.timwu.org/network_neutrality.html>. Acesso em: 15 abr. 2017.

WU, T. Network Neutrality, Broadband Discrimination. *Journal of Telecommunications and High Technology Law*, v. 2, p. 141, 2003.

A FRANQUIA DE BANDA LARGA FIXA PODE LIMITAR O ACESSO À INTERNET?

GABRIELA KNUPP

ANDRÉ APRIGIO

O presente artigo trata da polêmica envolvendo o modelo de franquia de banda larga fixa, que já era prevista em alguns contratos de prestação do serviço de conexão à internet no Brasil, mas que ganhou notoriedade a partir do anúncio feito pela Vivo no início de 2016.

Nosso objetivo é tratar o tema para além da dicotomia "podem ou não podem" ser mantidas as ofertas com franquia de dados. Isso porque entendemos que devem ser sopesados os interesses privado e da coletividade, de forma a garantir a manutenção do interesse dos provedores de acesso à internet em investir na expansão de rede e na manutenção da qualidade do serviço prestado, bem como a não onerar os consumidores com a limitação do acesso à internet.

A GÊNESE DA POLÊMICA

No início de 2016, a Telefônica – detentora da marca Vivo – informou que incluiria no contrato de prestação do serviço de banda larga fixa com tecnologia ADSL[1] a previsão de que, ao atingir o limite da franquia contratada, o serviço poderia ser bloqueado ou ter a velocidade reduzida. Os clientes que contratassem a banda larga popular com velocidades de 200 Kb/s ou de 1 e 2 Mb/s teriam franquia de 10 GB, os de 4 Mb/s teriam 50 GB, os de 8 e 10 Mb/s teriam 100 GB, os de 15 Mb/s teriam 120 GB e, por fim, os de 25 Mb/s teriam 130 GB. Essa regra valeria apenas para os contratos firmados após o anúncio da empresa, portanto não atingiria os demais clientes, e, em caráter promocional, não haveria bloqueio ou redução de velocidade até 31 de dezembro de 2016.

1 Asymmetric Digital Subscriber Line (ADSL) – em tradução livre, Linha Digital Assimétrica para Assinante – é um tipo de tecnologia que, usando uma linha telefônica comum, permite ao usuário transferir digitalmente dados em alta velocidade.

A Telefônica não seria, contudo, a precursora do modelo de franquia de banda larga fixa limitada, visto que a NET já previa nos contratos de seu serviço, o Vírtua, franquias que variavam de 30 GB – no plano com velocidade de 2 Mb/s – a 500 GB – no plano com velocidade de 500 Mb/s – com a possibilidade de redução de velocidade quando o limite fosse alcançado. A Oi também já previa em seus contratos do Velox essa possibilidade, mas ainda não havia implementado as restrições.[2] Todavia, o assunto teve grande repercussão e tomou conta imediatamente das redes sociais, com consumidores que não gostaram do anúncio feito pela Telefônica.

A Agência Nacional de Telecomunicações (ANATEL) não vislumbrou problemas na adoção de limite de franquias para a banda larga fixa. O superintendente de Competição da Agência, Carlos Baigorri, declarou que os usuários com baixo consumo de dados poderiam ser beneficiados pela medida, já que as empresas baseiam seus preços em uma média de uso mais alto.[3] O presidente da Agência à época, João Rezende, declarou que a adoção da internet ilimitada como modelo de negócio tem dificuldade de sustentabilidade no longo prazo.[4] O Ministério das Comunicações, no entanto, na pessoa do então ministro André Figueiredo, assumiu posição contrária ao fim da oferta de planos ilimitados. Segundo o ministro, seria possível que os provedores de serviço de acesso à internet adotassem o modelo de franquia de banda larga desde que fosse mantida a opção de um plano ilimitado e que os contratos vigentes fossem mantidos.[5] Retomaremos esse tema ao longo do artigo.

---

2 G1. Franquia de dados da internet fixa no Brasil gera críticas em redes sociais. 14 abr. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/franquia-de-dados-na-internet-fixa-no-brasil-gera-criticas-em-redes-sociais.html>. Acesso em: 17 abr. 2017.

3 BERBET, Lucia. Limite de franquia na banda larga fixa é benéfico, avalia Anatel. TEL COMP, 16 fev. 2016. Disponível em: <http://www.telcomp.org.br/site/index.php/noticias-setor/limite-de-franquia-na-banda-larga-fixa-e-benefico-avalia-anatel>. Acesso em: 26 mar. 2017.

4 ALEGRETTI, Laís. Imedir limite na internet fixa pode elevar preço do serviço, diz Anatel. G1, 20 abr. 2016. Disponível em: <http://g1.globo.com/economia/noticia/2016/04/impedir-limite-na-internet-fixa-pode-elevar-preco-do-servico-diz-anatel.html>. Acesso em: 26 mar. 2017.

5 GOVERNO DO BRASIL. Governo não permitirá retrocesso no acesso à banda larga, diz ministro. 20 abr. 2016. Disponível em http: <www.brasil.gov.br/infraestrutura/2016/04/governo-nao-permitira-retrocesso-no-acesso-a-banda-larga-diz-ministro>. Acesso em: 26 mar. 2017.

Em meio à polêmica, o presidente do NIC.br e membro do Comitê Gestor da Internet no Brasil (CGI), Demi Getschko, defendeu que o uso de franquia não fazia sentido na banda larga fixa. Uma vez que o cliente contrata uma linha da banda, o único limitador seria a velocidade com que o conteúdo trafega, mas não o volume de dados trafegados na linha.[6] Ademais, atualmente, o conteúdo já fica hospedado perto do usuário, seja por meio de CDN[7] ou de *cache,8* o que acaba onerando menos os provedores.

Diante da mobilização da opinião pública, a Superintendência de Relações com Consumidores da ANATEL publicou o Despacho n.º 1/2016/SEI/SRC de 15 de abril de 2016, determinando que os provedores de acesso à internet se abstivessem de adotar práticas de redução de velocidade, suspensão de serviço ou de cobrança de tráfego excedente após o esgotamento da franquia até que disponibilizassem ferramenta que permitisse ao usuário gerenciar seu consumo e que divulgasse amplamente informações sobre a adoção e funcionamento da franquia. Dias depois, no entanto, o Conselho Diretor da Agência decidiu suspender cautelarmente, por tempo indeterminado, a adoção de franquias pelos provedores. Até o presente momento,[9] a medida se mantém e os provedores de serviço de acesso à internet estão impedidos de disponibilizar planos com limite de franquia, não obstante a regulamentação atual permita a oferta com franquia de dados, como veremos mais adiante.

Em novembro de 2016, a ANATEL disponibilizou em sua plataforma, Diálogo ANATEL, a tomada de subsídios sobre franquia de dados na banda larga fixa. Segundo a Agência, "a providência marca uma mudança de paradigma na relação da Anatel com a sociedade. Pretende-se aproximar a Agência dos consumidores, destinatários últimos de toda atividade regulatória".[10] O documento disponibilizado direciona ao público diversas

---

6 MINOZZO, Paula. Cobrança por franquia de dados em banda larga ainda é impasse. GAUCHAZH, 21 out. 2016. Disponível em http: <//zh.clicrbs.com.br/rs/vida-e-estilo/tecnologia/noticia/2016/10/cobranca-por-franquia-de-dados-em-banda-larga-ainda-e-impasse-7865663.html>. Acesso em: 26 mar. 2017.

7 Content Delivery Network (CDN) é uma rede que hospeda um determinado conteúdo, permitindo a sua distribuição de forma eficaz.

8 Área aonde o conteúdo frequentemente utilizado é guardado para acesso futuro mais rápido.

9 Abril de 2017.

10 DIÁLOGO ANATEL. Tomada de subsídios sobre franquia de dados na banda larga fixa. Disponível em: <http://www.anatel.gov.br/dialogo/groups/profile/895/tomada-de-subsidios-sobre-franquia-de-dados-na-banda-larga-fixa>. Acesso em: 17 abr. 2017.

perguntas sobre o tema, organizadas em três tópicos: aspectos técnicos, aspectos econômicos e concorrenciais e aspectos jurídicos. A consulta estava disponível até 30 de abril de 2017.

A ADOÇÃO DE FRANQUIA É UMA JABUTICABA?[11]

A adoção de franquia de banda larga pelos provedores de acesso à internet não é uma inovação brasileira. De acordo com o relatório de 2016 da União Interacional de Telecomunicações (UIT), Measuring the Information Society, cerca de um terço dos países monitorados adotam o modelo de franquia de dados na oferta da banda larga fixa. Se comparado com o relatório de 2015, percebe-se um aumento de, aproximadamente, 3,5% do número de países que passaram a adotar a franquia (UIT, 2016).

Passamos, então, a analisar de maneira mais detalhada alguns dos países que adotam a franquia de dados.

CANADÁ

A Agência Reguladora canadense, Canadian Radio-television and Telecommunications Commission (CRTC), publicou, em dezembro de 2016, o documento intitulado *Modern Telecommunications Services – The Path Forward for Canada's Digital Economy,* no qual reconhece que qualquer cidadão canadense deve ter acesso à banda larga de alta velocidade.

A CRTC informa que suas ações visam atingir os seguintes objetivos:

I. o acesso de cidadãos em áreas urbanas e rurais aos serviços de telecomunicações de alta qualidade;

II. a continuidade dos investimentos do setor privado aliado ao financiamento do governo em infraestrutura robusta,

11 Para melhor compreensão do termo, optamos pela definição do diplomata Paulo Roberto de Almeida, que define a "Teoria da Jabuticaba" como "tudo aquilo que só existe no Brasil, como essa saborosa fruta selvagem da respeitada família das mirtáceas (*myrciaria jaboticaba*). Isso significa, para ser rápido, pertencer a uma família de "explicações sociais" única e exclusiva neste planeta Terra, situação inédita no plano universal, que consiste em propor, defender e sustentar, contra qualquer outra evidência lógica em sentido contrário, soluções, propostas, medidas práticas, iniciativas teóricas ou mesmo teses (em alguns casos, até antíteses) que só existem no Brasil e que só aqui funcionam, como se o mundo tivesse mesmo de se curvar ante nossas soluções inovadoras para velhos problemas humanos e antigos dilemas sociais." (ALMEIDA, 2005, p. 6).

III. o acesso dos cidadãos a serviços inovadores que podem contribuir para o desenvolvimento social e econômico;

IV. a tomada de decisão consciente pelos usuários. Para tanto, o governo deve investir $750 milhões nos próximos cinco anos para garantir que pelo menos 90% do país tenha internet de alta velocidade até 2021.[12]

As empresas provedoras de banda larga fixa deverão oferecer velocidade mínima de 50 Mb/s para *download* e de 10Mb/s para *upload*. O documento também estabelece que deve haver a oferta de pelo menos um plano de banda larga fixa com uso ilimitado.

Atualmente, a provedora de banda larga fixa Bell oferece, em sua página na internet,[13] opções de pacotes com franquia de dados limitada e uso ilimitado. No primeiro caso, as velocidades para *download* variam entre 3Mb/s, 15Mb/s e 25Mb/s e os limites podem ser de 20GB e 350 GB. Nas ofertas com uso ilimitado, o cliente pode optar pelas seguintes velocidades para *download*: 50Mb/s, 150 Mb/s, 300 Mb/s e 1Gb/s.

ESTADOS UNIDOS

O Open Internet Report and Order, publicado pela Federal Communications Commission (FCC) em 2010, apesar de não abordar diretamente o tema da franquia de dados, previa a possibilidade de o provedor de banda larga cobrar de acordo com o consumo do usuário. Isso porque, segundo a FCC, a proibição da cobrança diferenciada ou conforme o uso faria como que usuários que consomem menos subsidiassem os *heavy users*, vejamos:

> No entanto, proibir uma precificação nivelada, ou baseada no uso, e requerer que todos os assinantes paguem a mesma quantia por serviços de banda larga, desconsiderando a performance ou uso do serviço, acabaria forçando usuários mais casuais daquela rede a custear usuários que consomem mais. Essa proibição também excluiria práticas que podem alinhar adequadamente os incentivos para encorajar o uso eficiente das redes. O enquadramento que

12 ALECRIM, Emerson. Internet de alta velocidade agora é direito básico no Canadá. Disponível em https: <//tecnoblog.net/205198/canada-internet-direito-basico/>. Acesso em: 19 abr. 2017.

13 Disponível em http: <www.bell.ca/Bell_Internet/Internet_access>. Acesso em: 1 abr. 2017.

> adotamos hoje não impede que os provedores de banda larga de cobrarem menos dos usuários que consomem menos, e que usuários que consomem mais paguem um valor maior. (FCC, 2010, p. 41, tradução nossa).[14]

Todavia, ao publicar a segunda versão do seu Report and Order, em 2015, a FCC aborda expressamente, ainda que sem se estender muito, o tema das franquias. A Comissão reconhece que esse tipo de oferta pode ser vantajoso para o usuário ao permitir maior variedade de opções de serviço, mas também pode ser uma influência negativa no comportamento do usuário e no desenvolvimento de novas aplicações. Diante do cenário ainda nebuloso sobre as vantagens e desvantagens da adoção do limite de franquia de dados, a FCC decidiu tratar as controvérsias caso a caso (FCC, 2015).

Ao analisar, por exemplo, a aquisição dos ativos da Time Warner Cable e da Bright House pela Charter, terceira maior provedora de acesso banda larga e TV paga dos Estados Unidos, a FCC aprovou a operação mediante alguns condicionantes, dentre eles, a proibição por sete anos de oferecer planos com limite de franquia de dados ou de cobrar conforme consumo do usuário. Com essa imposição a FCC buscou evitar aumento dos preços praticados pela agora New Charter e práticas que limitassem o acesso dos usuários aos vídeos sob demanda, forçando-os a contratar pacotes tradicionais de TV paga, como se percebe em:

> Primeiramente, o aumento da capacidade de banda larga da New Charter e sua intenção de proteger seus lucros de vídeo irão aumentar os incentivos para impor limites de dados e preços baseados no uso, com o intuito de tornar o consumo de vídeo online mais caro, e particularmente mais caro do que adquirir um pacote tradicional de TV por assinatura. Em segundo lugar, o maior número de assinantes de banda larga da New Charter reforçaria o incentivo e capacidade de aumentar os preços para outras empresas – incluindo distribuidoras de vídeo online – que se interconectam com a rede da New Charter para entregar o tráfico de Internet que os consumidores desejam. Em terceiro lugar, a transação provavelmente irá reforçar o incentivo e capacidade da New Charter em extrair termos contratuais que irão frustrar a capacidade dos programadores em licenciar conteúdo para distribuição online. Ao fazê-lo, a New Charter irá excluir distribuidores de

14 No original: "However, prohibiting tiered or usage-based pricing and requiring all subscribers to pay the same amount for broadband service, regardless of the performance or usage of the service, would force lighter end users of the network to subsidize heavier end users. It would also foreclose practices that may appropriately align incentives to encourage efficient use of networks.220 The framework we adopt today does not prevent broadband providers from asking subscribers who use the network less to pay less, and subscribers who use the network more to pay more".

> vídeo online do conteúdo que os permite ser competidores mais vibrantes para os operadores de TV a cabo. (FCC, 2016, p. 4, tradução nossa).[15]

Atualmente, a AT&T oferece em sua página na internet[16] planos com os limites mensais de dados para *download* e *upload* de 150GB e 1TB ou até mesmo alguma oferta ilimitada. Aqueles que optam pela franquia podem excedê-la por até dois meses sem sofrer qualquer cobrança adicional. No terceiro mês, caso o cliente exceda o limite contratado, deverá pagar U$10 para cada 50GB consumidos até o limite de U$100. Já os clientes que optam pelo AT&T Fiber têm acesso ilimitado. Quem contratar a oferta conjunta de banda larga e TV, por um valor adicional de U$30, também poderá desfrutar da internet ilimitada.

EUROPA

Segundo o relatório da UIT, cerca de um terço dos países da União Europeia oferece planos de banda larga fixa com limite de dados. Como, no âmbito do bloco, não há legislação específica regulando a oferta, cada Estado-membro tem autonomia para dispor sobre o tema.

Na Alemanha, em abril de 2013, a Deutsche Telekom[17] anunciou mudança nas suas ofertas de banda larga fixa, introduzindo limite de franquia que variava de 75 GB a 400 GB, a depender da velocidade contratada. Quando o cliente atingisse o seu limite de franquia, a velocidade seria reduzida

---

15 No original: "First, New Charter's increased broadband footprint and desire to protect its video profits will increase incentives to impose data caps and usage-based prices in order to make watching online video more expensive, and in particular more expensive than subscribing to a traditional pay-TV bundle. Second, New Charter's larger number of broadband subscribers will increase its incentive and ability to raise prices on companies—including online video distributors—that interconnect with New Charter's network to deliver Internet traffic that consumers want. Third, the transaction will likely increase New Charter's incentive and ability to use its leverage over programmers to extract contractual terms that will frustrate the programmers' abilities to license content for online distribution. In doing so, New Charter will foreclose online video distributors from content that allows them to be more vibrant competitors to cable operators."

16 Disponível em: <https://www.att.com/support/internet/usage.html>. Acesso em: 1 abr. 2017.

17 REUTERS. Disponível em: <http://www.reuters.com/article/us-deutschete-lekom-flatrate-idUSBRE9B10BT20131202> e em: <http://www.fiercetelecom.com/telecom/deutsche-telekom-officially-launches-broadband-usage-limits>. Acesso em: 19 abr. 2017.

para 384 Kb/s – depois a operadora decidiu aumentar a velocidade mínima, passando para 2Mb/s – ou o cliente poderia contratar um adicional de franquia pelo período remanescente. Todavia, a discussão acabou se concentrando mesmo na quebra da neutralidade de rede, uma vez que o tráfego decorrente dos serviços VoIP e IPTV da Deutsche Telekom não seria descontado da franquia contratada. A operadora foi questionada pela Agência Reguladora alemã, Bundesnetzagentur, e, por fim, a Justiça do Distrito de Colônia determinou que a empresa não implementasse a prática.

Todavia, atualmente, a O2[18] oferece planos com limites de franquia de 300 MB e 500 MB. Caso o cliente ultrapasse o limite contratado por mais de dois meses consecutivos, sua velocidade será reduzida para 2 Mb/s.

Na Bélgica, a Proximus[19] oferece franquia de 100GB com velocidade para *download* de 50Mb/s e *upload* de 4Mb/s. Quando atingido o limite, o usuário pode recontratar pacotes adicionais de 20 GB e 150 GB. Há ainda a possibilidade de contratação de um plano ilimitado com velocidade para *download* de 100Mb/s e *upload* de 15Mb/s.

Por fim, na Inglaterra, apesar de a British Telecom[20] investir nas ofertas com uso ilimitado de dados, ainda há planos com limites de franquia de 12 GB, 25 GB e 45 GB. O cliente paga £1,80 por GB consumido, uma vez atingido o limite contratado, caso deseje continuar navegando e/ou utilizando dados.

A FRANQUIA É INIMIGA DA CONECTIVIDADE?

Em meio à polêmica após o anúncio da Telefônica, mencionado no início deste artigo, muitos manifestaram preocupação quanto aos prejuízos que a adoção da franquia de dados limitada poderia acarretar ao acesso à internet e à inovação.

Preliminarmente, cumpre ressaltar que, conforme já exposto, a previsão do limite de franquia já constava em alguns contratos de prestação de serviço, ainda que na prática não fosse adotado pelos provedores, uma vez que depende de desenvolvimento de sistema capaz de reduzir a velocidade ou parar a prestação do serviço do cliente ao atingir o limite contratado.

18 O2. Inklusiv-Volumen und Fair-Use-Mechanik. Disponível em: <https://dsl.o2online.de/provider/beratung-und-service/fair-use/>. Acesso em: 9 abr. 2017.

19 Disponível em: <https: //www.proximus.be/en/id_cr_int/personal/products/other-products/internet-subscriptions.html>. Acesso em: 3 abr. 2017.

20 BROADBAND. Products Sand Services. Disponível em: <http://www.product-sandservices.bt.com/products/upgrade-your-broadband>. Acesso em: 9 abr. 2017.

Essa previsão estava em consonância com a regulamentação do serviço, que impõe à ANATEL o princípio da mínima intervenção na vida privada, assegurando ao administrado que a liberdade será a regra e proibições, restrições e interferências do Poder Público serão exceções – cf. art. 128, *caput* e I, Lei n.º 9.472/1997. Ademais, o Regulamento do Serviço de Comunicação Multimídia – SCM, Resolução n.º 614/2013 da ANATEL, permite a existência de franquia de consumo no plano de serviço,[21] desde que, após o consumo integral da franquia contratada, seja possível o pagamento adicional pelo consumo excedente ou a redução da velocidade contratada, sem cobrança adicional pelo consumo excedente (art. 63, III, §1º, I e II).

Por outro lado, alguns argumentam que o Marco Civil da Internet, como é conhecida a Lei nº 12.965/2014, impediria a adoção da franquia de dados, uma vez que assegura ao usuário a não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização. Ocorre que essa disposição deve ser interpretada em consonância com o objeto da contratação do usuário. Dessa forma, o provedor não poderia, em regra, suspender a prestação do serviço no curso da franquia contratada pelo usuário ou do ciclo de cobrança, caso o uso seja ilimitado. Em caso de franquia de dados, a suspensão não pode ocorrer enquanto não for esgotado o consumo de dados contratado pelo usuário.

Portanto, em termos legais, não restam dúvidas de que a regulamentação atual não veda a adoção da franquia de dados pelos provedores de acesso à internet. Apenas a medida cautelar publicada pelo Conselho Diretor da ANATEL, em abril de 2016, estaria vedando temporariamente a sua implementação. No entanto, passamos agora a analisar quais seriam de fato as implicações da franquia de dados para a conectividade.

É importante ressaltar que o acesso à internet depende de alguns requisitos e a contratação de um plano de serviço de uma empresa de telecomunicações é apenas um deles. Antes disso, é preciso que haja disponibilidade de rede de telecomunicações, para prestação do SCM; e de dispositivos para acesso à rede, como computadores, *tablets*, TVs, vídeo games. O indivíduo precisa também ter conhecimento de como utilizar seu equipamento, para poder usufruir plenamente das funcionalidades das aplicações de internet.

21 Um documento que descreve as condições de prestação do serviço quanto às suas características, ao seu acesso, manutenção do direito de uso, utilização e serviços eventuais e suplementares a ele inerentes, preços associados, seus valores e as regras e critérios de sua aplicação, conforme art. 4º, XII, Res. nº614/2013.

Um dos receios do modelo de franquia de dados é que o indivíduo tenha seu acesso limitado ao esgotar a franquia contratada. Ocorre que, nesse caso, apenas um dos requisitos do acesso pode ficar comprometido, caso não haja possibilidade de recontratação adicional. Todavia, como mencionado acima, o Regulamento do SCM permite que seja adotada a franquia de dados desde que seja possível o pagamento adicional pelo consumo excedente ou a redução da velocidade contratada. Isso significa dizer que o indivíduo não perderá seu acesso à internet.

Todavia, para além da possibilidade de recontratar o adicional de franquia, existe o receio de que as opções de pacotes de dados sejam insuficientes para o uso mensal de um usuário médio e que a recontratação de adicionais a cada ciclo de cobrança seja a regra, e não a exceção. Isso acabaria por onerar demasiadamente o usuário. Nas experiências internacionais citadas anteriormente, podemos notar que há poucas opções de planos com limite inferior a 100 MB. É claro que a demanda pode variar de acordo com o país, mas é importante que os provedores de acesso à internet ofereçam planos com franquias que atendam diversos perfis de uso e sejam transparentes quanto ao real uso daquela franquia ofertada.

A TIM, por exemplo, disponibiliza em seu sítio eletrônico,[22] para os clientes da banda larga móvel, um simulador de dados, que permite ao usuário estimar qual seria a oferta mais aderente ao seu perfil de uso. Além disso, a operadora mantém uma página[23] dedicada a explicar ao usuário como se dá o consumo de internet e a fornecer dicas de como usar de maneira mais eficiente sua franquia de banda larga móvel contratada. Não obstante, a TIM ser uma operadora cuja atividade se concentra na prestação do SMP, esse é um bom exemplo de ferramenta que se propõe a prestar informações adequadas ao cliente.

Além de mais transparência por parte dos provedores de acesso à internet, é importante que os provedores de aplicação[24] sejam transparentes quanto ao real consumo de dados de seu conteúdo, pois parte desse consumo pode acontecer a despeito da anuência e, até mesmo, do conhecimento

22 TIM. CALCULE O VOLUME DE DADOS IDEAL PARA VOCÊ. Disponível em: <http://www.tim.com.br/go/para-voce/internet/simulador-de-dados>. Acesso em: 21 abr. 2017.

23 TIM. Dicas imperdíveis para aproveitar sua internet. Disponível em: <http://www.tim.com.br/sp/para-voce/atendimento/internet/dicas-para-uso-dos-dados>. Acesso em: 21 abr. 2017.

24 Aquele responsável pelo conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.

do usuário. Os anúncios que surgem ao longo da navegação, bem como as atualizações e envio de notificações, mesmo que o aplicativo não esteja em uso, consomem dados da sua franquia. O consumo de dados também pode variar conforme as opções de resolução disponibilizadas pelo provedor de aplicação. Quanto maior for a resolução, maior será o consumo de banda. Normalmente, essa informação não está clara para o usuário e nem sempre é possível optar pelo tipo de resolução a ser adotada para transmissão do conteúdo, o que pode acarretar em uso ineficiente de recursos de rede.

Sobre a alocação de recursos de maneira eficiente, é importante lembrar da chamada crise do apagão e das mudanças no consumo de luz e na indústria de eletrodomésticos que decorreram dela. O consumo crescente de energia elétrica aliado à falta de investimentos no setor levou a uma crise no abastecimento energético do país em 2001. O governo federal precisou adotar medidas que visavam o racionamento de energia, tais como a redução de 20% do consumo de eletricidade para aqueles que consumissem mais de 100 quilowatts/hora por mês, isto é, aproximadamente 70% da população. Quem não cumprisse as metas corria o risco de ter a luz cortada. Apesar de todo o desgaste com o racionamento, a partir desse episódio, os brasileiros passaram a se preocupar com o uso mais sustentável de energia, optando por lâmpadas mais econômicas, por não ligar vários eletrodomésticos ao mesmo tempo, por conhecer aqueles que mais consumiam energia. Por outro lado, a indústria começou a produzir equipamentos mais eficientes e econômicos, que evitavam o desperdício de recursos energéticos.

Esse episódio é importante para lembrarmos que os recursos são escassos e que devemos alocá-los de maneira eficiente. Portanto, a adoção de franquia pode estimular o consumo mais eficiente dos recursos disponíveis e o desenvolvimento de tecnologias com o menor consumo de banda.

Já para os provedores de acesso à banda larga fixa, a adoção da franquia de dados reequilibra custos e remuneração, podendo incentivar investimentos em expansão da capilaridade e da capacidade da rede. Segundo o professor da Universidade de Brasília (UnB), Rafael Timóteo, os investimentos em infraestrutura para prestação do serviço de telecomunicações dependem da adoção de um modelo rentável (COSTA, 2016).

Diante de todo o exposto, consideramos que a franquia de dados não é necessariamente inimiga do acesso à internet. Isso porque o usuário pode contratar um plano aderente ao seu perfil de uso e, mesmo atingido o limite da franquia contratada, o seu acesso à internet se mantém. Ainda, segundo a regulamentação, ele tem a oportunidade de recontratar dados adicionais ou navegar com velocidade reduzida, sem que precise pagar por isso.

Todavia, a franquia de dados pode se tornar um limitador do acesso à internet se não forem respeitadas algumas premissas. Em primeiro lugar, como já mencionado, é importante que os provedores de acesso à internet de fato ofertem franquias variadas, podendo, inclusive, manter planos com uso ilimitado para os usuários com grande consumo de banda. Dessa forma, evitar-se-ia limitar o desenvolvimento de novas aplicações, já que cada usuário poderia escolher a oferta mais adequada às suas necessidades, sejam profissionais ou pessoais.

A oferta de franquia pelos provedores de acesso à internet não deve servir, ainda, para privilegiar os seus serviços ou os serviços de seus parceiros, a exemplo do que fez a Deutsche Telekom, na Alemanha, conforme já demonstrado. De acordo com o decreto n.º 8.771/2016, que regulamenta o Marco Civil da Internet, estão vedadas condutas unilaterais ou acordos que privilegiem aplicações ofertadas pelo próprio provedor de acesso ou por empresas integrantes de seu grupo econômico. Isso quer dizer que, caso o provedor de acesso adote o modelo de franquia de dados, não é possível deixar de descontar da franquia do cliente o uso de aplicações do próprio provedor, como VoIP,[25] IPTV,[26] vídeo sob demanda. Esse dispositivo é importante para garantir que o provedor de acesso não se utilize de sua infraestrutura para oferecer serviços em condições mais vantajosas que as de seus concorrentes.

Importante, ainda, que os provedores de serviços de internet e fornecedores de equipamentos sejam transparentes com os usuários no limite de suas competências. O provedor de acesso à internet precisa garantir ao seu cliente ferramenta que permita controlar o uso da franquia contratada, bem como prestar os devidos esclarecimentos acerca do melhor plano para o seu perfil. Os provedores de aplicações de internet, por sua vez, precisam ser claros sobre o consumo de banda de seu conteúdo, incluindo o de caráter publicitário, e permitir que o usuário possa gerenciar o seu acesso. Já os fornecedores podem contribuir com desenvolvimento de equipamentos com menor consumo de banda e com funcionalidades que também permitam ao usuário gerenciar seu consumo.

---

25 Para melhor compreensão, entendamos o VoIP, do acrônimo em inglês *Voice over Internet Protocol*, ou Voz sobre Protocolo de Internet, como sendo uma tecnologia que permite a transmissão de voz por IP ou protocolos de internet. Em outras palavras, o VoIP transforma sinais analógicos de áudio, como aqueles de uma chamada, em dados digitais que podem ser transferidos pela Internet.

26 De forma sumária, entende-se o IPTV, do acrônimo em inglês *Internet Protocol Television*, como sendo o serviço de transmissão (*streaming*) de programas de TV ao vivo e de vídeo sob demanda por meio de uma rede IP.

Por último, caso alguma das premissas não seja respeitada, ou ainda todas sejam observadas, se alguma prática ameaçar o acesso à internet, cabe ao órgão competente – ANATEL, caso esteja relacionada à prestação de serviços de telecomunicações – analisar e tomar as medidas cabíveis, assim como fez a FCC na aquisição dos ativos da Time Warner Cable e da Bright House pela Charter, conforme relatado na seção "Estados Unidos".

UMA VELHA CONHECIDA

Como exposto, a adoção de franquia de dados não seria necessariamente um entrave ao acesso à internet. E ainda que sua adoção possa ser desvirtuada, há mecanismos para garantir o equilíbrio entre os interesses da sociedade e os interesses privados. Na verdade, como apontou a pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros, realizada em 2015 pelo Comitê Gestor da Internet no Brasil (CGI.br), um dos inimigos do acesso à internet é a desigualdade social.

De acordo com a pesquisa, 51% do total das residências brasileiras possuíam acesso à internet, mas, desse percentual, 9% não tinham acesso a computadores; 41% não contavam nem com computador e nem com acesso à internet. Nas áreas rurais, o percentual de domicílios com acesso à internet é bem inferior se comparado às áreas urbanas: 22% vs. 56% dos domicílios. Entre as regiões do país, o *ranking* de domicílios com acesso à internet é o seguinte: sudeste – 60% –, sul – 53% –, centro-oeste – 48% –, nordeste – 40% – e norte – 38%. Já entre as classes sociais, notou-se que praticamente todas as residências das classes A e B já possuem acesso à internet – 97% e 82% respectivamente –, enquanto que a classe DE conta com apenas 16% dos domicílios com acesso à internet.

Dentre os entrevistados, 57% na região norte e 53% nas áreas rurais informaram que a indisponibilidade do serviço em sua residência era uma barreira para o acesso. A pesquisa aponta uma convergência entre esse resultado e a carência de infraestrutura básica, como energia e saneamento, nessas mesmas regiões.

Acreditamos que, para garantir o acesso à internet, as políticas públicas devem se concentrar:

I. na expansão de rede de telecomunicações, com foco na diminuição dos entraves municipais para instalação de infraestrutura e no uso de diferentes tecnologias – como fibra, satélite, radiofrequência – para cobertura das regiões conforme suas especificidades;

II. na educação digital, não apenas para crianças e jovens, mas também para adultos;

III. no acesso a dispositivos, como computadores e *tablets*; e;

IV. na redução das desigualdades sociais, que garantirá ao indivíduo, no longo prazo, autonomia para decidir comprar seus dispositivos e contratar seus serviços.

REFERÊNCIAS

ALECRIM, Emerson. Internet de alta velocidade agora é direito básico no Canadá. Tecnoblog. 2016. Disponível em: <https://tecnoblog.net/205198/canada-internet-direito-basico/>. Acesso em: 19 abr. 2017.

ALEGRETTI, Laís. Impedir limite na internet fixa pode elevar preço do serviço, diz Anatel. Portal de notícias G1. Brasília, 20 abr. 2016. Disponível em: <http://g1.globo.com/economia/noticia/2016/04/impedir-limite-na-internet-fixa-pode-elevar-preco-do-servico-diz-anatel.html>. Acesso em: 17 abr. 2017.

ALMEIDA, Paulo Roberto de. Teoria da Jabuticaba, I: prolegômenos. Considerações sobre uma nova teoria em formação. Espaço Acadêmico. *Revista Espaço Acadêmico*, Brasília, n. 54, p. 6, 29 out. 2005.

BERBET, Lucia. Limite de franquia na banda larga fixa é benéfico, avalia Anatel. TEL COMP, 16 fev. 2016. Disponível em: <http://www.telcomp.org.br/site/index.php/noticias-setor/limite-de-franquia-na-banda-larga-fixa-e-benefico-avalia-anatel>. Acesso em: 26 mar. 2017.

BROADBAND. Products Sand Services. Disponível em: <http://www.productsand-services.bt.com/products/upgrade-your-broadband>. Acesso em: 9 abr. 2017.

BUCKLEY, Seam. Deutsche Telekom officially launches broadband usage limits. Fierce Telecom, 23 abr. 2013. Disponível em: <http://www.fiercetelecom.com/telecom/deutsche-telekom-officially-launches-broadband-usage-limits>. Acesso em: 19 abr. 2017.

BUNDESNETZAGENTUR. Report of the Bundesnetzagentur of 14 June 2013 concerning the rate changes which Deutsche Telekom AG implemented for Internet accesses as of 2 May 2013. 2013. Disponível em: <https://www.bundesnetza-gentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/TelecomRegulation/NetNeutrality/Report_BNetzA_NN.pdf?__blob=publica-tionFile&v=1>. Acesso em: 9 abr. 2017.

CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION. CRTC establishes fund to attain new high-speed Internet targets. Ottawa, 21 dez. 2016. Disponível em: <http://news.gc.ca/web/article-en.do?nid=1172599>. Acesso em: 19 abr. 2017.

COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros [livro eletrônico]: TIC domicílios 2015. São Paulo, 2016. Disponível em: <https://www.cgi.br/media/docs/publicacoes/2/TIC_Dom_2015_LIVRO_ELETRONICO.pdf>. Acesso em: 22 abr. 2017.

COSTA, Machado da. Limite da banda larga da internet divide opiniões de especialistas. Portal de notícias Folha. Brasília, 24 abr. 2016. Disponível em: <http://www1.folha.uol.com.br/mercado/2016/04/1764100-limite-da-banda-larga-da-internet-divide-opinioes-de-especialistas.shtml>. Acesso em: 21 abr. 2017.

CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION. Modern telecommunications services – The path forward for Canada's digital economy. Ottawa, 2016. Disponível em: <http://www.crtc.gc.ca/eng/archive/2016/2016-496.pdf>. Acesso em: 10 abr. 2017.

DIÁLOGO ANATEL. Tomada de subsídios sobre franquia de dados na banda larga fixa. Disponível em: <http://www.anatel.gov.br/dialogo/groups/profile/895/tomada-de-subsidios-sobre-franquia-de-dados-na-banda-larga-fixa>. Acesso em: 17 abr. 2017.

FCC (FEDERAL COMMUNICATIONS COMMISSION). Open Internet Report and Order. 2010.

FCC (FEDERAL COMMUNICATIONS COMMISSION). Memorandum Opinion and Order MB Docket No. 15-149. 2016.

FCC (FEDERAL COMMUNICATIONS COMMISSION). Open Internet Report and Order. 2015.

G1 (Redação). Franquia de dados da internet fixa no Brasil gera críticas em redes sociais. Portal de notícias G1, 12 abr. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/franquia-de-dados-na-internet-fixa-no-brasil-gera-criticas-em-redes-sociais.html>. Acesso em: 17 abr. 2017.

GOVERNO DO BRASIL. Governo não permitirá retrocesso no acesso à banda larga, diz ministro. 20 abr. 2016. Disponível em http: <//www.brasil.gov.br/infraestrutura/2016/04/governo-nao-permitira-retrocesso-no-acesso-a-banda-larga-diz-ministro>. Acesso em: 26 mar. 2017.

HIGA, Paulo. Vivo coloca limite mensal de consumo de internet na banda larga fixa. Tecnoblog, 2016. Disponível em: <https://tecnoblog.net/191493/vivo-limite-franquia-internet-fixa/>. Acesso em: 17 abr. 2017.

INTERNATIONAL TELECOMMUNICATION UNION. Measuring the Information Society Report 2016. Genebra, 2016. Disponível em: <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf>. Acesso em: 1 abr. 2017.

INTERNATIONAL TELECOMMUNICATION UNION. Measuring the Information Society Report 2015. Genebra, 2015. Disponível em: <http://www.itu.int/en/

ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf>. Acesso em: 19 abr. 2017.

MINOZZO, Paula. Cobrança por franquia de dados em banda larga ainda é impasse. Zero Hora. São Paulo, 21 out. 2016. Disponível em: <http://zh.clicrbs.com.br/rs/vida-e-estilo/tecnologia/noticia/2016/10/cobranca-por-franquia-de-dados-em-banda-larga-ainda-e-impasse-7865663.html>. Acesso em: 17 abr. 2016.

O2. Inklusiv-Volumen und Fair-Use-Mechanik. Disponível em: <https://dsl.o2online.de/provider/beratung-und-service/fair-use/>. Acesso em: 9 abr. 2017

PORTAL BRASIL. Governo não permitirá retrocesso no acesso à banda larga, diz ministro. Portal Brasil, 20 abr. 2016. Disponível em: <http://www.brasil.gov.br/infraestrutura/2016/04/governo-nao-permitira-retrocesso-no-acesso-a-banda-larga-diz-ministro>. Acesso em: 17 abr. 2017.

REUTERS. Deutsche Telekom plans new packages after internet cap blocked. Portal de notícias Reuters, 02 dez. 2013. Disponível em: <http://www.reuters.com/article/us-deutschetelekom-flatrate-idUSBRE9B10BT20131202>. Acesso em: 19 abr. 2017.TELESÍNTESE (Redação). Charter adquire Time Warner Cable. Portal de notícias Telesíntese, 25 jun. 2015. Disponível em: <http://www.telesintese.com.br/charter-adquire-time-warner-cable/>. Acesso em: 19 abr. 2017.

TIM. CALCULE O VOLUME DE DADOS IDEAL PARA VOCÊ. Disponível em: <http://www.tim.com.br/go/para-voce/internet/simulador-de-dados>. Acesso em: 21 abr. 2017.

TIM. Dicas imperdíveis para aproveitar sua internet. Disponível em: <http://www.tim.com.br/sp/para-voce/atendimento/internet/dicas-para-uso-dos-dados>. Acesso em: 21 abr. 2017.

VICENT, James. Canada declares 'high-speed' internet essential for quality of life. Portal de notícias The Verge, 22 dez. 2016. Disponível em: <http://www.theverge.com/2016/12/22/14052368/canada-broadband-internet-essential-service>. Acesso em: 19 abr. 2017.

INOVAÇÃO EM DISTRIBUIÇÃO DE VÍDEO DIGITAL: ENTRE *ENFORCEMENT* DE DIREITOS AUTORAIS E NOVOS MODELOS DE NEGÓCIOS

PEDRO NICOLETTI MIZUKAMI

INTRODUÇÃO

Desde o final da década de 90, os debates relativos à distribuição de bens culturais na internet são marcados por três conjuntos interrelacionados de questões, referentes aos:

1. problemas resultantes da reprodução, em larga escala, de conteúdo protegido por direitos autorais;
2. novos modelos de negócio para produção cultural industrial, decorrentes dos choques sofridos pelos modelos de negócio tradicionais; e
3. impactos, em qualidade e quantidade, provocados pelo amplo acesso a tecnologias da informação e comunicação, sobre o próprio *output* da produção cultural e hábitos de consumo de mídia.[1]

Em um primeiro momento, até meados dos anos 2000, esses debates foram informados por eventos como a aprovação do Digital Millenium Copyright Act (DMCA) nos EUA, o surgimento do Napster e popularização das redes de compartilhamento de arquivos *peer-to-peer* (p2p), e a subsequente campanha judicial contra os usuários dessas redes. Um segundo momento pode ser identificado a partir de um retorno ao plano normativo, tanto em nível doméstico, quanto internacional — multilateral, plurilateral

1 Sem a pretensão de uma lista exaustiva, e sem preocupação com ordem e importância, são significativas as seguintes publicações: LESSIG, 2002, 2005, 2006; BENKLER, 2006; FISHER, 2004; BOYLE, 1997, 2008; DRAHOS; BRAITHWAITE, 2003; SELL, 2003; KARAGANIS, 2011; PATRY, 2011; ANDERSON 2006, 2009; KEEN, 2007; LEVINE, 2011; LANIER, 2010; HELPRIN, 2009. É importante destacar a omissão da farta literatura voltada à verificação dos impactos decorrentes da violação em massa de direitos autorais, bem como dos trabalhos voltados à crítica dessas pesquisas.

e bilateral[2] — e a proposição de medidas como a da resposta graduada[3] (GIBLIN, 2014) e aquelas consubstanciadas nos projetos COICA, SOPA, PIPA e nos EUA,[4] envolvendo bloqueio de *sites* e ações direcionadas à publicidade online e meios de pagamento.

Paralelamente, o período que cobre os últimos 15 anos abrigou intensas disputas em torno da viabilidade de modelos de negócio que funcionem com base em uma lógica de não-exclusão em acesso, uso, reprodução de conteúdo protegido por direitos autorais (BENKLER, 2006, p. 41-43), ou que sejam, por seu próprio *design*, capazes de conviver com a pirataria de forma minimamente rentável, seguindo uma fórmula *soft enforcement, hard monetization*. A proliferação de plataformas de *streaming*, com base em pacotes *freemium* e por assinatura, bem como plataformas inteiramente subsidiadas por publicidade, são o novo padrão de mercado. Sua popularidade tem crescido ao mesmo tempo em que se observa uma diminuição do uso de redes p2p, refletindo uma transição de práticas de *download* –legal ou ilegal – e armazenamento local de conteúdo, para práticas de consumo imediato – novamente, legal ou ilegal – de conteúdo hospedado na nuvem.

O momento corrente parece representar as etapas finais de um processo de reintermediação no campo da produção e distribuição cultural. Se em um primeiro momento, o impacto tecnológico sobre os alicerces dos modelos de negócio estáveis e tradicionais das indústrias culturais parecia

2 O fracassado acordo ACTA (Anti-Counterfeiting Trade Agreement) e o bem-sucedido TPP (Trans-Pacific Partnership), que contém um extenso capítulo sobre propriedade intelectual, são os principais exemplos, bem como a atuação de EUA e União Europeia no âmbito bilateral.

3 Os modelos de "resposta graduada" envolvem o envio de notificações a usuários infringentes e a aplicação de uma sanção após um número fixado de ocorrências — o que pode incluir, nas versões mais radicais da proposta, a desconexão do serviço de acesso à internet. Há versões envolvendo a participação do Estado, como o da Hadopi na França, e o da Coreia do Sul. E há modelos que partem para uma "privatização" do processo de envio de notificações, como os arranjos de 6-strikes nos EUA (CAS, Copyright Alert System) e o VCAP no Reino Unido.

4 Combating Online Infringement and Couterfeits Act (2010), Stop Online Piracy Act (2011) e Protect IP Act (2011). Os projetos de lei fracassaram após mobilização da sociedade civil (BENKLER et al, 2013), mas as propostas continuam na agenda da indústria, que busca sua implementação por meio de acordos entre plataformas e detentores de direitos, ou aprovação de legislação semelhante em outros países e fóruns. Há discussão corrente, no âmbito da CPI de Crimes Cibernéticos na Câmara dos Deputados, para criar-se uma exceção ao princípio da neutralidade de rede incluído no Marco Civil da Internet, de modo a se autorizar bloqueio de *sites* que facilitem a violação de direitos autorais.

indicar para a desintermediação – com certos elos da cadeia desaparecendo ou perdendo posição de dominância, como as gravadoras no mercado fonográfico – , o que aconteceu foi algo diferente. As empresas que foram impactadas pela digitalização e pela internet se reestruturaram, e convivem agora com novos intermediários, em um cenário bem mais complexo do que o anterior. Não estão em uma trajetória de extinção, como se avaliou inicialmente, mas de franca reconfiguração.

Quatro parecem ser os elementos essenciais resultantes desse processo, envolvendo diferentes modelos de negócio para cada categoria de ator envolvido – plataformas, produtores de conteúdo, provedores de tecnologia etc.:

1. regimes legais de responsabilização de intermediários de internet, por conteúdo disponibilizado por seus usuários – *user-generated content*, UGC –, bem como sua extensão/modificação a partir de acordos entre detentores de direitos autorais e plataformas;
2. tecnologias de automação de *enforcement* e gestão de direitos autorais, que permitem identificar e atribuir titularidade a unidades específicas de conteúdo, transferindo ao titular a capacidade de determinar condições de acesso, uso e rentabilização dos bens identificados;
3. modelos de "monetização" de conteúdo, a partir da vinculação de uma série de métricas de audiência, visibilidade e engajamento, à repartição de receitas de publicidade e/ou de assinaturas;
4. novos arranjos e estratégias para a produção e distribuição de conteúdo, construídos com base em licenciamento de direitos autorais, agenciamento/representação de produtores individuais de conteúdo, e atuação multiplataforma.

O presente texto procura descrever como as tecnologias indicadas no item 2 da lista acima foram adotadas por plataformas de distribuição e hospedagem de conteúdo na internet, e integradas a modelos de negócio para a rentabilização de bens culturais. As tecnologias descritas são o sistema Content ID utilizado pela Google no YouTube, e a desenvolvida pela empresa Audible Magic, utilizada por serviços como SoundCloud, Vimeo, Twitch e Facebook.

Primeiramente, faremos uma breve revisão da trajetória histórica dos regimes atuais de responsabilização de intermediários por conteúdo gerado por terceiros – do modelo DMCA a medidas DMCA-plus –, para então descrever as tecnologias que auxiliam o processo de automação de *enforcement* de direitos autorais, e como elas inserem nos modelos de negócios para distribuição de vídeo pela internet. Finalmente, apontamos alguns tópicos não abordados pelo texto, mas que têm relevância para uma análise aprofundada do setor e das mudanças em curso.

REGIMES DE RESPONSABILIZAÇÃO DE INTERMEDIÁRIOS

Os conflitos decorrentes dos desafios representados pela internet ao sistema de direitos autorais já haviam sido antecipados, nos EUA, desde a publicação do Lehman White Paper, em setembro de 1995 (LEHMAN, 1995). Encomendado pela administração Clinton, o texto propôs, dentre outras medidas, a adoção de soluções tecnológicas para controle de acesso e uso de bens intelectuais protegidos, bem como para a gestão dos direitos autorais a eles referentes – medidas que posteriormente vieram a ser conhecidas pelas siglas TPM (Technological Protection Measures) e DRM (Digital Rights Management). Diante da possibilidade de sua violação por meios técnicos, sugeriu-se também a aprovação de proteção legal para TPMs e DRM, por meio das chamadas *anti-circumvention measures*.

Reações contrárias às propostas por parte de sociedade civil e academia resultaram em um ambiente político inviável, nos EUA, para a aprovação de uma lei que conferisse proteção legal a essas soluções tecnológicas (LITMAN, 2001; POSTIGO, 2012; HERMAN, 2013). Em razão disso, o governo americano e a indústria do entretenimento transferiram a discussão para a Organização Mundial da Propriedade Intelectual (OMPI), onde conseguiram a aprovação dos tratados de Direitos Autorais (WCT) e Performances e Fonogramas (WPPT), ambos de 1996. Os tratados adotaram as mesmas medidas propostas por Lehman,[5] e foram implementados nos EUA via Digital Millenium Copyright Act (DMCA), em 1998.[6]

Pressão exercida pelo nascente setor de empresas de internet, todavia, estabeleceu *safe harbors* para a responsabilização dessas empresas por conteúdo infringente a direitos autorais disponibilizado por terceiros em suas plataformas, inaugurando o regime de notificação e retirada – *notice-and-takedown*.[7] Em linhas gerais,[8] serviços que hospedem conteúdo

5 O Brasil, apesar de não ser signatário dos tratados, inseriu em sua legislação autoral de 1998 proteções semelhantes (art. 107 da Lei 9.610/98).

6 17 U.S. Code, § 1201 e §1202. Ver: COPYRIGHT.GOV. Chapter 12: Copyright Protection and Management Systems. Disponível em: <http://www.copyright.gov/title17/92chap12.html>. Acesso em: 21 ago. 2017.

7 17 U.S. Code, §512. Ver: COPYRIGHT.GOV. Chapter 5: Copyright Notice, Deposit, and Registration. Disponível em: <http://www.copyright.gov/title17/92chap5.html#512>. Acesso em: 21 ago. 2017.

8 Atenho-me, aqui, apenas a um componente do regime. Os *safe harbors* estabelecidos pelo DMCA afetam quatro tipos de intermediários, com condições específicas para cada um. Podem valer-se da proteção: provedores responsáveis pela infraestrutura de conectividade (como as empresas de telecomunicações), serviços de armazenamento (*caching*), motores de busca e aqueles que hospedem conteúdo disponibilizado por seus usuários.

disponibilizado por seus usuários estão imunes de responsabilização por violação de direitos autorais caso, uma vez recebida uma notificação do detentor dos direitos identificando o conteúdo infringente, efetuem sua remoção imediata. Apesar de amplamente criticado, o sistema do DMCA serviu de modelo para de vários países, em seu formato original ou com modificações.[9]

O Brasil não dispõe de um sistema de notificação e retirada por violação de direitos autorais. Houve a tentativa, durante a tramitação do Marco Civil da Internet – finalmente aprovado pela Lei 12.965/14 –, de se estabelecer salvaguardas para provedores de conexão e de aplicações de internet por qualquer ato ilícito praticado por usuários de suas redes com base na remoção de conteúdo posteriormente a ordem judicial nesse sentido. Em outras palavras: os provedores seriam responsabilizados apenas caso desrespeitassem a ordem judicial. No decorrer das discussões na Câmara dos Deputados, forte pressão exercida pelo Grupo Globo acabou por excluir do âmbito do Marco Civil as violações de direitos autorais.

Informalmente, entretanto, o modelo do DMCA é praticado pelas empresas brasileiras de internet e, como não poderia deixar de ser, pelas empresas estrangeiras que atuam no Brasil e dominam o mercado brasileiro de redes sociais, busca, e distribuição de vídeo *on-line*. O anteprojeto de reforma da Lei de Direitos Autorais elaborado pelo Ministério da Cultura, em suas várias versões, incluiu regimes semelhantes.

MEDIDAS DMCA-PLUS

Insatisfação com a efetividade de mecanismos de notificação e retirada levou as indústrias de conteúdo a iniciar uma campanha em favor de medidas DMCA-plus, que ampliam os níveis de proteção e controle sobre conteúdo divulgado na internet.

Bridy (2016) categoriza as medidas DMCA-plus em duas classes: tipo 1 e tipo 2. As medidas de tipo 1 são direcionadas aos intermediários que já seriam recipientes dos *safe harbors*, e acrescentam obrigações adicionais às já existentes em lei. As de tipo 2 afetam intermediários que não são normalmente responsabilizados por atos praticados por seus usuários e, portanto, não foram incluídos na lista de intermediários original do

9 O projeto WILMAP (World Intermediary Liability Map), do CIS de Stanford, apresenta um mapa comparativo de regimes de responsabilidade de intermediários em vários países. Ver: WORLD INTERMEDIARY LIABILITY MAP. <https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap>. Acesso em: 21 ago. 2017.

DMCA. As medidas DMCA-plus têm sido implementadas por acordos voluntários entre detentores de direitos e intermediários – usualmente com participação do estado através da redação de documentos de melhores práticas, cuja adoção ocorre em um ambiente de ameaças implícitas de intervenções legislativas mais cogentes. Em certos países, como o Brasil, a indústria do cinema e da música tem deixado de lado a estratégia de forçar autorregulação, atuando diretamente no nível legislativo.

As medidas DMCA-plus variam de acordo com o intermediário afetado, conforme indicado na tabela 1, abaixo. A medida que interessa ao presente texto é a de *bloqueio ativo de conteúdo*.

Tabela 1 – Medidas DMCA-plus

Tipo de enforcement	Tipo de intermediário	Medidas DMCA-plus
1	Provedor de acesso	Resposta graduada
	Motor de busca	Rebaixamento de links
	Plataforma de UGC	Bloqueio ativo de conteúdo
2	Meios de pagamento	Notificação e terminação/ bloqueio
	Ad networks	
	Registrars de nomes de domínio	

Fonte: BRIDY, 2016, p. 188.

Não há nenhuma obrigação de monitoramento – e bloqueio – ativo de conteúdo conforme o DMCA. De acordo com Karaganis e Urban (2015), a maior virtude do modelo, para empresas de internet que dependem de conteúdo gerado por terceiros, é seu caráter procedimental. Basta que os mantenedores de plataformas e aplicações de internet obedeçam ao protocolo estabelecido pelo DMCA – recebam notificações e removam o conteúdo indicado como infringente — para valer-se do *safe harbor*. O sistema do DMCA clássico funcionou bem por mais de uma década, mas conforme os serviços se expandiram e ganharam escala maior, o número de notificações também subiu, em parte devido a adoção tecnologias de automação para envio de notificações. Se o serviço de busca do Google recebeu, em 2009, menos de 100 notificações, em 2014 o número atingiu 345 milhões. Diante de um número elevado de notificações, a resposta

mais segura é também automatizar o processo de remoção, ou investir em tecnologias que confiram uma camada adicional de controle aos detentores de direitos. É o caso dos sistemas de detecção de conteúdo aqui estudados[10] (KARAGANIS; URBAN, 2015, p. 30).

Esses sistemas podem ser bastante disfuncionais. Falsos positivos, *over-blocking* e problemas na atribuição de titularidade ocorrem com frequência. Colocam o usuário que disponibiliza vídeos, ademais, em posição de desvantagem frente à plataforma e aos titulares de direitos, particularmente no exercício de direitos como os das exceções e limitações aos direitos autorais.

Conforme o mercado para entretenimento digital evolui, diz Bridy (2016, p. 4), detentores de direitos autorais e intermediários encontram-se em cada vez mais em uma relação de interdependência, seja por acordos de licenciamento, seja pelas fusões e aquisições que têm integrado verticalmente as empresas proprietárias de direitos autorais com as proprietárias das plataformas de distribuição de conteúdo. O exemplo do Content ID, de acordo com a autora, é uma representação precisa do *enforcement* DMCA-plus como uma relação simbiótica de negócios.

AUTOMAÇÃO DE *ENFORCEMENT* E GESTÃO DE DIREITOS AUTORAIS

As tecnologias aqui estudadas inserem-se na categoria maior dos sistemas digitais de gestão de direitos – Digital Rights Management (DRM). Um sistema de DRM não se confunde com uma Technological Protection M easure (TPM), apesar de usualmente incorporar TPMs a sua arquitetura. Sistemas de DRM representam arranjos de tecnologias que operam em conjunto de modo a vincular um determinado "grupo de permissões de acesso e uso" referentes a um conteúdo específico a "esquemas de licenciamento" vinculados a essas permissões, em operação integrada a "instrumentos de monitoramento e registro de consumo" (RUMP, 2013, p. 3-4). Automatizam, dessa maneira, o *enforcement* de direitos autorais.

10 No original: "The adoption of content filtering by video and music services such as YouTube, SoundCloud, and Vimeo represents a profound shift in the direction of enforcement—no longer basing takedown on the rights holder's identification of unauthorized uses after the fact, but on the a priori filtering of user activity in collaboration with rights holders. For many DMCA Classic services, such filtering represents new and potentially unsustainable costs and a threat to the wide latitude for expression on which their user communities are built. For the DMCA+ services, filtering is a response to a complex array of pressures, from staying on the right side of perceived enforcement norms, to exercising some control in keeping content up, to creating—in the case of ContentID—a new payment model for artists".

TPMs e sistemas de DRM são controversos e costumam ser alvo de uma variedade de críticas, usualmente centradas em sua falta de eficácia e nos grandes problemas – técnicos e jurídicos – que podem decorrer de sua implementação (GILLESPIE, 2007; LOBATO; THOMAS, 2012). Conforme Shapiro e Varian (1999, p. 97-98) há um *trade-off* entre o grau de controle determinado pelo titular de direitos e a utilidade que determinado bem informacional tem ao consumidor. Quanto maior o controle – e maiores as restrições de acesso e uso – menor a utilidade. Quanto menor o controle, potencialmente menores as vendas.

Há maneiras mais e menos óbvias, contudo, de se implementar um sistema de gestão de direitos. Boa parte da literatura e da reação contra a esses sistemas costuma se concentrar nas tecnologias mais invasivas. O caso Sony *rootkit* (SCHNEIER, 2005) é emblemático, assim como a remoção, do Kindle, de cópias de 1984, de George Orwell (STONE, 2009). É possível, contudo, construir sistemas cujo funcionamento seja menos transparente ao usuário, ou que invistam mais nos aspectos de rentabilização de conteúdo do que no de bloqueio a acesso.

Dois sistemas merecem atenção no campo da distribuição de vídeo digital, por dominarem atualmente o mercado. O primeiro, desenvolvido pela empresa Audible Magic,[11] é utilizado por várias plataformas de conteúdo gerado por usuário, como Vimeo, SoundCloud e Twitch. Com a inclusão de vídeo como mais um tipo de mídia a ser veiculado por sua rede – e crescente pressão para que a plataforma se adapte às práticas de suas concorrentes –, foi recentemente licenciado pelo Facebook. O segundo sistema é o Content ID da Google, que deixou de ser cliente da Audible Magic e decidiu criar uma versão própria para o YouTube.

A tecnologia que serve de base para o sistema é o *fingerprinting* digital de áudio e vídeo: a criação de marcas d'água identificadoras de conteúdo. Em termos técnicos, não é uma tecnologia particularmente nova. O que é efetivamente novo é a maneira como ela foi incorporada a plataformas de UGC, em atendimento a determinados modelos de negócios.

Em petição de *amicus curiae* submetida ao processo Viacom v. Google (2010), a Audible Magic define o processo de composição de uma marca d'água digital da seguinte maneira:

11 AUDIBLE MAGIC. About Audible Magic. Disponível em: <http://www.audiblemagic.com/about/>. Acesso em: 21 ago. 2017.

> A composição de uma marca d'água digital consiste no processo de extração de uma representação matemática, ou vetor de recurso, do conteúdo de um arquivo de mídia desconhecido, comparando esse vetor a milhões de outras marcas d'água referenciadas em uma base de dados, e retornando uma identificação exata daquele arquivo que era então desconhecido.[12]

O sistema Audible Magic é implementado a partir de conjunção de três componentes:

> 1) Seu algoritmo patenteado de composição de marca d'água digital e seu software proprietário de marca d'água para imagens de vídeo; 2) sua extensa base de dados de referência de conteúdo de áudio e vídeo; e 3) seus métodos e processos para integrar seu sistema de marca d'água em muitas plataformas de distribuição de mídia.[13]

Dos componentes listados, o que corresponde estritamente à tecnologia de base para marcas d'água digitais é do item 1. Todavia, o que torna um sistema como o da Audible Magic ou da Google uma inovação relevante é a composição de uma vasta base de dados de arquivos de referência, e a integração dessa base, associada a mecanismos varredura de conteúdo, às plataformas de distribuição. Quanto mais completa a base de dados, mais eficaz o sistema,[14] o que explica o sucesso conquistado pela Audible Magic, uma das primeiras entrantes no mercado – o que lhe conferiu uma vantagem

---

12 No original: "Digital fingerprinting is the process of extracting a mathematical representation, or feature vector, of the content in an unknown media file, comparing this feature vector to millions of known reference fingerprints in a database, and returning an exact identification of the unknown media file." Cf.: ELECTRONIC FRONTIER FOUNDATION. Case: 10-3270 Document: 117 Page: 1 12/10/2010 165080 34. Disponível em: <https://www.eff.org/files/filenode/viacom_v_youtube/2010-12-10_amicicuriae_audiblemagic_iso_neitherparty.pdf>. Acesso em: 21 ago. 2017.

13 No original: "1) its patented digital fingerprinting algorithm for audio and its proprietary video image fingerprinting software; 2) its extensive reference database of audio and video content; and 3) its methods and processes to integrate its fingerprinting system into many media distribution platforms." Cf.: ELECTRONIC FRONTIER FOUNDATION. Case: 10-3270 Document: 117 Page: 1 12/10/2010 165080 34. Disponível em: <https://www.eff.org/files/filenode/viacom_v_youtube/2010-12-10_amicicuriae_audiblemagic_iso_neitherparty.pdf>. Acesso em: 21 ago. 2017.

14 Os arquivos de referência – a partir dos quais são criadas as marcas d'água – são fornecidos pelos próprios detentores de direitos autorais, que devem provar a titularidade do conteúdo. Ver: YOUTUBE. <https://www.youtube.com/content_id_signup e http://www.audiblemagic.com/content-registration/>. Acesso em: 21 ago. 2017.

na composição da base –, e da Google, cujo Content ID foi alavancado a partir da posição dominante do YouTube enquanto plataforma de vídeo.

Conforme os sistemas de identificação de conteúdo são implementados nas plataformas, abre-se a possibilidade da fixação de *políticas* a serem aplicadas a cada detecção. A Audible Magic permite aos detentores de direitos que bloqueiem, permitam a disponibilização, coletem estatísticas, ou monetizem (rentabilizem) conteúdo de sua propriedade, bem como estabeleçam regras customizadas. O Content ID oferece a mesma funcionalidade.[15]

As informações sobre titularidade, por sua vez, viabilizam monetização. Associadas a métricas de publicidade *on-line*, dão margem à distribuição de receitas de publicidade, e ao refinamento de modelos de rentabilização com base nessas métricas. Um vídeo no YouTube, por exemplo, é remunerado a cada 1000 visualizações – o denominado Cost Per Mille (CPM) – com valores que variam de acordo com a modalidade de publicidade exibida, tempo de visualização da peça publicitária, base geográfica da audiência, valor do leilão da visualização em *ad exchanges* etc.

MODELOS DE NEGÓCIO PARA VÍDEO DIGITAL

Um dos mercados de bens culturais mais dinâmicos atualmente é o de vídeo digital. Há não muito tempo atrás, os principais canais de distribuição eram salas de cinema, videolocadoras, venda direta ao consumidor de DVDs – *sell-through* –, e televisão – aberta ou fechada. Atualmente, esses canais convivem com uma diversidade de serviços prestados *Over-the-top* (OTT), por meio de conexões à internet. Esses serviços, por sua vez, podem ser acessados a partir de telefones celulares, computadores de mesa, *tablets*, *apps* integrados a consoles de videogame, *smartTVs*, e *hardware* dedicado – Chromecast, AppleTV, Amazon Fire TV Stick.

Esse ambiente tem provocado mudanças consideráveis, em curtíssimo espaço de tempo. Observamos o constante estreitamente de janelas de lançamento – não é incomum ver estreias simultâneas no cinema e *on-demand* –, bem como a criação novos formatos de vídeo, novas modalidades de programação e empacotamento de conteúdo, bem como o surgimento de empresas de conteúdo com perfil diferente das produtoras já estabelecidas (HOLT; SANSON, 2014; LOTZ, 2014; CRISP; GONRING, 2015;

15 SUPPORT GOOGLE. How Content ID Works. Ver: <https://support.google.com/youtube/answer/2797370?hl=em>. Acesso em: 21 ago. 2017.

DIXON, 2013). Por outro lado, há crescente pulverização e fragmentação de audiências, e competição acirrada por sua atenção (WEBSTER, 2014).

Em relação às plataformas OTT, são três os principais modelos de negócio:

1. acesso condicionado a pagamento de assinaturas, em plataformas fechadas, com produção de conteúdo original exclusivo, para além do catálogo licenciado de terceiros (por exemplo Netflix, Amazon Prime Video);
2. acesso aberto, subsidiado por publicidade (p. ex. YouTube, Hulu); e
3. venda ou aluguel baseado em itens de catálogo (por exemplo iTunes, Google Play). Os três modelos podem se misturar, como no caso do Hulu e, recentemente, do YouTube, que criou o serviço YouTube Red, de assinaturas, e vai investir, assim como a Netflix, em produção de conteúdo original. Paralelamente, a Google também aposta no *unbundling* e segmentação de categorias de conteúdo, com *apps* dedicadas a cada nicho de produção – games, música, programação infantil etc.

A tecnologia descrita no item anterior foi particularmente importante para plataformas que operam com base em UGC. Ao associar sistemas de detecção de conteúdo a regimes de monetização, a Google assegurou a sobrevivência do YouTube enquanto plataforma, ao mesmo tempo que um canal bastante eficaz para a produção e divulgação de conteúdo amador, semiprofissional e, cada vez mais, profissional. Também foi responsável pela criação de um novo tipo de empresa de conteúdo na figura das *multi-channel networks* (MCNs), que começaram sua trajetória como simples agregadoras de conteúdo e depois se espalharam para outros ramos de atividades acessórias ao campo da produção, como o agenciamento e representação de artistas.

As MCNs posicionam-se como um elo adicional na cadeia que separa a plataforma e o produtor de vídeo, e inicialmente conquistaram espaço por solucionar um problema diretamente relacionado ao Content ID. O YouTube divide as verbas publicitárias com os criadores de vídeo em uma proporção 45%-55%. Para receber verbas por publicidade, todavia, os criadores de conteúdo devem manter, junto ao YouTube, um histórico de adesão aos termos de serviço do site, o que envolve o respeito aos direitos autorais. Recebendo três notificações de direitos autorais, os usuários podem ter suas contas suspensas e, a assim, perder relevante fonte de renda. As MCNs surgiram, desta maneira, absorvendo os ônus pelo licenciamento de direitos autorais, entrando em acordo com diversos detentores de direitos autorais e entidades de classe, e assumindo responsabilidade pelo

respeito a direitos autorais por parte de seus membros. Em contrapartida por esse – e outros serviços –, ficam com 40% dos valores recebidos pelos produtores individuais.

A vantagem de se associar a uma MCN por questões relacionadas a direitos autorais diminuiu a partir da categorização, pelo Google, entre canais afiliados e canais administrados pelas MCNs (SCHIELDS, 2013). Aos poucos, contudo, as MCNs foram compondo um portfólio de produtores considerável, e ganhando relevância em nichos específicos de conteúdo. Atualmente, gravitam não apenas em torno do YouTube, mas também de outras plataformas. Grandes MCNs, como Maker, Awesomeness TV e Fullscreen, foram compradas, integralmente ou em parte, pela Disney, Dreamworks e AT&T, respectivamente.

Tanto pelo lado da produção quanto da distribuição, parecemos caminhar para um mercado com grandes empresas integradoras, que empacotam elementos produzidos por outras, operando em estruturas oligopolísticas, rodeadas por empresas menores, especialistas, como descrito por Eli Noam em seu estudo sobre concentração midiática nos EUA:

> 1. Grandes empresas integradoras, que montam e empacotam elementos em sua maioria produzidos por terceiros, operando em uma estrutura industrial de oligopólio.
> 2. Várias empresas especializadas que orbitam ao redor das integradoras, em clusters geográficos e funcionais, fornecendo muitos dos elementos de serviço e produção. Algumas dessas especialistas podem ser elas mesmas bem grandes e/ou dominarem seus nichos. (NOAM, 2009, p. 437). [16]

Nesse contexto, empresas como Facebook e Google, administram e mantêm plataformas integradoras de conteúdo, com empresas menores produzindo conteúdo e oferecendo serviços de produção em nichos específicos. Para o produtor de conteúdo, mostra-se particularmente importante o esforço na construção de uma marca sólida, e a disseminação do conteúdo produzido pelo maior número de canais de distribuição possível. Na medida em que investem em produção de conteúdo original, contudo, as próprias plataformas podem ser vistas como competidoras em potencial.

16 No original: "1. Large integrator firms, assembling and bundling elements mostly produced by others, operating in a oligopolistic industry structure.

2. Numerous specialist firms surrounding the integrators in geographic and functional clusters and providing much of actual production and service elements. Some of these specialists may be quite large themselves and/or dominate their niche."

CONCLUSÕES

O objetivo do presente capítulo foi apenas lançar alguns apontamentos em preparação para um trabalho mais aprofundado a respeito do mercado de vídeo digital e políticas públicas para o setor. Como conclusão, parece menos oportuno resumir o que foi abordado do que indicar alguns pontos igualmente importantes que não foram discutidos:

- infraestrutura: quais as implicações das regras de neutralidade de rede sobre a distribuição e produção de conteúdo? Qual o impacto, por exemplo, que a exclusão de Content Distribution/Delivery Networks (CDNs)[17] (NUECHTERLEIN; WEISER, 2013, p. 184) do âmbito das regras de neutralidade de rede e exceções aos serviços de zero rating podem ter sobre a concentração do mercado de distribuição?
- *gatekeeping* por algoritmos: o que confere relevância e visibilidade a determinados bens informacionais em relação a outros é determinado por algoritmos desenvolvidos pelas plataformas de distribuição de conteúdo. Há pouca transparência em relação a como esses algoritmos operam e, consequentemente, sobre seus potenciais impactos econômicos e sociais (PASQUALE, 2015; PARISER, 2011). Como produtores de vídeo são afetados pela seletividade conferida pelos algoritmos?;
- privacidade e publicidade *on-line*: uma análise profunda do setor de distribuição de vídeo digital necessariamente passa pela investigação das relações existentes entre mensuração de audiências, mídia programática – publicidade via leilões em tempo real – e privacidade. Esse é um campo povoado por intermediários específicos – *ad networks, ad exchanges, data brokers* etc. –, e que influi diretamente nos modelos para monetização de conteúdo. A coleta de dados por parte de plataformas e serviços de internet envolve complexos problemas regulatórios, e que guardam relação direta com as estratégias e modelos de negócio de vários atores do setor;

17 "Today, instead of relying on backbone networks to carry your website's data across the Internet each time someone asks for it, you can hire (or build) a *content delivery network* to accomplish the same task much more efficiently. CDNs operate by arranging for the transport of data content to cache servers dispersed throughout the Internet, close to end users in many different locations. Each time an end user in one of those locations wishes to view your content, she generally communicates only with a nearby CDN server, not with your central database. And if the CDN you hire has interconnected directly with that end user's ISP, the localized communication from end user to cache server never needs to involve a backbone middleman at all".

- regulação e tributação: Ministério da Fazenda e ANCINE sinalizaram, em alguns momentos, a intenção de propor regimes especiais de tributação para serviços OTT. Como esses regimes afetariam os atores que operam no setor, e quais as limitações práticas existentes para as propostas em discussão diante de um contexto de distribuição global e digital?;
- radiodifusão, TV por assinatura e internet: quais as relações existentes entre os atores que atuam nos canais tradicionais de distribuição audiovisual e aqueles que operam na internet? Algumas fusões e aquisições apontam para uma relação de convergência. Por outro lado, há empresas e produtores independentes de conteúdo que permanecem presos – ou dão ênfase – a canais específicos. Quais as implicações para as tradicionais empresas brasileiras de mídia do domínio, por empresas americanas, das plataformas de distribuição?;
- monetização via plataformas *versus* gestão coletiva de direitos: De certa forma, o modelo de monetização por receita publicitária e distribuição com base em métricas de execução e audiência lembra o mecanismo básico que sustenta a ideia de gestão coletiva, mas partindo de uma estratégia totalmente diferente de licenciamento. Quais os impactos provocados pela dispersão de conteúdo em múltiplas plataformas sobre as práticas de licenciamento de direitos autorais praticadas por entidades de gestão coletiva?

REFERÊNCIAS

ANDERSON, Chris *et al.* Social mobilization and the networked public sphere: mapping the SOPA-PIPA debate. Berkman Center Research Publication, Cambridge: Berkman Center, n. 16, 2013.

ANDERSON, Chris. *Free:* the future of a radical price. Nova York: Hyperion, 2009.

ANDERSON, Chris. *The long tail:* why the future of business is selling less of more. Nova York: Hyperion, 2006.

AUDIBLE MAGIC. About Audible Magic. Disponível em: <http://www.audiblemagic.com/about/>. Acesso em: 21 ago. 2017.

BENKLER, Yochai. *The wealth of networks:* how social production transforms markets and freedom. Nova Haven; London: Yale University Press, 2006.

BOYLE, James. *Shamans, software and spleens:* law and the construction of the information society. Cambridge: Harvard University Press, 1997.

BOYLE, James. *The public domain:* enclosing the commons of the mind. Nova Haven; London: Yale University Press, 2008.

BRIDY, Annemarie. Copyright's Digital Deputies: Dmca-Plus Enforcement By Internet Intermediaries. In: ROTHCHILD, John A. (Ed.). *Research Handbook On Electronic Commerce Law.* Cheltenham; Northampton: Edgar Elwar, 2016.

COPYRIGHT.GOV. Chapter 12: Copyright Protection and Management Systems. Disponível em: <http://www.copyright.gov/title17/92chap12.html>. Acesso em: 21 ago. 2017.

COPYRIGHT.GOV. Chapter 5: Copyright Notice, Deposit, and Registration. Disponível em: <http://www.copyright.gov/title17/92chap5.html#512>. Acesso em: 21 ago. 2017.

CRISP, Virginia; GONRING, Gabriel Menotti. *Besides The Screen:* Moving Images Through Distribution, Promotion And Curation. Londres: Palgrave Macmillan, 2015.

DIXON, Wheeler Winston. *Streaming:* Movies, Media, And Instant Access. Lexington: University Press of Kentucky, 2013.

DRAHOS, Peter; BRAITHWAITE, John. *Information Feudalism:* Who Owns The Knowledge Economy? Nova York: The New Press, 2003.

ELECTRONIC FRONTIER FOUNDATION. Case: 10-3270 Document: 117 Page: 1 12/10/2010 165080 34. Disponível em: <https://www.eff.org/files/filenode/viacom_v_youtube/2010-12-10_amicicuriae_audiblemagic_iso_neitherparty.pdf>. Acesso em: 21 ago. 2017.

FISHER, William W. *Promises To Keep:* Technology, Law, And The Future Of Entertainment. Stanford: Stanford University Press, 2004.

GIBLIN, Rebecca. Evaluating graduated response. *The Columbia Journal of Law and the Arts*, v. 37, n. 2, 2014.

GILLESPIE, Tarleton. *Wired Shut:* Copyright And The Shape Of Digital Culture. Cambridge: The MIT Press, 2007.

HOLT, Jennifer; SANSON, Kevin. *Connected Viewing:* Selling, Streaming, & Sharing Media In The Digital Age. Nova York: Routledge, 2014.

HORTEN, Monica. *A Copyright Masquerade:* How Corporate Lobbying Threatens Online Freedoms. Londres; Nova York: Zed Books, 2013.

KARAGANIS, Joe (Org.). *Media Piracy In Emerging Economies*. Nova York: Social Science Research Council, 2011.

KARAGANIS, Joe; URBAN, Jennifer. The Rise Of The Robo Notice. *Communications of the ACM*, v. 58, n. 9, 2015.

KEEN, Andrew. *The Cult Of The Amateur*: How Blogs, Myspace, Youtube, And The Rest Of Today's User-Generated Media Are Destroying Our Economy, Our Culture, And Our Values. Nova York: Doubleday, 2007.

LEHMAN, Bruce A. Intellectual property and the national information infrastructure: the report of the working group on intellectual property rights. Washington: US

Department of Commerce, 1995. Disponível em: <http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf>. Acesso em: 21 ago. 2017.

LESSIG, Lawrence. The Future Of Ideas: The Fate Of The Commons In A Connected World. Nova York: Vintage, 2002.

LESSIG, Lawrence. *Code 2.0*. Nova York: Basic Books, 2006.

LESSIG, Lawrence. *Free Culture:* The Nature And Future Of Creativity. Nova York: Penguin Books, 2005.

LEVINE, Robert. *Free Ride:* How Digital Parasites Are Destroying The Culture Business, And How The Culture Business Can Fight Back. Nova York: Doubleday, 2011.

LITMAN, Jessica. *Digital Copyright*. Amherst: Prometheus Books, 2001.

LOBATO, Ramon; THOMAS, Julian. The Business Of Anti-Piracy: New Zones Of Enterprise In The Copyright Wars. *International Journal of Communication*, v. 6, 2012.

LOTZ, Amanda D. *The Television Will Be Revolutionized*. 2. ed. Nova York: New York University Press, 2014.

NOAM, Eli. *Media Ownership And Concentration In America*. Oxford: Oxford University Press, 2009.

NUECHTERLEIN, Jonathan E.; WEISER, Philip J. *Digital Crossroads*: Telecommunications Law And Policy In The Internet Age. 2 ed. Cambridge: The MIT Press, 2013.

PARISER, Eli. *The Filter Bubble*: What The Internet Is Hiding From You. Nova York: The Penguin Press, 2011.

PASQUALE, Frank. *The Black Box Society:* The Secret Algorithms That Control Money And Information. Cambridge; Londres: Harvard University Press, 2015.

POSTIGO, Hector. *The Digital Rights Movement:* The Role Of Technology In Subverting Digital Copyright. Cambridge: The MIT Press, 2012.

RUMP, Niels. Digital Rights Management: Technological Aspects. In: BECKER, Eberhard *et al*. (Eds). *Digital Rights Management:* Technological, Economic, Legal And Political Aspects. Berlin: Springer, 2003.

SCHNEIER, Bruce. Real story of the rogue rootkit. Wired, 17 nov. 2005. Disponível em: <http://www.wired.com/2005/11/real-story-of-the-rogue-rootkit/>. Acesso em: 21 ago. 2017.

SHAPIRO, Carlo; VARIAN, Hal R. *Information Rules:* A Strategic Guide To The Network Economy. Cambridge: Harvard Business School Press, 1999.

SHIELDS, Mike. How YouTube's new arrangements with MCNs work. AdWeek, 30 out. 2013. Disponível em: <http://www.adweek.com/videowatch/how-youtubes-new-arrangements-mcns-work-153492>. Acesso em: 21 ago. 2017.

STONE, Brad. Amazon erases Orwell books from Kindle. New York Times, 17 jul. 2009. Disponível em: <http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=0>. Acesso em: 21 ago. 2017.

SUPPORT GOOGLE. How Content ID Works. Ver: <https://support.google.com/youtube/answer/2797370?hl=em>. Acesso em: 21 ago. 2017.

WEBSTER, James G. *The Marketplace Of Attention:* How Audiences Take Shape In A Digital Age. Cambridge: The MIT Press, 2014.

WORLD INTERMEDIARY LIABILITY MAP. <https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap>. Acesso em: 21 ago. 2017.

YOUTUBE. <https://www.youtube.com/content_id_signup e http://www.audiblemagic.com/content-registration/>. Acesso em: 21 ago. 2017.

O FUTURO DAS COISAS

A TUTELA DA PRIVACIDADE NA INTERNET DAS COISAS (IOT)

CAITLIN MULHOLLAND

A (R)EVOLUÇÃO TECNOLÓGICA: DE PESSOAS RACIONAIS PARA COISAS QUE PENSAM POR VOCÊ

Costuma-se afirmar – não sem razão – que o Direito segue a reboque das mudanças sociais e que os institutos jurídicos, sentenças, leis e regulamentos configuram, em não raras ocasiões, uma resposta tardia a situações merecedoras de uma tutela previamente constatada. A premissa por trás de tal afirmação se deve ao fato de que o Direito, enquanto ciência social, não tem a característica da predição, nem tampouco serve de moldura apriorística de situações sociais, mas, pelo contrário, atua por meio de uma prognose póstuma, ou seja, traz respostas e soluções após se concretizarem conflitos que se colocam na sociedade e que merecem algum tipo de tutela jurídica demandada pelas pessoas. Isto, evidentemente, depois de verificado o "problema" posto. Primeiro o fato, depois o Direito.

Não é diferente tal afirmação quando nos deparamos com os avanços da tecnologia e sua insistente e rápida evolução. Pelo contrário, as inovações tecnológicas potencializam a velhice do Direito. Vivemos num momento em que a tecnologia se desenvolve a largos passos e o Direito não consegue acompanhar o seu ritmo. Não se tratando de ciência preditiva, o Direito sempre fica atrás na corrida com – ou para alguns, contra – a tecnologia. De fato, começam a surgir conflitos e questionamentos que devem ser respondidos ou referidos pelo Direito, sempre depois que eles se apresentam como resultado do uso de novas tecnologias.

É neste contexto de desenvolvimento tecnológico e retardo jurídico que se desenrola o tema deste ensaio. Pretende-se identificar quais os intrumentos do Direito aptos a possibilitar uma tutela jurídica de situações que eventualmente sequer existem concretizadas ou problematizadas na vida das pessoas, como num movimento de dar soluções antecipadas a

conflitos ainda não identificados ou incipientes. É no âmbito da tecnologia conhecida como Internet das Coisas – ou Internet of Things, ou, ainda, IoT – que se desenvolve o argumento desta perspectiva, revelando um dos principais debates que se realiza neste âmbito e que se refere à proteção da privacidade ou dos dados pessoais que são disponibilizados e coletados por estas "coisas" conectadas.

Em poucas palavras, a IoT representa inovação tecnológica que permite a criação de ambiente interligado através de sensores que conectam objetos ou bens por meio da internet possibilitando não só a comunicação e realização de funções específicas entre as coisas, como gerando a cada vez mais constante coleta, transmissão, guarda e compartilhamento de dados entre os objetos e, consequentemente, entre as empresas que disponibilizam este tipo de tecnologia às pessoas.

Com a popularização da tecnologia IoT e a sua utilização frequente em objetos de nosso cotidiano – *smartphones*, televisores, relógios inteligentes, pulseiras identificadoras de funções físicas e de saúde, *tablets*, dentre outros – o que se questiona do ponto de vista do Direito é se existe uma política eficiente de proteção dos dados e privacidade das pessoas que utilizam tais objetos e se, por outro lado, as pessoas estariam dispostas a renunciar a esta proteção de seus dados em contrapartida aos benefícios evidentes que tal tecnologia possibilita na vida delas, justificando o *trade off* com base na conveniência pessoal evidente.

Conveniência e utilidade, a propósito, são os termos habitualmente utilizados para qualificar os objetos que utilizam esta tecnologia. Desde o banal *tag* de estacionamento ou pedágio que permite ao motorista a passagem sem o "pagamento" imediato ou a necessidade de permanecer por longos minutos em filas, até os carros autônomos, passando por televisões inteligentes, a IoT é o tema do momento. Para o mundo "prático", a internet das coisas traz benefícios de tamanha ordem – ainda que alguns deles possam ser considerados fúteis – que o usuário do bem conectado sequer imagina quais são as consequências jurídicas eventuais – e maléficas – que podem surgir no que diz respeito à proteção de privacidade e de dados pessoais.

De fato, os objetos que utilizam a tecnologia que os permitem conectar-se com redes de internet ou com outros objetos que usam a mesma tecnologia são uma fonte inesgotável de dados que podem e serão utilizados pelos fornecedores de produtos e serviços sem a autorização expressa ou evidente do usuário do produto, e sem que este usuário saiba que existe esta possibilidade. Visto por este lado, a principal questão que surge no uso da IoT é a que se refere ao (des)conhecimento que o usuário dos objetos conectados detém sobre o fato de que as "coisas inteligentes" utilizam

tecnologia de resgate, coleta e compartilha de seus dados entre outras pessoas – geralmente fornecedores de produtos e serviços – que sequer estão incluídas no âmbito contratual do uso do bem referido.

Quando, por exemplo, um usuário de uma TV inteligente acessa os conteúdos *on-line* previamente inseridos no sistema da TV, ele sabe que está aceitando termos de uso e privacidade? Muito possivelmente não. Ainda, será que este mesmo usuário entende que ao conectar sua TV a uma rede de internet Wi-Fi seus dados serão compartilhados entre outros fornecedores de serviços? Mais uma vez, a reposta provável é não. Mas a pergunta fundamental é: será que o usuário da TV inteligente se importa com estas questões ou prefere ignorar eventuais abusos e violações em nome de uma conveniência e praticidade? E se a resposta for novamente uma defesa da ignorância, será que o Direito deve intervir tutelando aspectos da vida das pessoas que elas mesmas desconhecem ou preferem não ver tutelados? A resposta a estas questões definirá os rumos da tutela e proteção dos dados pessoais pelo uso da tecnologia IoT no Direito brasileiro.

Como relato, pode-se pensar no já mencionado caso dos *tags* que permitem o acesso a estacionamentos de shopping centers. Uma vez afixados no parabrisa do carro, a aproximação de determinada cancela que possua, por sua vez, um sensor conectado a uma rede, permite o acesso ao estacionamento, sem a necessidade de pagamento imediato. No momento seguinte ao da passagem da cancela, o usuário do automóvel recebe uma mensagem em seu celular avisando-o de promoções de lojas que se localizam no interior daquele shopping. Muito conveniente e prático, certamente. Será que podemos sustentar que nesse caso há violação do direito à privacidade ou violação de dados pessoais? Será que o contratante do *tag* sabe que sua presença seria identificada num shopping por determinadas lojas? Será que a informação da localização do usuário de *tag* para o contratante do serviço revela violação da privacidade?

Fato é que a sociedade atual é fundamentada num modelo de regulação tecnológica vigorosa que gera, por sua vez, a possibilidade de mercantilização de dados pessoais (RODOTÀ, 2013, p. 33-34),[1] sem que haja um adequado aparato legal capaz de proteger tal direito fundamental à priva-

1 Rodotà ensina que o "corpo eletrônico", conjunto de informações que constituem a nossa identidade, deve ser juridicamente regulado e protegido da mesma forma que o "corpo físico", considerando a unidade e integridade da pessoa humana, a evitar que a pessoa seja considerada como um tipo de mina a céu aberto onde qualquer um possa escavar quaisquer informações pessoais e, assim, construir um perfil individual, familiar, de grupo, permitindo que a pessoa se transforme em objeto de poderes externos, economicamente avaliado. O corpo não pode ser objeto de lucro.

cidade. É imperioso pensar o papel que o Direito deve desempenhar neste cenário, especialmente no Brasil, considerando o déficit informacional que há no uso de tecnologia em nossa sociedade.

Mas para responder às perguntas formuladas acima, é necessário entender-se qual o conceito de privacidade atual – e que devemos utilizar – e como devemos relacioná-lo com a proteção de dados pessoais para a tutela de interesses não só patrimoniais, como principal e especialmente os existenciais.

O DIREITO DA PRIVACIDADE ENQUANTO DIREITO À PROTEÇÃO DE DADOS

Em nosso ordenamento jurídico, o artigo 5º, X, da Constituição Federal,[2] e o artigo 21, do Código Civil,[3] fundamentam a proteção da esfera privada de uma pessoa, referindo-se tanto à vida privada, quando à intimidade da pessoa humana. O direito à privacidade, e mais especificamente, o direito à intimidade (LEWICKI, 2003, p. 31),[4] alude à proteção da esfera privada ou íntima de uma pessoa, sendo esta abrigada contra ingerências externas, alheias e não requisitadas, e tutelada na medida em que não se permite, sem autorização do titular da informação ou dado, a sua divulgação no meio social.

Este conceito habitual de privacidade está, contudo, superado. Se, tradicionalmente, o direito à privacidade – *right to privacy* – está associado ao direito de ser deixado só,[5] contemporaneamente pode-se afirmar que a privacidade evoluiu para incluir em seu conteúdo situações de tutela

2 Artigo 5º, X, CF – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

3 Art. 21, CC – A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

4 Diverge a doutrina quanto ao uso de expressões como privacidade, intimidade, segredo, vida privada, etc. Neste sentido, ensina Bruno Lewicki que "o conjunto das situações hoje ligadas à proteção da vida privada representa um 'conglomerado de interesses diversos'", configurando as inúmeras e variáveis facetas de um conceito em ampliação constante.

5 Veja, nesse sentido, a concepção trazida por Warren e Brandeis, em 1890, em artigo intitulado "The right to privacy", publicado na *Harvard Law Review*.

de dados sensíveis,[6] de seu controle pelo titular e, especialmente, de "respeito à liberdade das escolhas pessoais de caráter existencial" (LEWICKI, 2003, p. 9). Para Stefano Rodotà, "a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações" (RODOTÀ, 2008, p. 92), sendo a esfera privada "aquele conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo".[7]

Foi com base naquele primeiro conteúdo que em 1890, os Justices da Supreme Court Americana, Warren e Brandeis, determinaram a necessidade de tutela dessa esfera existencial. À época, a interpretação que se dava ao direito à privacidade era restrita e se aplicava a casos em que existia a atuação de terceiros contra aquela esfera. Isto é, a interpretação que se dava a este direito restringia-se a tutelar a esfera privada de uma pessoa, impedindo que outros pudessem nela ingressar sem sua autorização. Associada à idéia de casa, moradia, este princípio foi primeiramente utilizado para proteger a vida privada das pessoas, dentro de seu próprio lar, representando nesta tutela um ideal burguês de proteção patrimonial, mais do que de proteção existencial. Esta afirmativa é especialmente verdadeira quando se percebe que as formas de tutela jurídica da privacidade naquele determinado momento histórico se reportam aos instrumentos de proteção da posse e propriedade. Vem daí o uso da expressão *trespass*, que poderia ser traduzido como esbulho em nosso direito possessório. A privacidade, neste contexto, se resumiria a um direito de tutela de uma situação de resguardo, mas com uma forte conotação patrimonial.

A ampliação do conceito de *privacy* se deu, em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais. Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, consequentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada.

---

6 Dados sensíveis são aquelas informações que dizem respeito à essência da personalidade de uma pessoa.

7 *Idem*.

Há, portanto e a princípio, três concepções sobre o direito à privacidade acima apresentadas (RODOTÀ, 2008, p. 61-65), quais sejam:

I. o direito de ser deixado só, em acepção originária, tradicional, e referenciada a um período de liberalismo político e econômico, que direciona a proteção da privacidade a um ideal burguês de tutela patrimonial;

II. o direito de ter controle sobre a circulação dos dados pessoais, determinado por meio da construção teórica e jurisprudencial da denominada autodeterminação informativa, estabelecendo a prerrogativa da pessoa de acessar, corrigir, controlar e disponibilizar dados pessoais, por sua livre escolha; e

III. o direito à liberdade das escolhas pessoais de caráter existencial, representando a ligação entre a autonomia existencial da pessoa – liberdade – e a construção de sua identidade pessoal por meio da proteção dos seus dados sensíveis – isto é posição política, expressão partidária, afiliação sindical, opção sexual, condições de saúde, etc. – dignidade (RODOTÀ, 2008, p. 92)

Parte-se, portanto, de seu tradicional conceito, qual seja, a do direito a ficar sozinho; passa-se pela definição que sustenta ser o direito à privacidade o direito que cada um tem de controlar a utilização de informações que digam respeito a si próprio; e, finalmente, chega-se ao seu conteúdo atual: as pessoas têm a liberdade de fornecer as informações que desejarem. Esta última definição nos leva ao debate a respeito do consentimento para coleta, tratamento ou compartilhamento de dados, que antes era implícita e hoje se torna necessariamente expressa e explícita – ainda que por meio de termos de uso e políticas de privacidade consideradas inadequadas por estabelecerem uma cláusula de aceite dos termos por *default*, com a simples adesão por um clique. Também é preciso levar em conta que esse consentimento nem sempre é verdadeiramente livre, pois não raras são as situações em que a utilização de um determinado serviço depende da cessão de dados pessoais. Ainda assim, pode-se criticar que o consentimento da pessoa como requisito legitimador e contratual para a coleta de dados apenas reforçaria o caráter proprietário – e não existencial – da privacidade.

Desta forma, para que seja possível conciliar os direitos fundamentais da pessoa com a crescente coleta de dados possibilitada pelas novas tecnologias, a privacidade assume um conceito menos liberal e passa a ser analisada como um instrumento de controle dos "mineradores" das informações, limitando a sua capacidade de coleta e disposição dos dados. Contudo, angustia reconhecer o descompasso entre a rapidez do progresso tecno-

lógico e a lentidão da capacidade de elaboração de instrumentos jurídicos que moldurem essa nova realidade. Com base nesta constatação, é preciso pensar em remédios institucionais adequados – políticas regulatórias, por exemplo –, na medida em que os remédios jurídicos existentes – normas jurídicas proibitivas – encontram-se engessados, obsoletos ou fadados à obsolescência, na medida em que a tecnologia vai se aprimorando e evoluindo.

Por tudo o que foi exposto acima, verifica-se que não é adequado relegar as questões e problemas relacionados à proteção a privacidade na justificativa patrimonial e liberal do livre, esclarecido e desimpedido consentimento da pessoa detentora dos dados. São necessárias novas formas de tratamento jurídico da privacidade, para fins de permitir um maior amparo da pessoa no que diz respeito ao controle dos seus próprios dados.

A IOT E A TUTELA DA PRIVACIDADE: QUE TIPO DE REGULAÇÃO?

Um dos casos emblemáticos a respeito dos potenciais abusos no uso da tecnologia da IoT, representando um aspecto negativo relevante, foi denunciado pelo *site* The Daily Beast,[8] em artigo no qual foi apontado que determinadas SmartTVs da Samsung estariam gravando o que se fala no ambiente e disponibilizando as informações coletadas por meio de compartilhamento para fins de criação de perfis de consumo. Isso se tornou possível porque alguns modelos de TVs da Samsung possuem uma funcionalidade de busca de conteúdos por meio da utilização de um microfone embutido no controle remoto da TV. Como o padrão de fábrica das TVs pré-determina que o microfone estará em modo operacional, o consumidor deve realizar a opção nas configurações da TV para desabilitar o microfone, o que raramente é feito, seja por conveniência, seja por ignorância.

Depois de denunciado o caso, buscou-se analisar os termos de uso e política de privacidade para as TVs inteligentes – que sempre estiveram disponibilizados, diga-se, no qual se lia, entre outras cláusulas, que: "Esteja ciente de que se suas palavras faladas provenientes de sua TV incluem informações pessoais ou confidenciais, tão possível quanto provável que estes dados sejam capturados e transmitidos a terceiros".[9] Confrontada

8 HARRIS, Shane. Your Samsung SmartTV Is Spying on You, Basically. Disponível em: <http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smart-tv-is-spying-on-you-basically.html>. Acesso em: 04 dez. 2017.

9 No original: Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and trans-

com questionamentos sobre eventuais violações ao direito de privacidade dos usuários de suas TVs inteligentes, a Samsung, indagada sobre a configuração do microfone do controle remoto, respondeu que:

> A Samsung trata a privacidade do consumidor de maneira séria. Em todas as nossas SmartTVs nós utilizamos padrões de segurança de fábrica, incluindo criptografia de dados, para assegurar as informações pessoais do consumidor e prevenir a coleta ou uso não autorizados por terceiros. O reconhecimento de voz, que permite ao usuário controlar sua TV por meio de comandos de voz é uma característica da Samsung SmartTV, que pode ser ativada ou desativada pelo usuário. O usuário da TV pode também desconectar sua TV da rede wi-fi.[10]

A declaração da Samsung tenta justificar a coleta de dados e a violação eventual da privacidade, mais uma vez, na existência de um consentimento por parte da pessoa a respeito dos termos que ela adere ao adquirir uma SmartTV, ainda que se saiba que esta adesão consensual é mera ficção e pode não representar verdadeiramente o desejo do usuário.

Tem-se, em conclusão, um problema jurídico que surge do uso de uma determinada tecnologia, que leva à necessária construção de critérios que podem nortear decisões – sejam elas privadas, legislativas ou judiciais – no que diz respeito à tutela da privacidade. O primeiro destes critérios é a necessidade de descrição da tecnologia e de sua potencialidade no que diz respeito aos dados eventualmente coletados. Em outras palavras, a pessoa que utiliza a tecnologia deve ter o conhecimento da possibilidade de coleta de dados pessoais. Logo em seguida, deve ser possível ao usuário da tecnologia ter conhecimento da política de privacidade do fornecedor do produto/serviço, de forma clara e eficiente, levando a um entendimento sobre o que significa a adesão aos termos de uso do serviço. Em continu-

---

mitted to a third party. HARRIS, Shane. Your Samsung SmartTV Is Spying on You, Basically. Disponível em: <http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html>. Acesso em: 04 dez. 2017.

10 No original: Samsung takes consumer privacy very seriously. In all of our Smart TVs we employ industry-standard security safeguards and practices, including data encryption, to secure consumers' personal information and prevent unauthorized collection or use," the company said in a statement to The Daily Beast. "Voice recognition, which allows the user to control the TV using voice commands, is a Samsung Smart TV feature, which can be activated or deactivated by the user. The TV owner can also disconnect the TV from the Wi-Fi network. HARRIS, Shane. Your Samsung SmartTV Is Spying on You, Basically. Disponível em: <http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html>. Acesso em: 04 dez. 2017.

ação, o critério da finalidade deve ser assegurado, isto é, o usuário deve ser avisado de que em caso de coleta de dados, estes serão usados para determinada finalidade que seja restrita ao âmbito do serviço utilizado, e não compartilhado com terceiros que não são parte do contrato de uso. Ainda, e mais importante, o usuário sempre terá a possibilidade de decidir sobre as formas de coleta, uso e compartilhamento de seus dados, exercitando de maneira plena a sua autodeterminação informativa, inclusive para fins de verificação e correção dos dados coletados, evitando o acesso não autorizado, o uso indevido dos dados, sua modificação e sua divulgação sem autorização.

A questão primordial suscitada no início deste ensaio é a que diz respeito à ignorância da sociedade de uma maneira geral a respeito da importância da proteção dos dados pessoais. É necessário criar uma cultura e fomentar a educação das pessoas no que diz respeito aos problemas que surgem com o compartilhamento e a divulgação de dados pessoais. A sociedade é muito pouco mobilizada para fins de debates sobre o que significa um dado pessoal, um dado sensível, e porque é relevante protegê-los. Além de eventuais projetos legislativos que permitam o desenvolvimento desta tecnologia e ao mesmo tempo a tutela dos dados, é necessário se pensar em políticas públicas em educação com relação a proteção de dados.

Deve-se reconhecer que se a regulação tecnológica está crescendo mais rápido do que a nossa capacidade de garantir segurança e privacidade aos usuários, estamos falhando em ter uma regulamentação apropriada confirmada pela lei. Um cenário jurídico adequado seria a resposta a esses novos desafios legais (MAGRANI, [s.d.]). Mas será que somente a promulgação de leis seria suficiente? Seria interessante se pensar num regime de proteção de dados pessoais que ao mesmo tempo fosse embasado em leis, como também por meio da autorregulação e pelo uso da tecnologia, com o desenvolvimento de mecanismos de segurança cada vez mais sofisticados e criptografia de última geração.

Contudo, considerando que há uma dependência crescente entre a cessão de dados e o acesso a serviços, observa-se que a regulação da tecnologia como forma de proteção da privacidade, ao invés de possibilitar a tutela adequada dos dados pessoais, revela um problema de ordem prática: é que a privacidade passa a se tornar obsoleta, considerando a necessidade de constante revelação dos dados pessoais para a aquisição de produtos e serviços. O dilema reside no fato de que para estar no mundo da tecnologia e usufruir da sua potencialidade de conveniências e utilidades é necessário renunciar à proteção dos dados pessoais, que se tornam, em grande medida, a moeda de troca padrão destes serviços.

Presencia-se agora um período de hiato regulatório/legislativo que se deve, em grande medida, ao fato de não ter sido ainda possível identificar na sociedade brasileira a forma mais eficiente de tutela dos dados pessoais:

I. se por lei restritiva, impedindo por vezes, o avanço da tecnologia, ou tornando-se obsoleta pela implementação de novas tecnologias com novos problemas jurídicos em seu enlace;

II. se por regulação por meio de agências públicas (como a autoridade garantidora da privacidade na Itália), que determinam passo a passo quais as condutas que devem ser permitidas e quais as que devem ser proibidas, gerando, por vezes um casuísmo exacerbado e por outras uma omissão na atividade regulatória, ocasionada pela pressão das empresas de tecnologia em lucrar;

III. se pela autorregulação pela tecnologia, por meio de adoção de sistemas de segurança por meio de criptografia ou outras técnicas inovadoras que protejam os dados pessoais; ou, por fim, se pela autorregulação pelo mercado e pela economia, considerando os dados pessoais como insumos e moeda de troca possível na sociedade hiperconectada.

Esta última alternativa é, de longe, a que deve ser evitada e afastada, pois a "coisificação" dos dados pessoais configura uma mercantilização do corpo eletrônico e uma violação frontal ao direito fundamental à identidade e à integridade. As demais formas de regulação e proteção de dados pessoais são possíveis e conciliáveis. O próximo passo é encontrar o equilíbrio entre conceder de forma plena o direito à autodeterminação informativa e permitir, ao mesmo tempo, o pleno desenvolvimento de novas tecnologias que utilizam os dados pessoais como insumo para a efetiva realização de suas finalidades.

REFERÊNCIAS

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/anexos/8196-8195-1-PB.htm>. Acesso em: 04 dez. 2017.

DONEDA, Danilo; ALMEIDA, Virgilio; MONTEIRO, Marilia. Governance challenges for the Internet of Things. Disponível em: <ieeexplore.ieee.org/document/7131425/>. Acesso em: 04 dez. 2017.

HARRIS, Shane. Your Samsung SmartTV Is Spying on You, Basically. Disponível em: <http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smart-tv-is-spying-on-you-basically.html>. Acesso em: 04 dez. 2017.

LEWICKI, Bruno. *A privacidade da pessoa humana no ambiente de trabalho*. Rio de Janeiro: Renovar, 2003.

MAGRANI, Eduardo. Threats of the internet of things in a techno-regulated society. Mimeografado. [S.l.: s.n.: s.d.].

OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, Colorado, v. 57, p. 1701, 2010.

PAGALLO, Ugo. What Is New with the Internet of Things in Privacy. Disponível em: <link.springer.com/chapter/10.1007%2F978-3-319-50796-5_3>. Acesso em: 04 dez. 2017.

RODOTÀ, Stefano. *La vida y las reglas:* entre el derecho y el no derecho. Traducción de Andrea Greppi. Madrid; Trotta: Fundación Alfonso Martín Escudero, 2010.

RODOTÀ, Stefano. **A** *vida na sociedade da vigilância:* a privacidade hoje. Organização, seleção e apresentação de: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. *La rivoluzione della dignità*. Napoli: La Scuola di Pitagora, 2013.

SOLOVE, Daniel. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, v. 154, n. 3, 2006.

WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty (2004). Faculty Scholarship Series. Paper 649. Disponível em: <http://digitalcommons.law.yale.edu/fss_papers/649>. Acesso em: 04 dez. 2017.

INTERNET DAS COISAS ANÔNIMAS (ANIOT): CONSIDERAÇÕES PRELIMINARES

EDUARDO MAGRANI
LUIZ ABRAHÃO

ANONIMATO *ONLINE* EM FOCO[1]

A imagem reproduzida a seguir consiste em um mapa cartográfico elaborado por pesquisadores do Oxford Internet Institute.[2] Eles se basearam em informações disponíveis no portal Tor Metrics,[3] o qual nos auxilia a observar a dinâmica dos acessos globais à Internet através de redes TOR.[4] Contudo, apesar dos dados mostrarem um interesse crescente pela anonimização *on-line* (LEVMORE; NUSSBAUM, 2010; ALLEN, [s.d.]) em várias partes do mundo, os aspectos técnicos, legais ou éticos subjacentes ao anonimato permanecem suscitando controvérsias (GREEN; KAROLIDES, 1990; STRYKER, 2012). O pensador Zygmunt Bauman estruturou um ataque acadêmico ao anonimato *on-line* no ensaio *Sobre a internet, anonimato e irresponsabilidade* (BAUMAN, 2012). Nele, o pensador diz que o anônimo é uma espécie de "mosca antissocial", cujas "armas mortais" seriam a calúnia, a injúria, a difamação, o insulto, a ofensa, a infâmia etc. Os fun-

1 Algumas ideias elaboradas e discutidas neste texto foram originalmente apresentadas e debatidas por ocasião do II Seminário Governança das Redes e o Marco Civil da Internet, promovido pelo Grupo de Estudos Internacionais de Propriedade Intelectual, Internet e Inovação (GNet), da UFMG, e o Instituto de Referência em Internet e Sociedade (IRIS), ocorrido entre os dias 26 e 27 de outubro de 2016 na Faculdade IBMEC, Belo Horizonte/MG.

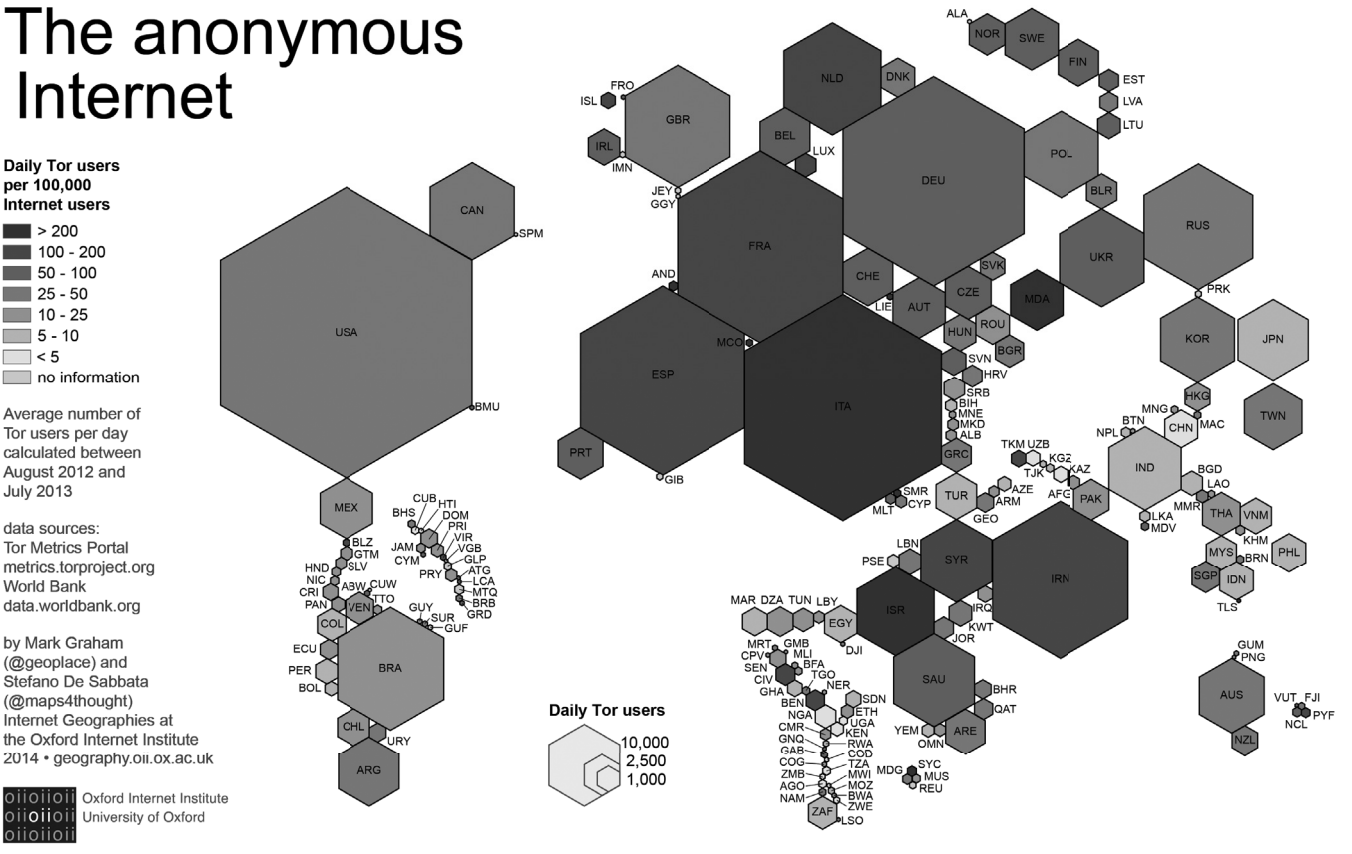
2 INFORMATION GEOGRAPHIES.. <http://geography.oii.ox.ac.uk/>. Acesso em: 05 jul. 2018.

3 TOR METRICS. Users. Disponível em: <https://metrics.torproject.org/users-stats-relay-country.html>. Acesso em: 05 jul. 2018.

4 Acrônimo para The Onion Router é um software livre que proporciona o anonimato pessoal ao navegar na Internet e em atividades online.

cionários da Google E. Schmidt e J. Cohen formularam um ataque moral ao anonimato *on-line* na obra *The New Digital Age: Reshaping the Future of People, Nations and Business* (SCHMIDT; COHEN, 2013). No capítulo V, intitulado "The Future of Terrorism - No Hidden People Allowed", eles escreveram que "pessoas ocultas" no "ecossistema tecnológico" poderiam ser qualificadas como "terroristas em potencial" (ASSANGE, 2015). Os ataques técnicos ao anonimato *on-line* foram expostos no vazamento do "TOR Stinks Document". Relatórios da NSA/CGHQ mostravam tentativas de desanonimizar computadores com *software* TOR através de invasões remotas. Por fim, há também ataques institucionais que pretendem criminalizar a anonimização *on-line*. Por exemplo, a emenda à "Rule 41" das Federal Rules of Criminal Procedure, U.S. Supreme Court foi elaborada visando autorizar o Departamento de Justiça e o FBI a buscar informações em computadores que instalaram o sistema TOR. Então, como podemos perceber, o anonimato *on-line* é alvo de críticas acadêmicas, morais, técnicas e governamentais.

Figura 1 – Mapa da internet anônima



Fonte: INFORMATION GEOGRAPHIES. Disponível em: <http://geography.oii.ox.ac.uk/?page=tor>. Acesso em: 09 jul. 2018.

Em defesa do anonimato *on-line*, no entanto, existem figuras de destaque como o jornalista e ativista Glenn Greenwald (2014, p. 263, grifos nossos):

> […] para impedir os governos de se intrometerem em suas comunicações e em sua atividade pessoal na internet, *todos os usuários deveriam adotar ferramentas de criptografia e de anonimato para a navegação*. Isso é particularmente importante para quem trabalha em áreas sensíveis, como jornalistas, advogados e ativistas de direitos humanos. E a comunidade de tecnologia deve continuar a desenvolver programas de anonimato e criptografia mais eficazes e mais fáceis de usar.

Essa postura converge com um valor fortemente associado à cultura *hacker* (HIMANEN, 2001; JORDAN, 2002; THOMAS, 2003; ERICKSON, 2008; LEVY, 2010; COLEMAN, 2012) a saber, a *expertise* tecnológica pode contribuir para equilibrar as relações de poder na sociedade, permitindo que os cidadãos resistam contra as diversas ameaças de invasão de privacidade na era digital. Nessa perspectiva, a democratização e a disseminação de práticas de anonimização *on-line* constituem métodos não violentos de proteção da privacidade – ou "*hacking* defensivo". Seguindo o que Julian Assange afirmou em *Cypherpunks* (ASSANGE, 2013, p. 151), ferramentas e técnicas de anonimização *on-line* podem ser encaradas como "formas específicas de tecnologia" capazes de garantir "direitos e liberdades fundamentais que diversas pessoas passaram tanto tempo desejando".

ANONIMATO *ON-LINE* ENQUANTO INSTÂNCIA DO DIREITO À PRIVACIDADE E O IMPACTO DA INTERNET DAS COISAS (IOT)

O direito à privacidade, esfera do direito correspondente à vida privada, está intimamente conectado à proteção da dignidade e personalidade humana (SARLET, 2012, p. 390), e pode ser extraído do reconhecimento constitucional e infraconstitucional que é dado à intimidade, vida privada[5] inviolabilidade de dados (DONEDA; MENDES, 2014, p. 15).[6] [7] Com o

5 Constituição Federal de 1988, art. 5º (…) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

6 Constituição Federal de 1988, art. 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

7 A doutrina destaca que apesar de haver alguns instrumentos no ordenamento jurídico brasileiro e até leis que se destinam a proteger a privacidade, é preciso de algo mais específico: "Although some problems regarding data protection in Brazil

desenvolvimento social e tecnológico, diferentes facetas da privacidade surgiram. Na sociedade da informação, a privacidade deve ser entendida de forma funcional, de modo a assegurar a um sujeito a possibilidade de "conhecer, controlar, endereçar e interromper o fluxo das informações a ele relacionadas" (RODOTÀ, 2008, p. 92-95). Neste sentido, Stefano Rodotà define a privacidade como "o direito de manter o controle sobre as próprias informações" (RODOTÀ, 2008, p. 92-95). A privacidade, atualmente, possui uma amplitude conceitual maior em comparação à sua acepção original – "direito de ser deixado só" ou *right to be let alone* – (WARREN; BRANDEIS, 1890, p. 193-220). Ela transcende, assim, tanto o caráter de liberdade negativa – liberdade de não ser impedido ou de não ser obrigado a fazer algo – como o de liberdade positiva[8] (BOBBIO, 1997, p. 48-49) – liberdade como autonomia, liberdade enquanto possibilidade de direcionar seu próprio querer sem ser determinado por outros, ligada ao controle dos dados, o que se deve ao contexto social advindo de evoluções tecnológicas (MACEDO JÚNIOR, 1999, p. 245-259). Com efeito, a noção de privacidade na era da informação também deve englobar o próprio controle dos dados digitais (MULHOLLAND, 2012, p. 3).[9]

Uma das evoluções tecnológicas contemporâneas que tende a impactar profundamente a proteção da privacidade é a "Internet das Coisas" – Internet of Things" (IoT), em inglês. A expressão consiste em um termo "guarda-chuva" (MIORANDI, 2012, p. 1497-1516) e foi atribuída a Kevin Ashton (1999).[10] Sinteticamente, a IoT refere-se a um complexo ecossistema

---

require enforcement measures […], there are some issues that can only be adequately addressed by a broad regulation such as a comprehensive data protection act. This would increase the legal certainty of business activities against the risks to privacy arising from data processing. This explains why there have been many attempts to create a general legal framework for data protection in Brazil."

8 Para Bobbio, [p]or liberdade positiva, entende-se -na linguagem política -a situação na qual um sujeito tem a possibilidade de orientar seu próprio querer no sentido de uma finalidade, de tomar decisões, sem ser determinado pelo querer de outros. Essa forma de liberdade é também chamada de autodeterminação ou, ainda mais propriamente, de autonomia".

9 Caitlin Mulholland, por exemplo, apresenta três concepções sobre o direito à privacidade, quais sejam, "(i) o direito de ser deixado só, (ii) o direito de ter controle sobre a circulação dos dados pessoais, e (iii) o direito à liberdade das escolhas pessoais de caráter existencial" e acrescenta a esta lista o direito de não tomar conhecimento acerca de um dado pessoal".

10 Kevin Ashton utilizou a expressão "Internet of Things" em 1999 em uma apresentação realizada na P&G.

sociotécnico e infofísico de artefatos dinâmicos interconectados entre si. A IoT engloba tecnologias de interação comunicativa pessoas-máquinas e máquinas-máquinas por meio de redes sem fio com vistas aos mais diversos usos – doméstico/pessoal; empresarial/negócios; industrial.

Em certo sentido, a IoT seria análoga a uma "ontologia *hiperconectada*": a efetiva transmissão de *qualquer* conteúdo ou *qualquer* serviço, em *qualquer* lugar, a *qualquer* hora, para *qualquer* dispositivo ou por *qualquer* usuário, e assim por diante. Pesquisas recentes estimam que em menos de cinco anos a quantidade de objetos interconectados estará na casa de dezenas de bilhões. Mais especificamente, projeções referentes ao impacto da IoT projetam a existência de cerca de 100 bilhões de dispositivos inteligentes conectados entre si, implicando um impacto econômico global superior a US$ 11 trilhões em 2025 (ROSE; ELDRIDGE; CHAPIN, 2015). Nessa linha, em pouco tempo, a IoT poderá alterar significativamente nossa forma de vida, despontando, inclusive, como possível solução para desafios de gestão pública, trazendo saídas mais eficazes para variados problemas – por exemplo, poluição, congestionamentos, criminalidade e eficiência produtiva.

A IoT, no entanto, ainda suscita diversos desafios técnicos e conceituais (AGRAWAL; VIEIRA, 2013, p. 78-95). Dentre eles, convém destacar os referentes ao endereçamento e questões de rede, aos protocolos de roteamento em comunicação, à padronização, ao congestionamento de tráfego e à sobrecarga na rede, e até questões mais basilares, como o próprio acesso à rede. Além disso, o cenário de IoT também impõe reflexões ético-legais, em particular as relacionadas à proteção da privacidade e segurança dos dados pessoais e sensíveis, uma vez que no horizonte da IoT inúmeros dispositivos conectados entre si acompanharão diariamente a rotina digital de equipamentos, empresas, indústrias, instituições e pessoas.

Uma quantidade imensurável de dados, incluindo aqueles estritamente pessoais e sensíveis será coletada, transmitida, armazenada e compartilhada. Portanto, o aumento exponencial de usos, camadas e tipos de dispositivos conectados – muitos já acessíveis ou em vias de lançamento no mercado – pode consistir em um risco substancial aos usuários. A preocupação com a privacidade dos dados no âmbito da IoT se revela ainda mais relevante quando notamos a prevalência de um cenário ainda fortemente marcado pela falta de uma regulação específica que tutele os dados pessoais *on-line* de forma suficiente e eficaz.

ANONIMIZAÇÃO *ON-LINE* E ANONIMATO NO CONTEXTO DA IOT: A TESE DO "DIREITO AO NÃO-RASTREIO"

É perceptível um aumento na literatura especializada sobre o anonimato *on-line* e as técnicas de anonimização.[11] De forma esquemática, tais estudos podem ser organizados em três eixos principais: (i) *análise de legislação* (KERR; STEEVES, 2009), (ii) *guias técnicos e de prática* (WANG; REEVES, 2015; LOSHIN, 2013); e (iii) *estudos históricos e conceituais* (WEBER; HEINRICH, 2012). Um esclarecimento conceitual que convém realizar de saída se refere à crítica da abordagem estritamente etimológica para a noção de "anonimato". Liddell e Scott (2001) mostram que o campo semântico original de *anonymous* – bem como dos correlatos gregos *anonymei* ou *anonymia* – envolve, essencialmente, a ideia de algo ou alguém "sem nome". Porém, diversamente do que a visão tradicional considera, a categoria do anonimato *on-line* não diz respeito a qualquer aspecto relacionado estritamente ao "nome" – seja o nome real, um apelido ou um pseudônimo – do usuário de um dispositivo conectado à Internet. Isso se deve ao fato de que, na era da informação, existem diversos mecanismos de identificação pessoal que dispensam qualquer identificação do "nome" em si.

Marx (1999) nos ajuda a compreender essa tese ao mostrar que, mesmo *off-line*, podemos ser parcialmente identificados por meios que não recorrem ao nome, tais como: (i) localização física ou lógica – endereço ou CEP –; (ii) símbolos numéricos ou alfabéticos associados – CPF ou apelido –; (iii) pseudônimo que não pode ser associado ao nome ou à localização; (iv) padrão de conhecimento – aparência ou comportamento –; (v) categorização social – gênero, ideologia, orientação sexual etc. –; ou (vi) símbolos de elegibilidade – uniformes, habilidades, performances etc. De forma a complementar esse esclarecimento conceitual, cumpre salientar, na esteira de Nissenbaum (1999), a existência de diversas tecnologias de rastreio digital as quais possibilitam uma espécie de "identificação sem nome". São exemplos dessas tecnologias de rastreio digital: estatística analítica por extração de dados – *data mining* –, *click-stream tracking* – rastreio de interesses –, identificação de usuário via padrões de navegação – *browsing Patterns* –, interceptação e análise de tráfego de redes/pacotes de dados – *sniffer* – ou coleta automática de dados – IP, histórico de navegação e *downloads* – (JAWORSKI, 2011).

Portanto, em certa medida, na era da informação digital a identificação pessoal se deslocou do "nome" para a possibilidade técnica de rastrear

11 Cf.: FREE HAVEN. Selected Papers in Anonymity. Disponível em: <https://www.freehaven.net/anonbib/topic.html>. Acesso em: 18 abr. 2017.

dados associados a dispositivos conectados à rede internacional de computadores. Com base nisso, Kathleen Wallace (1999, 2008) propôs uma definição específica de anonimato *on-line* a qual se concentra na ideia da "não coordenação de traços conhecidos" – características, ações, endereços etc. – em determinadas relações comunicativas. Segundo essa leitura exprime, algumas características importantes da anonimização *on-line* seriam: gradualidade – distribui-se por níveis: fraco/forte, mínimo/máximo –; parcialidade – não total – (STRYKER, 2012); circunstancialidades – depende de ferramentas e saberes –; contextualidade – refere-se a traços específicos –; volitividade – envolve uma intenção de anonimização –; e bidirecionalidade – relação de pessoa/dispositivo A com B.

Com efeito, o anonimato *on-line* poderia ser descrito como uma *resistência ao rastreio digital* – ou um direito ao não-rastreio. Em uma conceituação mais global, o anonimato *on-line* envolveria capacidades cognitivas e materiais para elaborar e empregar voluntariamente, pelo máximo tempo e na maior extensão possível, ferramentas tecnológicas – *softwares*, aplicativos, navegadores, buscadores etc. – e saberes técnicos com o objetivo de assegurar a invisibilização de informações confidenciais e a ocultação de dados privados por meio da limitação da interceptação, da coleta, da análise, do monitoramento, do controle, do armazenamento ou do rastreio digital de metadados sigilosos ou de dispositivos pessoais conectados à rede mundial de computadores.

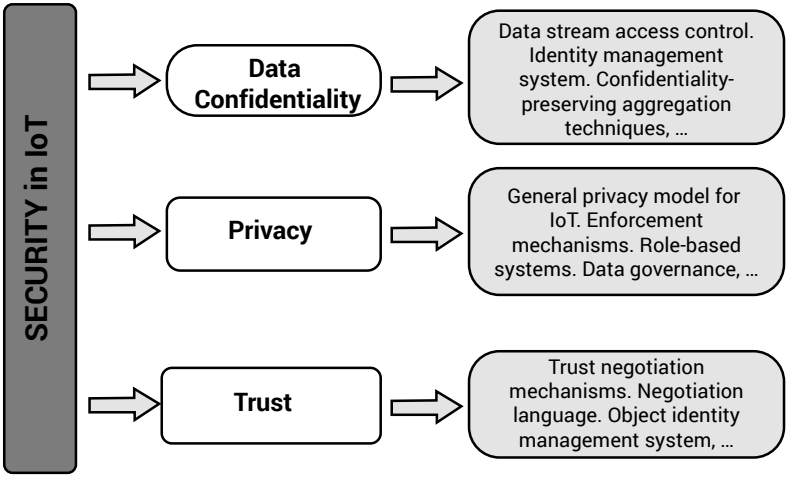
Quando, porém, consideramos o contexto específico da IoT, a discussão geral concernente à privacidade na Internet – e, em particular, aquela atinente ao anonimato *on-line* – atinge um novo – e, em certa medida, até mesmo inexplorado – patamar. Afinal, isso equivaleria a formular questões como: Será possível garantir tamanha hiperconectividade e, ao mesmo tempo, proteger a privacidade? O que seria uma "coisa" anônima na IoT? Ou ainda, em que medida deveríamos reconhecer máquinas como sujeitos de direitos? (CASTRO, 2013).

Roman, Najera e Lopez (2011) elencam diversos obstáculos para a implementação plena da IoT no que concerne à questão da privacidade e segurança, incluindo: (i) o risco de ataques – DDoS; clonagem/emulação de RFID; *cracking* –, (ii) os erros no funcionamento – *spamming* –, (iii) a insuficiência das proteções digitais usuais – protocolos de segurança; garantias de privacidade; métodos criptográficos – e a (iv) estrutura técnica e legal. Miorandi *et al.* (2012) também admitem que a segurança consiste em um "componente crítico" para a adesão ampla das tecnologias e aplicações da IoT, insistindo na insuficiência de soluções não *ad hoc* de confidencialidade, autenticidade e privacidade, conforme a Figura 2.

Por sua parte, Ziegeldorf, Morchon e Wehrle (2014) compreendem a interconexão e cooperação ampla de objetos inteligentes como uma "evolução da Internet" em direção ao "mundo real". Entretanto, reconhecem que a "coleta ou rastreio de dados ubíquos" consiste em uma "ameaça à privacidade" que colocaria em dúvida o êxito pleno da IoT. Jing *et al.* (2014) sublinham que os problemas de segurança e privacidade no contexto da IoT apresenta semelhanças com os das redes tradicionais, mas admite que a IoT represa um "ambiente mais perigoso". Assim, propõem um modelo de proteção da arquitetura do sistema que abarque, no mínimo, três camadas básicas: (i) Camada de percepção – Uniform Coding, Conflict Collision, RFID Privacy Protection, Trust Managemen –; (ii) Camada de transporte – *network access control technology* –; e (iii) Camada de aplicação – *network control technology, communications technology e mobile terminal technology*.

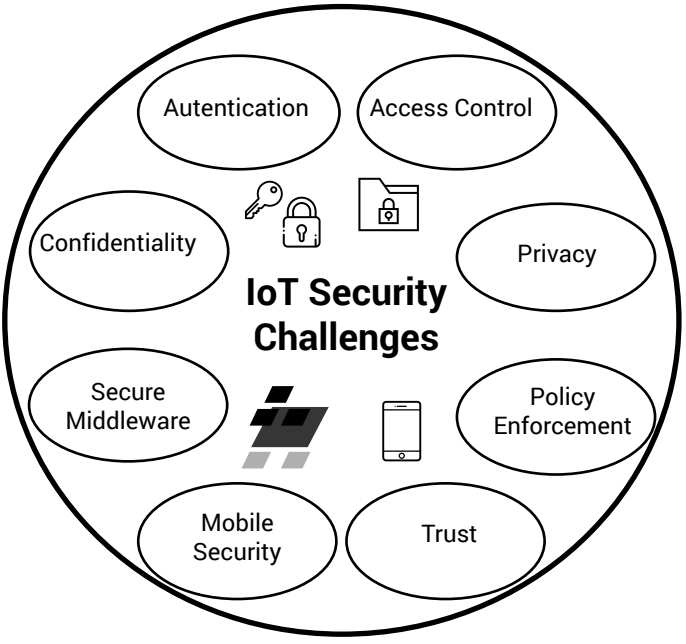
Por fim, Sicari *et al.* (2015) descrevem a IoT como um conjunto de tecnologias heterogêneas com serviços inovadores os quais reavivam as questões atinentes à "satisfação com segurança" e às "exigências de privacidade", dentre elas: (i) confidencialidade de dados, (ii) autenticação, (iii) controle de acesso à rede, (iv) privacidade e confiança entre usuários e (v) políticas de segurança e privacidade. Nesse cenário, como vemos na Figura 3, eles apontam para uma insuficiência dos métodos tradicionais frente aos padrões flexíveis e infraestrutura da IoT.

Figura 2 - Representação gráfica dos desafios de segurança na Internet das coisas



Fonte: Miorandi *et al.* (2012), p. 1505.

Figura 3 - Panorama da insuficiência dos métodos tradicionais de segurança no contexto da Internet das coisas



Fonte: Sicari *et al.* (2015), p. 147.

Como podemos notar, há uma crescente e variada discussão sobre segurança e privacidade na recente bibliografia especializada devotada à IoT:

I. em *artigos*: Atzori *et al.* (2010), Bandyopadhyay e Sem (2011), Roman, Najera e Lopez (2011), Tobias Heer *et al.* (2011), Miorandi *et al.* (2012), Bin Guo *et al.* (2013), Roman *et al.* (2013), Ziegeldorf *et al.* (2014), Chabridon *et al.* (2014), Qi Jing *et al.* (2014), Borgia (2014), Ashraf *et al.* (2015) ou Sicari *et al.* (2015);

II. em *livros*: Michahelles (2011), Wang e Zhang (2012), Boswarthick e Elloumi (2012), McEwen e Cassimally (2013), Nik Bessis e Ciprian Dobre (2014), Jan Höller (2014), Joe Weinman e Fred Wiersema (2015), Jonathan Follett (2015), Nitesh Dhanjani (2015) ou Philip N. Howard (2015);

III. em *manuais técnicos*: Daniel Kellmereit e Daniel Obodovski (2013), Shancang Li *et. al.* (2014), Salvatore Gaglio e Giuseppe Lo Re (2014), Hazim Dahir, Bil Dry e Carlos Pignataro (2015), Othmar Kyas (2015),

Peter Waher (2015), Robert Stackowiak *et al.* (2015) ou Alasdair Gilchrist (2016). Esse aumento, entretanto, contrasta com o espaço restrito dedicado à inexplorada questão do anonimato *on-line* no contexto da IoT.

De forma esquemática, o tema do anonimato *on-line* na IoT (AnIoT) pode ser distribuído nas seguintes categorias analíticas:

1. Gerenciamento de identidade dos objetos;
2. Mecanismos de proteção da privacidade;
3. Proteção contra a associação de "biodado" à identidade/endereço IP;
4. Proteção da privacidade em tecnologias RFID de esquemas baseados em senhas;
5. Impedir usuários –humanos e máquinas – não autorizados de acessar o sistema.

Uma aposta de aprimoramento da discussão acerca da AnIoT pode residir em pesquisas sobre Privacy Enhancing Technologies (PET) (FISCHER-HÜBNER; WRIGHT, 2012). Em seus aspectos gerais, há PETs referentes (i) ao nível indivíduo/objeto/transação/dado e sistema, (ii) à Platform for Privacy Preferences (P3P) – por exemplo, a programação do próprio *browser* – ou (iii) às iniciativas de certificação digital referentes a técnicas, práticas e procedimentos em infraestrutura de chave pública (ICP). No âmbito estritamente técnico, destacam-se o recurso a Virtual Private Networks (VPN), Transport Layer Security (TLS), DNS Security Extensions, Roteamento por camadas, Private Information Retrieval (PIR), Sistemas *peer-to-peer* (P2P) ou RFID Tags. O importante nesse momento, porém, consiste em reconhecer – como detalha a Figura 3 – que todas abordagens mencionadas apresentam vantagens e desvantagens (WEBER;WEBER, 2010, p. 51).

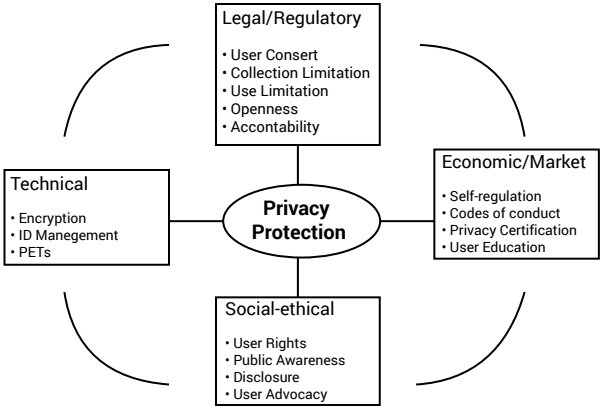
A iminência da IoT coloca as questões de segurança e privacidade em nova chave. São necessárias a elaboração de abordagens técnica, regulatórias e educativas para lidar, no contexto da IoT, com as ameaças potenciais à privacidade, as falhas na confidencialidade, a autoproteção – anonimização –, a interação segura e a identificação e notificação de falhas. Com efeito, conforme a Figura 4 (WEBER; WEBER, 2010, p. 67) revela, somente uma abordagem global – técnica, regulatória e educacional – (Baggio; Beldarrain, 2011) da proteção da privacidade proporcionará uma navegação segura na IoT.

Figura 4 – Quadro de vantagens e desvantagens de métodos/ técnicas disponíveis para proteção da privacidade

	Measure	Functioning	Advantage	Disadvantage
1	VPN	Extranets	Confidentiality Data integrity	No global exchange
2	TLS	Additional layers	Confidentiality Data integrity	Negative effect on search of information
3	DNSSEC	Public-key Cryptography	Authenticity Data integrity	Confidentiality not adressed Scalability issues Only one root Problems in building chains of trust
4	Onion Routing	Multiple encryption layers	Anonymity	Performance issues Confidentiality & integrity not adressed
5	PIR	Conceal identity of users	Anonymity	Scalability issues Performance issues
6	P2P	Decentralized data	Decentralization Anonymity if encryption	Access control has to be introduced
7	Switching off of Tags	Disable or "kill"	Protection of Privacy	Not all tags "killed"/deactivated Used as incentive by business Useful information "killed"/ deactivated

Fonte: Weber; Weber, 2010, p. 51.

Figura 5 – Eixos principais da proteção da privacidade no contexto da Internet das coisas



Fonte: Weber; Weber, 2010, p. 67.

CONCLUSÃO

A literatura especializada reconhece que debates sobre segurança e privacidade são centrais para a plena implementação da IoT. Pesquisadores destacam a necessidade de soluções robustas para temas como confidencialidade, autenticidade e privacidade, inclusive com modelos e métodos não tradicionais de proteção da arquitetura do sistema os quais abarquem as camadas de percepção, transporte e aplicação. Porém, por mais que esteja crescendo a discussão sobre segurança e privacidade no contexto da IoT, são poucos os artigos, livros ou manuais técnicos que se dedicaram à temática do anonimato *on-line* no contexto da IoT – AnIoT, como designamos.

Como vimos, a IoT desponta como uma das tecnologias contemporâneas potencialmente mais disruptivas no que concerne à proteção da privacidade. A capacidade da IoT coletar, transmitir, armazenar e compartilhar dados pessoais/sensíveis de equipamentos, empresas, indústrias, instituições ou indivíduos suscita enormes desafios ético-legais, uma vez considerada a imensurável interação comunicativa entre pessoas-máquinas e máquinas-máquinas por meio de redes sem fio. Nesse sentido, a concepção clássica de privacidade enquanto "direito de ser deixado só" – *right to be let alone* – já não parece ser suficiente, especialmente diante do cenário da hiperconectividade encenado pela IoT.

Ressaltamos que a era da informação desenvolveu diversas tecnologias para rastrear dados pessoais/sensíveis associados a dispositivos conectados à rede internacional de computadores e, por isso, sugerimos que uma reformulação conceitual da noção de privacidade deveria abarcar a ideia de "não rastreio" – ou da "não coordenação de traços conhecidos" como características, ações, endereços etc. – em determinadas relações comunicativas. A tese do anonimato como *direito ao não-rastreio* – e, por conseguinte, não-coleta, não-transmissão, não-armazenamento e não-compartilhamento – é, com efeito, uma definição mais geral acerca do conceito de privacidade relacionado aos dados digitais.

Embora o anonimato seja interpretado diversas vezes como proibido por meio de uma interpretação literal do art. 5º inc. IV da Constituição Federal, deve ter sua legitimidade – *on-line* e *off-line* – melhor compreendida e valorizada em determinadas situações onde constitui ferramenta fundamental – ainda que isso não seja amplamente reconhecido – para a garantia de direitos constitucionais – não somente relacionado à liberdade de expressão, mas também ao acesso à informação e ao direito à privacidade. Por outro lado, quando o anonimato – seja *off-line* ou *on-line* – é usado como artifício para o cometimento de ilícitos civis e criminais, entende-se neste caso como ilegítimo (FROOMKIN,1999).

Assim, por mais que encontremos propostas relativas ao gerenciamento de identidade dos objetos ou à proteção da privacidade em tecnologias RFID de esquemas baseados em senhas, ainda é preciso avançar uma análise – conceitual e técnica – referente ao ajuste da tese do direito ao não-rastreio ao contexto da IoT. Em outros termos, a ideia de uma AnIoT enquanto instância da privacidade no contexto da IoT ainda carece de maiores esclarecimentos conceituais e, inclusive, requer análises de viabilidade técnica, uma vez que, como mostramos acima, todas as abordagens de anonimização na IoT apresentam vantagens e desvantagens.

REFERÊNCIAS

AGRAWAL, Shashank; VIEIRA, Dario. A survey on internet of things. *Abakós*, v. 1, n. 2, p. 78-95, 2013.

ALLEN, Christina. Internet Anonymity in Contexts, The Information Society. *An International Journal,* n. 15, v. 2, p. 145-146, [s.d.].

ASHRAF, Qazi Mamoon; HABAEBI, Mohamed Hadi. Autonomic Schemes for Threat Mitigation in Internet of Things. *Journal of Network and Computer Applications*, v. 49, p. 112-127, 2015.

ASSANGE, J. *et al*. *Cypherpunks:* Liberdade e o futuro da Internet. São Paulo: Boitempo, 2013.

ASSANGE, J. *Quando o Google encontrou o WikiLeaks.* Tradução de Cristina Yamagami. São Paulo: Boitempo, 2015.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The Internet of Things: A Survey. *Computer Networks,* v. 54, n. 15, p. 2787-2805, 2010.

BAGGIO, Bobbe; BELDARRAIN, Yoany. *Anonymity and Learning in Digitally Mediated Communications:* Authenticity and Trust in Cyber Education. IGI Global, 2011.

BANDYOPADHYAY, Debasis; SEN, Jaydip. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, v. 58, n. 1, p. 49-69, 2011.

BAUMAN, Zygmunt. *Sobre a internet, anonimato e irresponsabilidade*: isto não é um diário. Rio de Janeiro: Zahar, 2012.

BESSIS, Nik; DOBRE, Ciprian. *Big Data and Internet of Things:* a Roadmap for Smart Environments. Nova York: Springer International Publishing, 2014.

BOBBIO, Norberto. *Igualdade e liberdade.* Tradução: Carlos Nelson Coutinho. 2. ed. Rio de Janeiro: Ediouro, 1997.

BORGIA, Eleonora. The Internet of Things Vision: Key Features, Applications and Open Issues. *Computer Communications*, v. 54, p. 1-31, 2014.

CASTRO, Marco Aurélio. *Direito e pós-humanidade:* quando os robôs serão sujeitos de direito. Curitiba: Juruá. 2013.

CHABRIDON, Sophie *et al*. A Survey on Addressing Privacy Together with Quality of Context for Context Management in the Internet of Things. *Annals of telecommunications-annales des télécommunications,* v. 69, n. 1-2, p. 47-62, 2014.

COLEMAN, Gabriella. *Coding Freedom*: The ethics and aesthetics of hacking. Princeton: Princeton University Press, 2012.

DAHIR, Hazim; DRY, Bil; PIGNATARO Carlos. *People, Processes, Services, and Things:* Using Services Innovation to Enable the Internet of Everything. Nova York: Business Expert Press, 2015.

DHANJANI, Nitesh. *Abusing the Internet of Things:* Blackouts, Freakouts, and Stakeouts. Newton: O'Reilly Media, Inc., 2015.

DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul De. (Eds.) **R***eloading Data Protection:* Multidisciplinary Insights and Contemporary Challenges. Londres: Springer, 2014.

ERICKSON, Jon. *Hacking:* the art of exploitation. San Francisco: No Starch Press, 2008.

FISCHER-HÜBNER, Simone; WRIGHT, Matthew (Ed.). *Privacy Enhancing Technologies:* 12th International Symposium, PETS 2012, Vigo, Spain, July 11-13, 2012, Proceedings. Nova York: Springer, 2012.

FOLLETT, Jonathan. *Designing for Emerging Technologies:* UX for Genomics, Robotics, and the Internet of Things. Newton: O'Reilly Media, Inc., 2014.

FREE HAVEN. Selected Papers in Anonymity. Disponível em: <https://www.freehaven.net/anonbib/topic.html>. Acesso em: 18 abr. 2017.

FROOMKIN, Michael. Legal Issues in Anonymity and Pseudonymity, **T***he Information Society: An International Journal*, n. 15, v. 2, p. 113-127, 1999.

GAGLIO, Salvatore; RE, Giuseppe Lo. *Advances onto the Internet of Things.* Nova York: Springer, 2014.

GILCHRIST, Alasdair. Introducing Industry 4.0. In: GILCHRIST, Alasdair. *Industry 4.0*. Nova York: Apress, 2016. p. 195-215.

GREEN, Jonathon; KAROLIDES, Nicholas J. *Encyclopedia of censorship*. Nova York: Facts on File, 1990.

GREENWALD, Glenn. *Sem lugar para se esconder*. Rio de Janeiro: Sextante, 2014.

GUO, Bin *et al*. From the Internet of Things to Embedded Intelligence. *World Wide Web*, v. 16, n. 4, p. 399-420, 2013.

HEER, Tobias *et al*. Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications,* v. 61, n. 3, p. 527-542, 2011.

HERSENT, Olivier; BOSWARTHICK, David; ELLOUMI, Omar. *The Internet of Things:* Key Applications and Protocols. Hoboken: John Wiley & Sons, 2011.

HIMANEN, Pekka. *The Hacker Ethics:* and the Spirit of Information Age. NY: Random House Trade Paperbacks, 2001.

HOLLER, Jan *et al*. *From Machine-to-Machine to the Internet of Things***:** Introduction to a New Age of Intelligence. Cambridge: Academic Press, 2014.

HOWARD, Philip N. *Pax Technica:* How the Internet of Things may set us Free or Lock Us Up. Nova Haven: Yale University Press, 2015.

INFORMATION GEOGRAPHIES. Disponível em: <http://geography.oii.ox.ac.uk/?page=tor>. Acesso em: 09 jul. 2018.

INFORMATION GEOGRAPHIES.. <http://geography.oii.ox.ac.uk/>. Acesso em: 05 jul. 2018.

JAWORSKI, Wojciech. Identifying Web Users on the Base of their Browsing Patterns. *International Journal of Computational Intelligence Systems*, v. 4, n. 5, p. 1062-1069, set. 2011.

JING, Qi *et al*. Security of the Internet of Things: Perspectives and Challenges. *Wireless Networks*, v. 20, n. 8, p. 2481-2501, 2014.

JORDAN, Tim**.** Activism! Direct Action, Hactivism and the Future of Society. London: Reaktion Books, 2002.KERR, Ian R.; STEEVES, Valerie M.; LUCOCK, Carole (Ed.). *Lessons from the Identity Trail:* Anonymity, Privacy and Identity in a Networked Society. Nova York: Oxford University Press, 2009.

KELLMEREIT, Daniel; OBODOVSKI, Daniel. *The Silent Intelligence:* the Internet of Things. São Francisco: DnD Ventures, 2013.

KYAS, Othmar. *How To Smart Home:* A Step by Step Guide to Your Personal Internet of Things. Wyk auf Föhr (Alemanha): Key Concept Press, 2015.

LEVMORE, Saul; NUSSBAUM, Martha C. *The Internet's Anonymity Problem:* The Offensive Internet. Speech, Privacy, and Reputation. HUP: Cambridge, Massachusetts, and London, England, 2010.

LEVY, Steven. *Hackers.* Sebastopol: O'Relly, 2010.

LI, Shancang; XU, Li. *Securing the Internet of Things.* Cambridge: Syngress, 2017.

LIDDELL and SCOTT. *Greek-English Lexicon*. 7. ed. Nova York: Oxford, 2001.

LOSHIN, Peter. *Practical Anonymity:* Hiding in Plain Sight Online. Waltham: Syngress, 2013.

MACEDO JÚNIOR, Ronaldo Porto. Privacidade, Mercado e Informação. *Justitia*, São Paulo, n. 61, p. 245-259, jan./dez. 1999.

MARX, G. What's in a Name? Some Reflections on the Sociology of Anonymity.*The Information Society, n.* 15, v. 2, p. 99-112, maio 1999.

MCEWEN, Adrian; CASSIMALLY, Hakim. *Designing the Internet of Things*. Hoboken: John Wiley & Sons, 2013.

MIORANDI, Daniele *et al*. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, v. 10, p. 1497-1516, 2012.

MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. *Civilistica.com*, Rio de Janeiro, v. 1, n. 1, p. 3, 2012.

NISSENBAUM, Helen. The Meaning of Anonymity in an Information Age. *The Information Society,* 15:141-144, 1999.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução deDanilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROMAN, Rodrigo; ZHOU, Jianying; LOPEZ, Javier. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. *Computer Networks*, v. 57, n. 10, p. 2266-2279, 2013.

ROMAN, Rodrigo; NAJERA, Pablo; LOPEZ, Javier. Securing the Internet of Things. *IEEE Computer*, v. 44, p. 51-58, 2011.

ROSE, Karen; ELDRIDGE, Scott; CHAPIN, Lyman. The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World. ISOC, 2015, p. 1. Disponível em: <https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf>. Acesso em: 09 jul. 2018.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional.* São Paulo: Editora Revista dos Tribunais, 2012.

SCHMIDT, Eric; COHEN, Jared. *The New Digital Age*: Reshaping The Future Of People, Nations And Business. Londres: Hachette UK, 2013.

SICARI, Sabrina *et al*. Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks*, v. 76, p. 146-164, 2015.

STACKOWIAK, Robert *et al*. *Big Data and the Internet of Things*: Enterprise Information Architecture for a New Age. Nova York: Apress, 2015.

STRYKER, Cole. *Hacking the Future*. Privacy, Identity, and Anonymity on the Web. NY: Overlook Duckworth, 2012.

THOMAS, Douglas. *Hacker Culture*. Minneapolis, London: University of Minnesota Press, 2003.

TOR METRICS. Users. Disponível em: <https://metrics.torproject.org/userstats-relay-country.html>. Acesso em: 05 jul. 2018.

UCKELMANN, Dieter; HARRISON, Mark; MICHAHELLES, Florian. *Architecting the Internet of Things.* Berlin: Springer, 2011.

WAHER, Peter. *Learning Internet of Things.* Birmingham: Packt Publishing Ltd, 2015.

WALLACE, K.A. On-line Anonymity. In: HIMMA, K.E.; TAVANI, H.T. (Eds.). *Handbook on Information and Computer Ethics*. New Jersey: Wiley, 2008. p. 165-189.

WALLACE, K.A. Anonymity**.** *Ethics and Information Technology,* n. 1, v. 1, p. 23-35, 1999.

WANG, Xinyuan; REEVES, Douglas. *Traceback and Anonymity*. Nova York: Springer, 2015.

WANG, Yongheng; ZHANG, Xiaoming (Ed.). *Internet of Things:* International Workshop, IOT 2012, Changsha, China, August. Nova York: Springer, 2012.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220,1890.

WEBER, Rolf H.; HEINRICH, Ulrike I. *Anonymization*. Berlin: Springer Science & Business Media, 2012.

WEBER, Rolf H.; WEBER, Romana. *Internet of Things.* Nova York: Springer, 2010.

WEINMAN, Joe. *Digital Disciplines:* Attaining Market Leadership via the Cloud, Big Data, Mobility, Social Media, and the Internet of Everything. Hoboken: John Wiley & Sons, 2015.

ZIEGELDORF, Jan; MORCHON, Oscar; WEHRLE, Klaus. Privacy in the Internet of Things: Threats and Challenges. Security Comm. *Networks*, v. 7, n. 12, 2014.

OS DIREITOS DE PRIVACIDADE NA INTERNET E A PROTEÇÃO DE DADOS PESSOAIS: UMA COMPREENSÃO CONCEITUAL PARA OS DIREITOS FUNDAMENTAIS

VINÍCIUS BORGES FORTES

INTRODUÇÃO

Quando a Internet ainda ensaiava os primeiros passos em território brasileiro, há pouco mais de uma década, Gilberto Gil, compositor brasileiro e defensor da liberdade dos direitos civis no ciberespaço, sobretudo como Ministro da Cultura, referenciou na música *Pela internet* uma das primeiras impressões do que a rede representava na vida dos usuários: "Eu quero entrar na rede, promover um debate, juntar via internet, um grupo de tietes de Connecticut, [...] Eu quero entrar na rede para contatar, os lares do Nepal e os bares do Gabão". (ROHTER, 2011).

No sentido apresentado por Gil, vive-se na era dos *websites* e a transcendência dos *gigabytes* nas "nuvens" com a *cloud computing*. Definitivamente, se vive em um tempo no qual a simultaneidade proporcionada pela Internet oportuniza a vivência de uma experiência revolucionária da comunicação, do relacionamento social e do consumo. Assim, inevitavelmente as relações estabelecidas no ambiente virtual também são submetidas à análise da ciência jurídica sob os prismas sociológico, hermenêutico, jurisdicional e do *modus operandi* que a tecnologia instiga a investigar.

O consumidor moderno, cada vez mais, procura a internet para realizar transações comerciais. Isso ocorre por diversos fatores, por exemplo, a otimização do tempo disponível, a tentativa de manutenção da privacidade, a amplitude na realização de pesquisas de preços. Figura-se uma geração de indivíduos sempre mais familiarizados com o ato de "googlear". A internet e, especialmente, o ato de "googlear" trouxeram repercussões das mais diversas para a vida individual e em sociedade, colocando em xeque diversos paradigmas da vida pós-moderna: o consumo, as relações sociais, a comunicação e a informação jamais serão as mesmas. (FORTES; BOFF, 2014).

A rede oferece novas e diferentes perspectivas e expectativas para o futuro. Há um tempo, quando se assistia a um filme de ficção científica, imaginava-se o futuro que estava por vir. Agora, tem-se a impressão de que se aproxima da certeza de que o futuro é agora. Nesse futuro presente, indubitavelmente, é necessário promover uma imersão conceitual do Direito na tecnologia da informação e comunicação, nas redes e no ciberespaço, visando preservar os direitos fundamentais à privacidade e à proteção de dados pessoais. (BOFF; DIAS, 2013).

A partir da revisão e análise bibliográfica, o texto ora apresentado tem como objetivo apresentar os fundamentos que constituem a base teórica dos direitos fundamentais, estabelecendo a conexão destes com a proteção da privacidade e a tutela dos dados pessoais na internet, especialmente a partir da abordagem do inovador conceito de direitos de privacidade na internet, a partir do seguinte problema de pesquisa: o reconhecimento expresso dos direitos de privacidade na internet no ordenamento jurídico brasileiro poderá fortalecer o direito fundamental à proteção da vida privada?

O DIREITO À PRIVACIDADE E À PROTEÇÃO DOS DADOS PESSOAIS COMO DIREITOS FUNDAMENTAIS

De modo emblemático, o artigo intitulado *The Right to Privacy*, de autoria de Warren e Brandeis, na *Harvard Law Review,* no ano de 1890, representou um marco para o debate jurídico sobre o tema da privacidade. No texto, os autores analisam o contexto das invenções recentes da época e os novos métodos de negócio para chamar a atenção, surgindo a necessidade de instrumentos jurídicos de proteção da pessoa, de modo a assegurar o que Cooley denominou, anos antes, "o direito de ser deixado em paz", ou originalmente "*the right to be let alone*" (WARREN; BRANDEIS, 1890, p. 1-10).

No contexto do artigo que se tornou um paradigma para o estudo jurídico da privacidade, as fotografias instantâneas publicadas pelas empresas jornalísticas invadiram a vida privada e familiar. Por isso, durante certo tempo houve a sensação de que o direito deveria oferecer alguma solução para a circulação não autorizada de fotografias privadas de pessoas. A intensidade e a complexidade da vida, que acompanham os avanços da civilização, provocaram a necessidade de certo distanciamento do mundo. Os indivíduos, influenciados pela cultura da época, viram-se mais vulneráveis à publicidade, de modo que a solidão e a intimidade se transformaram em algo essencial às pessoas. Para os referidos autores, os novos modos de difusão da informação e as novas tecnologias vinculadas a esses modos, ao invadirem a intimidade de outrem, produzem um sofrimento

espiritual e uma angústia que superam meros danos pessoais (WARREN; BRANDEIS, 1890, p. 1-10).

De acordo com Saldaña (2012), que analisou historicamente os fundamentos e o contexto que levaram à publicação do artigo de Warren e Brandeis (1890, p. 1-10), as possibilidades invasivas da tecnologia fizeram com que os autores manifestassem a necessidade de definir um princípio que pudesse ser invocado para amparar a intimidade do indivíduo frente à imprensa, ao fotógrafo ou a qualquer outro possuidor de um aparato de reprodução de imagens ou sons.

Assim, materializou-se o conceito por eles defendido de um direito à privacidade, originalmente denominado *the right to privacy*, o qual outorga a toda a pessoa plena disponibilidade para decidir em que medida podem ser comunicados a outros seus pensamentos, sentimentos e emoções. O que significa dizer, nesse contexto, que a finalidade do direito passa a ser a de garantir àquelas pessoas cujos assuntos não são causa de preocupação legítima para a parcela da sociedade que não se vê conduzida por uma publicidade indesejável e indesejada, bem como proteger essas pessoas, seja quem elas forem, independente de *status* ou posição social, de verem divulgados, contra sua vontade, assuntos prefeririam manter absolutamente reservados (WARREN; BRANDEIS, 1890, p. 1-10).

Nessa perspectiva, com o objetivo de configurar com autonomia própria o direito à privacidade, Warren e Brandeis diferenciaram-no do genérico direito à liberdade e do clássico direito burguês à propriedade. Com efeito, os autores afirmam que o direito à liberdade assegura extensivos privilégios civis, mas não outorga proteção frente à ofensa aos sentimentos pela invasão da esfera privada. De outra banda, o direito à propriedade garante apenas a posse, tangível ou intangível, mas não assegura a tranquilidade de espírito que proporciona impedir a publicação de aspectos reservados da pessoa (SALDAÑA, 2012).

O direito à privacidade, contudo, garante a proteção aos âmbitos mais imateriais, aos interesses espirituais da pessoa, configurando-se como um direito autônomo que adquire substantividade própria. Por essa razão, Warren e Brandeis fundamentaram diretamente o denominado *right to privacy* no direito de desfrutar a vida, rechaçando expressamente qualquer conexão ou associação com os direitos de liberdade ou propriedade. Eles situaram o direito à privacidade em uma categoria geral do direito individual de ser deixado em paz ou de, simplesmente, não ser incomodado – *right to be let alone* (SALDAÑA, 2012, p. 195-240).

No caso em que originou a reflexão sobre o direito à privacidade, a *common law* assegurava a cada pessoa o direito de dizer até que ponto podem ser comunicados a outrem seus pensamentos, sentimentos e emoções.

Dentro desse sistema, nunca se pode forçar alguém a expressá-los – exceto na condição de testemunha – e, ainda que decida expressá-los, o sujeito tem, por regra geral, o poder de fixar os limites da publicidade. Assim, a existência desse direito não depende do meio de difusão da informação utilizado. Não importa se for por meio de palavras ou códigos, por pintura, escultura ou música. A existência desse direito não depende tampouco da natureza do valor do pensamento, nem da qualidade dos meios empregados para sua expressão. Em qualquer desses casos, o autor é quem tem o direito de decidir se o que é seu deve sair à "luz pública" (WARREN; BRANDEIS, 1890, p. 1-10).

Em continuidade à percepção conceitual do direito à privacidade concebido por Warren e Brandeis, Tapper (1973) diz que, em um mundo no qual a reprodução das espécies não é realizada espontaneamente e a sobrevivência depende da cooperação dos outros, não é possível ocorrer a exclusão de um indivíduo da vida do outro. Nesse contexto, os outros têm olhos, ouvidos e língua, são curiosos e adoram fofocar. Verifica-se, pois, que a privacidade existe naturalmente nas mais primitivas comunidades, ainda que, por vezes, expressa na forma de rituais. No contexto vivenciado na década de 1970, a privacidade possuía facetas do desejo por isolamento, anonimato e pelo direito de controle da disseminação de informações sobre si mesmo, representando uma criação advinda essencialmente da civilização urbana.

Em uma perspectiva historicamente mais recente, Tapper identifica duas maneiras de violação de privacidade. A primeira consiste na coleta de informações pessoais e a segunda concentra-se em seu uso. O primeiro modo de violação da privacidade pode ser realizado de dois modos: ilícito, quando, clandestinamente, alguém coleta informações pessoais, a fim de descobrir aquelas que ainda não se tornaram públicas; lícito, quando voluntariamente um indivíduo fornece informações pessoais para uma finalidade e, sem seu consentimento, tais informações são disponibilizadas para finalidade diversa. No contexto pautado pela construção de bancos de dados informatizados, os dois modos de violação do direito à privacidade adquirem relevância e devem ser considerados sob o olhar do direito (TAPPER, 1973).

De modo diverso à concepção de que a privacidade representa apenas o direito de ser deixado em paz ou de não ser incomodado, Warner e Stone (1970) defendem ser essa uma concepção paradoxal, pois privacidade também significa o direito de se comunicar, assegurando-se, contudo, de que as informações geradas não serão utilizadas contra o indivíduo que as produziu.

A temática da privacidade passou a ser vista como um problema, a partir da década de 1960 entre a década de 1970, quando as pessoas passaram a reclamar da violação do direito à privacidade, requerendo que tal violação fosse examinada. De acordo com citados os autores, quando os psicólogos afirmam que os seres humanos precisam reter coisas de certas pessoas, em determinadas épocas, é necessário olhar para os mecanismos de defesa gerados em reação. Quando o peso da opinião pública oscila para uma visão em que algumas violações são intoleráveis, a definição de privacidade torna-se um pré-requisito essencial para a legislação sobre o tema (WARNER; STONE, 1970).

Assim, a privacidade passou a ser considerada uma "virtude extremamente escorregadia", intangível, sobre a qual é difícil estabelecer uma definição e eventuais mensurações. Significa dizer que um "direito à privacidade" não é e não pode ser um estatuto imutável. Para diferentes pessoas possui sentidos diferentes em espaços de tempo diversos e está diretamente ligado com o que se compreende por anonimato (WARNER; STONE, 1970).

Em contraponto à construção proposta por Warren e Brandeis (1890, p. 1-10) sobre a efetivação do direito à privacidade, Warner e Stone (1970) defendem que, à época da publicação ora referenciada, o direito não conferia um "direito de privacidade", nem no Reino Unido, nem na maior parte dos Estados norte-americanos. Isso porque esse direito está assegurado apenas em relação à proteção legal de reputações e propriedades, não garantindo proteção à dor emocional trazida com a invasão da privacidade de outrem.

Ainda assim é possível afirmar que a privacidade encontra reconhecimento como direito humano e, portanto, como direito fundamental, sobretudo ao manto dos fundamentos apresentados por Warren e Brandeis (1890, p. 1-10) e Warner e Stone (1970).

O primeiro documento internacional a recepcionar o direito à privacidade foi a Declaração Americana dos Direitos do Homem, explicitando, no artigo V, que "Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar". Na sequência, a Declaração Universal dos Direitos Humanos, legitimada por seus signatários, no ano de 1948, expressa, no artigo 12, que "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques"[1] (ASSEMBLEIA, 1948).

1 ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. The Universal Declaration of Human Rights. Disponível em: <http://www.un.org/en/documents/udhr/index.shtml>. Acesso em: 14 mar. 2015.

Ainda no sentido de reconhecer o direito à proteção da vida privada como um direito humano, a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, aprovada em Roma, no ano de 1950, apresenta, em seu artigo 8º, intitulado *Direito ao respeito pela vida privada e familiar*.

Observe-se que o disposto na Declaração Universal dos Direitos Humanos não apresenta qualquer hipótese de exceção ao direito de proteção da vida privada, ao contrário da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Esta, em seu parágrafo segundo, justifica a ingerência de autoridades públicas sobre o exercício desse direito, em casos específicos que se vinculam à proteção da democracia, da segurança pública ou da segurança nacional. Fica evidente, no dispositivo da convenção europeia, o reflexo do recente processo de paz, pós II Guerra Mundial, a qual conturbou o continente europeu poucos anos antes da edição dessa convenção, o que é compreensível, em que pese não seja absolutamente aceitável sob o prisma das sociedades democráticas da contemporaneidade.

Em um sentido desapegado de regimes de exceção, o artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos, aprovado, no ano de 1966, pela Assembleia Geral das Nações Unidas e recepcionado, em 1992, pelo Brasil, que o convalidou por meio do Decreto n.º 592.[2] (BRASIL, 1966)

Na visão de Warner e Stone (1970), a International Comission of Jurists' Nordic Conference's on the Right to Privacy, conferência internacional de juristas, realizada no ano de 1967, definiu dez importantes diretrizes para delimitar o direito individual à privacidade como a proteção contra: a interferência na vida privada, familiar e doméstica; a interferência na integridade física ou mental, ou sobre a liberdade moral ou intelectual; os ataques contra a honra ou reputação; situações de *false light* – que correspondem aos atos ilícitos contra a honra do indivíduo, afetando não apenas a reputação, mas causando danos aos sentimentos e à dignidade da vítima –; a divulgação de fatos irrelevantes ou embaraçosos, relatando a vida privada de alguém; o uso do nome, da identidade ou qualquer outra semelhança de outrem; a prática de espionagem, curiosidade, observação ou assédio sobre a vida alheia; a interferência sobre a correspondência; o tratamento inadequado de correspondência escrita ou verbal; e a divulgação de informações fornecidas ou recebidas de alguém em circunstâncias de sigilo profissional.

2 BRASIL. Decreto n.o 592/1966. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm>. Acesso em: 14 jan. 2015.

Ao tratar dos fundamentos históricos da proteção jurídica dos dados pessoais, é relevante observar sua gênese. Contudo, convém ressaltar o entendimento de Rodotà (2008) de que, hodiernamente, vivencia-se uma reinvenção conceitual da proteção de dados, não apenas pelo reconhecimento expresso como direito fundamental autônomo, mas pelo papel indispensável para o desenvolvimento da personalidade. Assim, "[…] A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio" (RODOTÀ, 2008, p. 17).

É com base nesses fundamentos que Rodotà (2008, p. 19) afirma que a proteção de dados não é apenas um direito fundamental, mas o mais significativo da humanidade na contemporaneidade. Em sentido análogo, Doneda [s.d.] refere que o tema da privacidade adota, cada vez mais, uma estrutura em torno da informação e, de modo específico, dos dados pessoais, o que pode ser observado na evolução normativa relacionada ao tema. Em que pese existirem diferenças conceituais, a proteção jurídica do direito à privacidade conecta-se com o direito à inviolabilidade dos dados pessoais, previsto em diversos diplomas legais, inclusive com o reconhecimento, como direito fundamental, conforme aprofundado ao longo deste texto.

Diante dessas considerações, que compreendem que a internet instituiu um espaço ocupado por pessoas, empresas e governos, e dentro do qual os direitos fundamentais tem um relevante a desempenhar. Assim, passou-se a questionar o modo como o Direito deverá estar comprometido com a transição paradigmática da sociedade industrial para a sociedade da informação, especialmente como o Direito poderia sistematizar o desenvolvimento de novos campos de pesquisa e investigação que relacionassem os direitos fundamentais, a sociedade e as tecnologias da informação e comunicação.

Evidentemente, o aumento considerável da presença de computadores e do acesso à internet nos domicílios possibilita o potencial aumento do número de indivíduos sujeitos a transgressões de direitos na internet, especialmente do direito fundamental à privacidade através da violação dos dados pessoais. Além dos riscos relacionados à mineração de dados por empresas privadas, especializadas na coleta de dados privados para fins comerciais, os usuários de serviços de internet e telefonia móvel estiveram – e possivelmente estejam e ainda estarão no futuro – sujeitos a práticas de vigilância em massa pelo governo dos EUA, pelos programas da NSA (GREENWALD; KAZ; CASADO, 2013).

De modo complementar às reações institucionais globais já referidas nesse texto, a partir da Resolução n.º 69/166, de 18 de dezembro de 2014, emitida pela Assembleia Geral das Nações Unidas, em especial após propostas apresentadas pelo Brasil em conjunto com a Alemanha, foi aprovada,

no mês de março do ano 2015, a constituição de uma relatoria especial do Conselho de Direitos Humanos para acompanhamento das questões relacionadas às violações ao direito humano à privacidade em âmbito global[3] (ASSEMBLEIA, 2014).

Salienta a mencionada Resolução da Assembleia Geral da ONU o reconhecimento da discussão e análise dos assuntos vinculados à promoção e proteção do direito à privacidade e a outros direitos humanos na era digital, à luz do direito internacional dos direitos humanos, além de avaliar o impacto dos atos de vigilância em massa. A Resolução registra que a internet é uma tecnologia de natureza global e aberta, a qual, associada ao ritmo acelerado de desenvolvimento de tecnologias da informação e comunicação, amplia consideravelmente a capacidade de governos, organizações empresariais e indivíduos realizarem vigilância, interceptação e coleta de dados, tendo como consequência direta a ocorrência de abusos de direitos humanos, em especial do direito à privacidade, protegido pelo artigo 12 da Declaração Universal dos Direitos Humanos[4] e pelo artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos[5] (CONSELHO, 2015).

A Resolução pondera que, diante da ampla possibilidade da utilização de metadados como forma de revelar informações pessoais, tais como comportamento individual, relações sociais, preferências privadas e identidade do usuário de internet, tratar da proteção da privacidade como direito humano é imprescindível. Outro ponto de relevância da Resolução diz respeito à preocupação da comunidade internacional com o impacto negativo gerado pelas denúncias públicas dos atos de vigilância e/ou interceptação de comunicações, inclusive extraterritoriais, bem como da coleta de dados

---

3 ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. Resolution adopted by the General Assembly on 18 December 2014 - 69/166. The right to privacy in the digital age. [S.l: s.n.].

4 Artigo 12.º - Ninguém deverá ser submetido a interferências arbitrárias na sua vida privada, família, domicílio ou correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques todas as pessoas têm o direito à proteção da lei (ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, 1948).

5 Artigo 17 - 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

pessoais em grande escala, o que reforça a constatação do desrespeito ao direito humano à proteção da privacidade e à garantia da inviolabilidade dos dados pessoais[6] (CONSELHO, 2015).

Nesse contexto, o conceito de "direitos de privacidade na internet" poderá contribuir com a normatização do tema da privacidade e da proteção de dados pessoais na internet, principalmente frente à iminente regulamentação do Marco Civil da Internet e do avanço na discussão do anteprojeto de lei de proteção dos dados pessoais no Brasil.

A TUTELA DOS DADOS PESSOAIS A PARTIR DA PROTEÇÃO DOS "DIREITOS DE PRIVACIDADE NA INTERNET" COMO DIREITOS FUNDAMENTAIS

Convém esclarecer, desde já, que essa pesquisa filia-se à categoria de direitos construída por Bernal (2014), que consiste não apenas ao reconhecimento do direito à privacidade na internet, mas na definição de um conjunto de "direitos de privacidade na internet".

A relação existente entre a proteção jurídica da privacidade e dos dados pessoais e a sociedade em rede é absolutamente próxima, visto que a internet oferece ampla gama de oportunidades de coleta, análise, uso e armazenamento de dados pessoais, que são revertidos para múltiplas finalidades. Nesse ponto, o modelo sugerido pela *web* simbiótica tem forte influência sobre a geração dessas oportunidades de coleta, análise, uso e armazenamento de dados e informações pessoais.

Torna-se incrivelmente difícil, nos dias atuais, separar dados e informações *on-line* e *off-line*. Desde que a internet se tornou mais integrada com o "mundo real", dados *on-line* e *off-line* se misturam facilmente. Um típico exemplo de que alguns dados gerados no "mundo real" são aproveitados dentro do ciberespaço pode ser observado no caso da rede britânica de supermercados Tesco. A partir do Tesco Clubcard, um programa de fidelidade criado pela rede, é possível coletar dados de compras realizadas no "mundo real" que são mapeados e cruzados com compras realizadas na internet (BERNAL, 2014).

---

6 CONSELHO DE DIREITOS HUMANOS DAS NAÇÕES UNIDAS. Criação da Relatoria Especial sobre "O Direito à Privacidade na Era Digital". Disponível em: <http://www.itamaraty.gov.br/index.php?option=com_content&view=article&id=8460:criacao-da-relatoria-especial-sobre-o-direito-a-privacidade-na-era-digital&catid=42&Itemid=-280&lang=pt-BR>. Acesso em: 31 mar. 2015.

Desta forma, a rede passou a armazenar detalhes de cada consumidor no Reino Unido, desde o domicílio até uma gama de características demográficas, socioeconômicas e de estilo de vida. Por meio de um sistema de inteligência artificial, denominado Zodiac, foi possível criar perfis inteligentes e de segmentação dos dados dos clientes. Assim o perfil do cliente pode ser classificado conforme seu entusiasmo por promoções, sua fidelidade às marcas e outros hábitos de compra (LEITH, 2009).

Não bastasse isso, a companhia passou a vender o acesso à base de dados denominada Crucible a empresas de diferentes segmentos, como a Sky – televisão por assinatura –, Gillette – barbeadores e produtos cosméticos – e Orange – provedora de televisão e internet por assinatura. Juntos, a base de dados Crucible e o sistema Zodiac podem gerar um mapa de como um indivíduo pensa, trabalha e quais lojas frequenta. Ademais, o mapa é capaz de classificar os consumidores em dez categorias: riqueza; promoções; viagens; caridade; consumo "verde"; dificuldades financeiras; crédito; estilo de vida; hábitos; aventuras (THE GUARDIAN, 2015).

Outro exemplo de que há cruzamento de informações entre ambientes *on-line* e *off-line* foi apresentado em um estudo intitulado *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata,* que demonstrou o desenvolvimento de um algoritmo matemático que, instalado dentro do sistema informacional de uma instituição financeira, foi capaz de coletar metadados anônimos, armazenados sob sigilo, obtidos a partir de compras realizadas com cartões de crédito, em estabelecimentos comerciais. De acordo com os resultados da pesquisa, foi possível identificar um consumidor pela coleta de dados de, em média, quatro operações financeiras com cartão de crédito (DE MONTJOYE, 2015).

Destarte, metadados anônimos e até mesmo protegidos por normas de sigilo bancário, tal como prevê a lei brasileira, tornam-se dados pessoais vulneráveis, eis que passíveis de identificação da pessoa em questão, ainda que sujeitos às proteções legais, especialmente as relacionadas com a tutela constitucional e civilista da vida privada. Abrem-se, com isso, diversas possibilidades de registro e tratamento dos dados, inclusive de maneira ilícita, por governos, empresas e indivíduos. Apesar da tutela constitucional e infraconstitucional mencionada, acredita-se na necessidade de melhor compreensão da internet no âmbito jurídico, de modo a conferir maior eficácia à proteção dos direitos fundamentais.

Conforme evidenciado, a internet introduziu novos níveis de vulnerabilidade a novas formas de coleta dos dados pessoais, os quais antes eram coletados, "roubados" ou obtidos de outras formas, adequada ou inadequadamente: eles agora podem se perder pelo mundo para as mais

diversas finalidades. É, pois, fundamental aproximar o estudo dos direitos fundamentais às transgressões, cada vez mais frequentes, desses direitos na internet, sobretudo em relação à proteção da privacidade e dos dados pessoais.

Nesse prisma, este texto defende a necessidade do reconhecimento de direitos-base para a efetiva proteção jurídica da privacidade e dos dados pessoais na internet, em especial na incorporação do conceito de "direitos de privacidade na internet" como um dos pilares para a regulamentação da proteção dos dados pessoais no Brasil, buscando, assim, maior eficácia do direito fundamental à privacidade. Todavia, para que seja possível pontuar, de maneira propositiva, é relevante observar quais os direitos-base identificados pela doutrina, para que os ajustes contextuais ao direito brasileiro sejam realizados de maneira adequada.

Nesse intuito, são apresentados quatro direitos-base os quais transcendem a acepção de direitos legais, já que representam desejos reais compreendidos e considerados pelas pessoas como um direito seu, sobretudo a partir da proteção da autonomia de cada indivíduo. Nesse mister, são considerados os quatro direitos-base que constituem os direitos de privacidade na internet ou, como denominados originalmente, Internet Privacy Rights, o direito de navegar pela internet com privacidade; o direito de monitorar quem monitora; o direito de deletar os dados pessoais; o direito a uma identidade *on-line* (2014).

O primeiro direito, vincula-se à possibilidade de navegação por páginas da internet – seja na busca de informações, seja na busca de dados, seja na compra de produtos em plataformas de comércio eletrônico – com a expectativa razoável de fazê-lo com privacidade, não como um padrão absoluto, mas como uma regra geral (2014).

Evidentemente, sugerir isso significa colocar em xeque todos os modelos de negócio que se utilizam integralmente da internet para interagir com os usuários – serviços *web-based*, portanto –, e que estão absolutamente fundamentados na *web* simbiótica. A maior parte dos motores de busca, como o Google, foram desenvolvidos para trabalhar em simbiose com os usuários, ou seja, em troca de serviços gratuitos, o usuário fornece seus dados pessoais e consente, ao iniciar o uso dos serviços, que suas informações pessoais de navegação sejam coletadas, armazenadas e utilizadas para diversos fins, inclusive comerciais.

Todavia, o direito de navegar pela internet com privacidade deveria se estender para além dos motores de busca, alcançando também qualquer outro serviço de navegação, como os provedores de acesso – originalmente denominados Internet Service Providers (ISPs). O reconhecimento

formal do direito de navegar pela internet com privacidade poderia gerar conflitos inevitáveis com práticas governamentais, especialmente com as de vigilância, *surveillance* (MORAIS; NETO, 2014) e retenção de dados. Todavia, essa inevitável tensão é fundamental, de modo que o argumento da segurança nacional ultrapasse, automaticamente e sempre, os fundamentos da proteção da privacidade (MORAIS; NETO, 2014).

Logo, o reconhecimento do direito à navegar na internet com privacidade não significa uma "carta branca" para operar sem equilíbrio, sem a devida *accountability* ou sem as devidas consequências para cada ato cometido na rede (BERNAL, 2014), o que conecta com o segundo direito-base que compõe o núcleo dos "direitos de privacidade na internet".

O segundo direito, complementar ao anterior, diz respeito ao direito de saber quem monitora, o quê monitora, quando monitora e para quais fins o faz. Assim como há circunstâncias vinculadas ao direito de ter uma navegação com privacidade, há situações em que os indivíduos desejam ser monitorados, por alguma razão benéfica. Sob a ótica da proteção da privacidade, a coleta de dados e o monitoramento constantes são atos absolutamente negativos. Entretanto, sob o prisma da *web* simbiótica, são atos absolutamente benéficos à usabilidade da rede pelo usuário (2014).

Diante desse impasse conceitual e antagônico, os usuários têm o direito de saber quando, por quem, para que e o quê está sendo precisamente rastreado, registrado, armazenado e analisado. Monitorar os monitores significa mais do que o simples conhecimento de quais dados estão sendo coletados. Trata-se de o indivíduo saber se está sendo monitorado, eventualmente até sem retenção de dados e informações, e para qual finalidade tal ato se destina. Trata-se de estabelecer um princípio de consentimento colaborativo, com o consentimento considerado de modo imediato, interativo, dinâmico e binário, dentro dos processos de interação na internet (BERNAL, 2014).

O terceiro direito, o de deletar os dados pessoais, merece aqui diferenciações importantes. Anteriormente, essa pesquisa trouxe a lume a expressão *right to be let alone*, empregada por Cooley e reproduzida por Warren e Brandeis, para configurar o direito de ser deixado em paz, conferindo o início do reconhecimento do direito à privacidade (BERNAL, 2014).

Todavia, tal expressão é frequentemente entendida como sinônimo de um direito já reconhecido, inclusive no direito brasileiro, qual seja o direito ao esquecimento. Entretanto, o direito ao esquecimento, tal como se aborda nesse tópico, está adequado à conceituação utilizada por Bernal (2014), ou seja, ao denominado *right to be forgotten*, visto que vai além da simples proteção da vida privada, conferindo a possibilidade de um usuário deletar dados e informações pessoais da internet.

Um exemplo dessa confusão conceitual pode ser observado em Rulli Júnior e Rulli Neto (2012), que explicam que o direito ao esquecimento é denominado, no direito norte-americano, *the right to be let alone*. Ele significa a garantia de que os dados sobre um indivíduo somente serão conservados para possibilitar a identificação de um sujeito conectado aos acontecimentos e apenas pelo tempo necessário ao alcance de suas finalidades. O direito aqui tratado, o do esquecimento, corresponde ao *right to be forgotten*.

A discussão sobre a possibilidade de ter "um" direito ao esquecimento é antiga. Ela advém do conflito de indivíduos com a imprensa e com a mídia, em publicações não autorizadas ou cujo conteúdo não corresponderia à integralidade dos fatos e à verdade. Há alguns anos, a preocupação residia na retirada de circulação de revistas e jornais das prateleiras das bancas, para que a informação supostamente equivocada não circulasse entre os leitores, evitando-se, com isso, a deflagração de supostas inverdades. Nesse contexto, a questão vinculava-se mais ao conceito de *right to be let alone*.

Todavia, em tempos de internet e com a consolidação do ciberespaço, mostra-se inevitável o debate sobre a possibilidade de se instituir um "botão *delete*", capaz de excluir dos registros da *web* informações não desejadas por algum dos sujeitos envolvidos.

A questão da aplicação de "um" direito ao esquecimento foi submetida à análise do Tribunal de Justiça da União Europeia, demandado pelo judiciário espanhol. A partir de uma ação judicial movida pelo advogado espanhol Mario Costeja contra a Google, com o objetivo de deletar um artigo do jornal *La Vanguardia*, datado de 1998, o qual fazia referência a um leilão de imóveis e a uma penhora por dívidas com a previdência social. Nessa circunstância, o advogado-geral da União Europeia manifestou-se, em parecer, pela não aplicação do direito ao esquecimento em casos dessa natureza.

Assim, de acordo com o advogado-geral da União Europeia, os motores de busca, no caso o Google, não devem ser responsabilizados pelo tratamento das páginas indexadas, logo não podem ser responsabilizados pelas buscas e, portanto, não podem ser obrigados a excluir determinados resultados de busca. Além disso, a determinação do Poder Judiciário direcionada ao motor de busca para o bloqueio de *sites* significaria a autorização judicial da censura, eis que interferiria na liberdade de expressão no ciberespaço. Ainda, a Diretiva 95/46/CE, que regulamentou o tratamento dos dados pessoais na União Europeia, possibilita a exclusão de informações inverídicas, incorretas ou incompletas. Todavia, para as informações verdadeiras, não há que se falar em "esquecimento" (JÄÄSKINEN, 2013).

Devido a esse tipo de demanda, a Google constituiu o que denominou Conselho Consultivo do Google para o Direito de ser Esquecido, formado por *experts* no tema. Após uma agenda de trabalho que contemplou reuniões e audiências com partes interessadas, o Conselho Consultivo emitiu, no dia 6 de fevereiro de 2015, um relatório de 44 páginas, com recomendações sobre o que a empresa de tecnologia da informação e comunicação pode fazer nos casos de requisição do direito ao esquecimento (GOOGLE, 2015).

Nesse ponto, é relevante refletir sobre os limites que uma organização empresarial como a Google, que é detentora de uma parte significativa das informações organizadas dentro da internet, de definir categorias de grupos para os quais deve ser aplicável, e sob quais circunstâncias e condições, o direito de deletar dados pessoais deverá ocorrer. A simples possibilidade de determinar ditas categorias já aponta uma fragilidade sobre as normas jurídicas que tutelam, implicitamente, o direito ao esquecimento.

Na sequência de categorização apresentada pelos *experts* da Google, foram elencados os tipos de informação, bem como a natureza desta, para efeitos de observação sob o viés do interesse público. Todavia, os tipos de informação apresentados podem colidir com o que se compreende normativamente como 'dados sensíveis', dos podem colidir com o que se compreende como 'íveis', que podem revelar informações pessoais como "[…] a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos".[7] Nessa lógica, conforme pode-se observar no quadro abaixo, muitas das informações categorizadas dentro da natureza de interesse público, com baixa possibilidade de exclusão dos registros de internet dentro dos critérios da Google, podem violar a proteção dos dados pessoais, especificamente dos dados sensíveis (BRASIL, 2015).

De forma complementar aos anteriores, o quarto direito divide-se em três frentes: um direito a criar uma identidade *on-line*; um direito de afirmar essa identidade *on-line;* um direito de proteger essa identidade *on-line*. De acordo com o autor, a relação entre privacidade, identidade e autonomia é complexa, sutil e sempre em evolução, sobretudo pelo fato de as relações estabelecidas na internet exigirem, de uma forma ou de outra, uma identidade para ser usada, seja nas redes sociais, no acesso a serviços de banco *on-line*, seja como um nome de usuário para jogar *on-line* (BERNAL, 2014).

7 BRASIL. Anteprojeto de Lei para a Proteção de Dados Pessoais. Disponível em: <http://participacao.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 28 abr. 2015.

O quanto a identidade revela sobre o "indivíduo real" por trás do "indivíduo virtual" é uma questão adstrita exclusivamente ao direito desse indivíduo em determinar as ditas informações "reais". Em alguns lugares e em algumas situações, a conexão entre as identidades "real" e "virtual" precisa se mostrar clara e explícita, mas essas situações são muito mais raras do que os negócios em operação nessa sistemática geralmente sugerem. Em outras palavras, a internet que adota como regra padrão uma política de "nomes reais" é a mesma em que a privacidade e a autonomia das pessoas são desnecessariamente comprometidas. Assim, uma mudança de paradigma, relevante na visão de autor, reside justamente na inversão da regra, sendo a exigência de identidades reais a exceção (BERNAL, 2014).

A quantidade de informações que um usuário de internet precisa revelar para acessar um serviço ou um sistema deveria, em geral, ser minimizada. A ideia de divulgação minimizada – e nisso se inclui a divulgação da identidade *on-line* como um conjunto de informações pessoais – associa-se à concepção de minimização dos dados, o que configura um aspecto-chave para um regime de proteção de dados e uma parte crucial para a privacidade dos dados na internet. Logo, a privacidade na internet está primariamente relacionada com a proteção de identidades, enquanto a autonomia relaciona-se com o controle dessas identidades por seus titulares.

CONCLUSÃO

Conceber a privacidade na internet como um direito fundamental, em sentido amplo, capaz de recepcionar em seu bojo a proteção da vida privada, da intimidade, da imagem, da honra e dos direitos-base vinculados ao conceito de direitos de privacidade na internet, significa dizer que, na contemporaneidade, o direito de navegar na internet com privacidade, o direito de monitorar quem monitora, o direito de deletar dados pessoais e o direito de proteger a identidade *on-line* devem ser tutelados, explícita e expressamente, como um dos pilares de garantia da eficácia do direito fundamental à privacidade em sentido amplo.

Assim, a recepção expressa dos direitos de privacidade na internet pelas normas jurídicas, que tratam e ainda tratarão de temas afins no Brasil, permite a recomposição do núcleo do direito fundamental à privacidade que, de acordo com as teorias apresentadas nesta pesquisa, integram tão somente a proteção da vida privada, da honra, da intimidade e da imagem. Em outras palavras, ressalta-se que o direito fundamental à privacidade deve também integrar à sua estrutura nuclear os direitos de privacidade na internet, de modo que, no Brasil, a regulamentação do Marco Civil da

Internet e a edição de uma lei de proteção de dados pessoais contemplem expressamente o direito de navegar na internet com privacidade; o direito de monitorar quem monitora; o direito de deletar os dados pessoais; o direito à proteção da identidade *on-line*.

Destarte, o direito fundamental à privacidade na internet passa a ter dimensão mais ampla e, sobretudo, atual e contextualizada com a sociedade da informação, permitindo melhor encaixe do Direito sobre os novos modos de interação social que a internet apresenta de forma recorrente, bem como torna viável o enfrentamento das problemáticas de natureza jurídica, decorrentes de uma sociedade em rede ou de um "Estado de Vigilância".

Estabeleceu-se, portanto, um elo teórico-conceitual para determinar que os direitos de privacidade na internet devem estar expressos e explícitos, para assegurar maior amplitude na eficácia das normas jurídicas brasileiras que tutelam o direto fundamental à privacidade no contexto da internet, respondendo ao problema de pesquisa proposto nesse texto.

REFERÊNCIAS

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. Resolution adopted by the General Assembly on 18 December 2014 - 69/166. The right to privacy in the digital age. [S.l: s.n.].

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. The Universal Declaration of Human Rights. Disponível em: <http://www.un.org/en/documents/udhr/index.shtml>. Acesso em: 14 mar. 2015.

BERNAL, P. *Internet Privacy Rights:* Rights to Protect Autonomy. Cambridge (UK): Cambridge University Press, 2014.

BRASIL. Anteprojeto de Lei para a Proteção de Dados Pessoais. Disponível em: <http://participacao.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 28 abr. 2015.

BRASIL. Decreto n.o 592/1966. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm>. Acesso em: 14 jan. 2015.

BOFF, S.; DIAS, F. da. O tratamento jurisdicional das liberdades comunicativas na sociedade da informação no brasil. *Boletín Mexicano de Derecho Comparado*, v. 46, n. 137, p. 573-599, maio 2013. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0041863313711438>. Acesso em: 14 maio 2015.

CONSELHO DE DIREITOS HUMANOS DAS NAÇÕES UNIDAS. Criação da Relatoria Especial sobre "O Direito à Privacidade na Era Digital". Disponível em: <http://www.itamaraty.gov.br/index.php?option=com_content&view=article&id=8460:criacao-da-relatoria-especial-sobre-o-direito-a-privacidade-na-era-digital&catid=42&Itemid=-280&lang=pt-BR>. Acesso em: 31 mar. 2015.

DE MONTJOYE, Y.-A.; RADAELLI, L.; SINGH, V. K.; PENTLAND, A. S. Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. *Science*, v. 347, n. 6221, p. 536-539, 29 jan. 2015. Disponível em: <http://www.sciencemag.org/content/347/6221/536>. Acesso em: 30 jan. 2015.

DONEDA, D. *Da privacidade à proteção de dados pessoais*. [S.l: s.n.: s.d.].

FORTES, V. B.; BOFF, S. O. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. *Seqüência: estudos jurídicos e políticos*, v. 35, n. 68, p. 109-127, jun. 2014. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109>. Acesso em: 14 maio 2015.

GOOGLE. *Report of The Advisory Council to Google on the Right to be Forgotten Members of the Council*. [S.l.: s.n.: s.d.]. Disponível em: <https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view>. Acesso em: 12 set. 2017.

GREENWALD, G.; KAZ, R.; CASADO, J. EUA espionaram milhões de e-mails e ligações de brasileiros. O Globo, 6 jul. 2013. Disponível em: <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934#ixzz2q7eRkKbW>. Acesso em: 3 jan. 2015.

JÄÄSKINEN, N. Conclusões do advogado-geral apresentadas em 25 de junho de 2013 - Processo C-131/12 - Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos, Mario Costeja González. [S.l.: s.n.: s.d.].

JÚNIOR, A. R.; NETO, A. R. Direito ao Esquecimento e o Superinformacionismo – Apontamentos no Direito Brasileiro dentro do Contexto de Sociedade da Informação. *Revista do Instituto do Direito Brasileiro*, v. 1, n. 2012, p. 419-434, 2012. Disponível em: <http://www.idb-fdul.com/uploaded/files/RIDB_001_0419_0434.pdf>. Acesso em: 12 set. de 2017

LEITH, P. Privacy as slogan. In: SAARENPÄÄ, A. (Ed.). *Legal privacy.* Zaragoza: Prensas de la Universidad de Zaragoza, 2009. p. 93–112.

MORAIS, J. L. B.; NETO, E. J. A insuficiência do Marco Civil da Internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. In: LEITE, G.; LEMOS, R. (Ed.). *Marco Civil da Internet.* São Paulo: Atlas, 2014. p. 417-439.

RODOTÀ, S. *A vida na sociedade da vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 17.

ROHTER, L. Gilberto Gil Hears the Future, Some Rights Reserved. New York Times. Disponível em: <http://www.nytimes.com/2007/03/11/arts/music/11roht.html?pagewanted=all&_r=1&>. Acesso em: 29 ago. 2011.

SALDAÑA, M. N. "The right to privacy". La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. *Revista de Derecho Político*, n. 85, p. 195-240, 2012.

THE GUARDIAN. Tesco stocks up on inside knowledge of shoppers' lives. The Guardian, 20 set. 2005. Disponível em: <http://www.theguardian.com/business/2005/sep/20/freedomofinformation.supermarkets>. Acesso em: 8 fev. 2015.

WARNER, M.; STONE, M. G. *The data bank society:* organizations, computers and social freedom. [S.l.]: Allen & Unwin, 1970.

TAPPER, C. *Computers and the law.* [S.l.]: Weidenfeld & Nicolson, 1973.

WARREN, S. D.; BRANDEIS, L. D. The Right to Privacy. *Harvard Law Review VO - 4*, n. 5, p. 193, 1890. Disponível em: <http://roble.unizar.es:9090/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsjsr&AN=edsjsr.10.2307.1321160&lang=es&site=eds-live>. Acesso em: 12 set. 2017

INTERNET DAS COISAS E INOVAÇÃO NA AMÉRICA LATINA[1]

OLGA CAVALLI
FEDERICO MEINERS

INTRODUÇÃO

A Internet das Coisas é baseada em tecnologias conhecidas, mas o seu potencial de transformação será grande. A nova onda de conectividade e *software* de desenvolvimento será centrada em objetos cotidianos, que, de algum modo, podem ser controlados ou ligados à Internet. O que hoje é chamado de Internet das Coisas – Internet of Things (IoT) – é um conjunto de tecnologias e protocolos associados que permitem que objetos se conectem a uma rede de comunicações e são identificados e controlados através desta conexão de rede.

Diferentes tipos de sensores são integrados com os objetos para fornecer informações de diversos parâmetros que podem ser medidos. Isso permite a criação de ambientes que podem analisar e diagnosticar situações, minimizando erros. Qualquer objeto pode ser conectado à Internet usando etiquetas Radio Frequency Identification (RFID), que são adicionadas ao objeto para coletar informações. Numa comunicação de rádio frequência, a informação é enviada para um computador que está ligado à Internet.

O desenvolvimento de redes Wi-Fi, LTE e 4G-5G é relevante, mas haverá uma evolução no sentido de conectividade entre os objetos. A Internet das Coisas requer uma compreensão da conectividade entre os dispositivos e o desenvolvimento de normas para a transmissão de informações e ferramentas que permitem o comportamento autônomo de objetos de acordo com as funções a serem cumpridas e as instruções recebidas da rede que os interliga. O Transporte e a Logística há muito incorporaram essas tecnologias, em particular para melhorar a prestação de serviços.

1 Assistente de pesquisa: Bibiana Rivadeneira

Há uma série de definições e previsões sobre a Internet das Coisas. Recentemente, durante um seminário organizado pela IDC, foram compartilhadas com o público algumas projeções futuras:

- Internet das Coisas e a nuvem: dentro dos próximos 5 anos, 90% dos dados da Internet das Coisas serão armazenados na nuvem;
- Internet das Coisas e segurança: dentro de dois anos, 90% de todas as redes de TI terão causado problemas de segurança pelo uso da Internet das coisas, de modo que é preciso criar novas políticas de segurança relacionadas à Internet das Coisas;
- Internet das Coisas e diversificação: a Internet das Coisas, hoje, centra-se na fabricação, no transporte e em cidades inteligentes, mas, dentro dos próximos cinco anos, todas as indústrias vão incorporar a IoT na sua infraestrutura;
- Internet das Coisas e cidades inteligentes: em 2018, os governos locais vão investir para desenvolver, testar e instalar uma infraestrutura baseada em Internet das Coisas.

O presente trabalho analisa os estudos de diversas universidades em nossa região no desenvolvimento de aplicações inovadoras que utilizam Internet das Coisas.

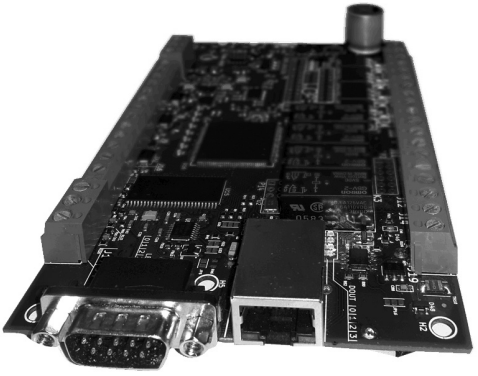
Estes desenvolvimentos terão um grande impacto sobre a indústria, a saúde, a educação e o ambiente urbano em nossa região.

O "ARDUINO" LATINO-AMERICANO

O projeto Computadora Industrial Abierta Argentina (CIAA) é o resultado de um trabalho colaborativo e articulado entre a indústria e a universidade pública.[2]

2 Ver: COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Objetivos del proyecto. Disponível em: <http://proyecto-ciaa.com.ar/devwiki/doku.php?id=start>. Acesso em: 12 set. 2017.

Figura 1 – Imagem da Computadora Industrial Abierta Argentina (CIAA)



Fonte: COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Disponível em: <http://proyecto-ciaa.com.ar/images/placa3b.png>. Acesso em: 12 set. 2017.

Este projeto começou em 2013 por iniciativa do Ministério da Indústria da Argentina e do Ministério da Educação. A ideia inicial do projeto era encontrar um sistema eletrônico aberto de uso amplo e geral, com o qual as empresas poderiam incorporar elementos de automação em seus processos sem a necessidade de determinados fornecedores.

O projeto envolveu as principais Câmaras Nacionais de Comércio, empresas e universidades. Este trabalho colaborativo foi capaz de criar um dispositivo que combina duas qualidades importantes:

- *Industrial:* o projeto está preparado para as exigências de confiabilidade, temperatura, vibração, ruído eletromagnético, tensão, curto-circuito, etc., exigidos pelos produtos e processos industriais;
- *Aberto:* todas as informações sobre o desenho de hardware, firmware, software, etc., estão disponíveis gratuitamente na Internet, sob a licença BSD.[3]

Seu escopo é amplo e se concentra, principalmente, na indústria e educação, áreas que possuem processos acerca dos quais se deseja entender o uso desses dispositivos, tais como o dimensionamento de protótipos de nova automação de produtos ou processos de produção.[4]

3 Ver: WIKIPEDIA. Licencia BSD. Disponível em: <https://es.wikipedia.org/wiki/Licencia_BSD>. Acesso em: 12 set. 2017.

4 Ver: COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Cursos Abiertos de Programación de Sistemas Embebidos (CAPSE). Disponível em: <http://proyecto-ciaa.com.ar/devwiki/doku.php?id=educacion:cursos:cursos_programacion_ciaa>. Acesso em: 12 set. 2017.

A vantagem destes dispositivos desde a perspectiva da educação é de grande importância, uma vez que a aprendizagem é organizada para uma audiência com ou sem experiência prévia em trabalhar com este tipo de sistemas. Assim, os professores de nível secundário, estudantes de universidades e funcionários de empresas são beneficiados.

Com a finalidade de promover processos educativos, o projeto desenvolveu uma versão econômica do dispositivo, o EDU-Kit CIAA Económica, que consiste em todas as partes relevantes em uma versão simplificada, orientada à educação. Este kit econômico é vendido sem fins lucrativos através de um sistema de venda antecipada *on demand*, que permite financiar a produção dos *kits*.

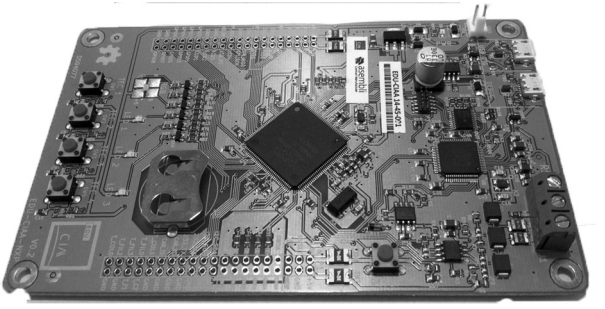
Sendo um projeto de grande impacto educacional e industrial, o CIAA foi homenageado com prêmios importantes, sendo eleito produto inovador e declarado de interesse nacional pela Câmara dos Deputados da Argentina. Um dos objetivos do projeto é a criação de novos métodos de desenvolvimento de produtos e processos de produção na indústria, além da promoção de capacidades tecnológicas na educação.

O Ministério da Ciência, Tecnologia e Inovação Produtiva da Argentina apoiou este projeto lançando um concurso de projetos com base no CIAA. Câmaras industriais também estão envolvidas na sua utilização e desenvolvimento. O projeto conta com o apoio das universidades da Argentina e da sua rede de especialistas de universidades em todo o mundo.[5]

Atualmente, o CIAA está disponível em diferentes versões e trabalha-se para que sua programação em diferentes idiomas seja possível. O projeto é apoiado por uma grande comunidade de milhares de desenvolvedores. A lista inclui empresas de diversos países da América Latina e outras regiões. Também tem despertado grande interesse na imprensa, pois atende duas características notáveis: é um produto industrial e tem base em padrões abertos, incluindo o impacto na educação.

5 Para lista de universidades do projeto, ver: COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Aportes de las Universidades. Disponível em: <http://proyecto-ciaa.com.ar/devwiki/doku.php?id=aportes_universidades>. Acesso em: 12 set. 2017.

Figura 2 – EDU-CIAA Kit educativo econômico pronto para uso



Fonte: COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Disponível em: <http://proyecto-ciaa.com.ar/devwiki/lib/exe/fetch.php?media=edu-ciaa-nxp:lg_31-finales.jpg>. Acesso em: 12 set. 2017.

COMO EMPREENDER COM A IOT

Muitos dos projetos de empreendedorismo estão relacionados a novas tecnologias. Neste contexto, a Internet das Coisas não é exceção. Existem vários programas para promover o empreendedorismo na América Latina e muitos dos projetos que são selecionados e que receberão financiamento são baseadas no uso desta tecnologia.

O Chile é um país conhecido por vários programas de criação de empresas. Um deles é promovido pela Universidade Tecnológica do Chile, através do seu Instituto de Formação Profissional e Centro Técnico INACAP.[6] Através de sua rede de empreendedorismo e de seu programa "50 ideias para a inovação", recebe abordagens inovadoras para resolver problemas urbanos.[7] O INACAP, em parceria com as empresas Hiway, Cisco, Samsung e Corfo, leva adiante o "Desafio da Internet das Coisas: Chile Prende", competição onde projetos recebidos relacionam os sistemas de tecnologia com uso da Internet das Coisas para monitoramento de pessoas em estado crítico, como capacetes inteligentes para monitoramento de trabalhadores expostos a risco, filtros inteligentes que podem ser monitorados pela Internet ou dispositivo móvel, modelos inteligentes para diabéticos que transmitem informações para dispositivos móveis, roupa de trabalho arnês ligada ao sistema de monitoramento integrado, auto cultivo de flores com monitoramento remoto, etc.

6 Ver: INACAP. Disponível em: <http://www.inacap.cl/web/2016/sites/50ideas/index.html>. Acesso em: 12 set. 2017.

7 Ver: CENTRO DE EMPRENDIMENTO INACAP. Disponível em: <http://www.redemprendimientoinacap.cl/>. Acesso em: 12 set. 2017.

O Innovation Center da Universidade Católica do Chile, juntamente com o Banco Santander, criou o BrainChile, que promove e financia projetos de desenvolvimento inovadores. Um dos destaques foi a proposta de criação de robôs para a limpeza de painéis solares para aumentar a eficiência na geração de energia.[8]

Esta liderança levou o Chile a ocupar a posição de número 16 dentro do Índice Global de Empreendedorismo 2016, sendo o único país da América Latina na lista dos 20 primeiros países.[9] O *ranking* destaca o potencial da América Latina e o espírito empreendedor de seus profissionais.

AGRICULTURA, BIODIVERSIDADE E VULCÕES

A agricultura é um componente muito importante da economia de todos os países da América Latina. De acordo com a FAO, a Organização das Nações Unidas para Alimentação e Agricultura, se a população mundial crescer para 9,1 bilhões em 2050, será necessário um aumento de 70% na produção global de alimentos. Isto significa que a produção de cereais anual terá que aumentar em 46% e a produção de carne, em 76%. Os agricultores terão que aumentar a produção de alimentos em 68% para atender a demanda mundial de alimentos. Neste contexto, a Internet das Coisas será relevante para a implementação da chamada agricultura de precisão, que irá aumentar significativamente até 2020.[10] De acordo com a FAO, a América Latina vai produzir 50% do aumento da demanda mundial de alimentos.

De acordo com a OMC, o México ocupa o número 12 na produção de alimentos frescos em todo o mundo.[11]

---

8 Ver: PONTIFICIA UNIVERSIDADE CATÓLICA DE CHILE. GRUPO ENGIE PREMIA ROBOT QUE LIMPIA PANELES SOLARES DESARROLLADO POR INGENIEROS UC. 20 jun. 2016. Disponível em: <https://www.ing.uc.cl/grupo-engie-premia-robot-que-limpia-paneles-solares-desarrollado-por-ingenieros-uc/>. Acesso em: 12 set. 2017.

9 Ver: CENTRO DE DESARROLOO Y TRANSFERENCIA TECNOLOÓGICA. CHILE SE INSERTÓ EN EL TOP 20 DEL EMPRENDIMIENTO MUNDIAL. Disponível em: <http://inria.cl/chile-se-inserto-en-el-top-20-del-emprendimiento-mundial/>. Acesso em: 12 set. 2017.

10 Ver: THE WORLD BANK. Disponível em:< http://www.worldbank.org/en/topic/water/publication/high-and-dry-climate-change-water-and-the-economy>. Acesso em: 12 set. 2017.

11 Ver: CONSEJO MEXIQUENSE DE CIENCIA E TECNOLOGÍA. Disponível em: <http://comecyt.edomex.gob.mx/>. Acesso em: 12 set. 2017.

Para avaliar esta situação e as oportunidades potenciais para a economia mexicana, o Governo do México criou, através do INFOTEC CONACYT, o Laboratório Nacional da Internet do futuro. Este centro fornece a infraestrutura necessária para as universidades, as empresas e as organizações, de modo que possam trabalhar no uso de tecnologias baseadas na conectividade com a Internet, tais como a Internet das Coisas, a computação em nuvem e o *Big Data*. O centro também tem organizado uma parte da rede global FIWARE, que fornece uma plataforma para aplicativos de software criados a partir de padrões abertos, adaptáveis e inoperáveis.[12]

A fim de proteger a biodiversidade do Peru no Parque Nacional Manu, que foi reconhecido pela UNESCO como patrimônio mundial em 1987, desenvolveu-se um projeto para monitorar em tempo real este habitat natural. Muitas horas são necessárias para percorrer a estrada de acesso ao Parque Nacional de Manu e ela possui rios e selva. Durante esta viagem, pode haver chuvas e muito calor, de forma que este projeto desenvolvido pela empresa Libelium tem como objetivo fornecer informações em tempo real para os investigadores que trabalham nesta reserva natural e outros que estão interessados nela. Todos os dispositivos instalados funcionam com energia solar, o que também gera um baixo impacto ambiental.[13]

Vulcões são um fenômeno natural imprevisível. Prever sua atividade poderia salvar vidas e ajudar a economia e a saúde, pois seus gases e cinzas causam grandes complicações. Vulcanólogos estão, atualmente, trabalhando com a tecnologia para conhecer em tempo real o que acontece em torno da cratera do vulcão e, assim, poder predizer erupções. O vulcão Masaya na Nicarágua é um dos mais ativos na América Latina. A mesma empresa Libelium desenvolveu um projeto que tem como objetivo fornecer em tempo real um serviço de informação ao público sobre a atividade de um vulcão ativo.

Sensores conectados no vulcão enviam os dados a suas ferramentas de análise de informação, incluindo uma base de dados de mais de 20 anos no vulcão Masaya, em Honduras. Toda esta informação poderia ajudar a evitar uma crise vulcânica, criaria um sistema de alerta único no seu gênero e sua aplicação poderia ser usada a nível mundial.[14]

---

12 Ver: FIWARE. Disponível em:<https://www.fiware.org/>. Acesso em: 12 set. 2017.

13 Ver: LIBELIUM. Rain forest monitoring for climate change control in Peru. Disponível em: <http://www.libelium.com/rain-forest-monitoring-for-climate-change-control-in-peru/>. Acesso em: 12 set. 2017.

14 Ver: LIBELIUM. Predicting eruptions in the Masaya Volcano with wireless sensors. Disponível em: <http://www.libelium.com/predicting-eruptions-in-the-masaya-volcano-with-wireless-sensors/>. Acesso em: 12 set. 2017.

De acordo com a Organização Mundial da Saúde, atualmente 285 milhões de pessoas têm problemas de visão. Destes, 39 milhões têm problemas de visão completos e 246 milhões têm baixa visibilidade. Estes cidadãos têm grandes problemas para se mover através de uma cidade ou apenas circulam no interior de edifícios.

A equipe da Universidade Nacional de Engenharia do Peru e da Universidade de Castilla-La Mancha, Espanha, desenvolveu um dispositivo robusto e de baixo custo que permite que esses usuários só necessitem de um dispositivo móvel que interage por voz com uma aplicação para que sejam capazes de se mover de forma segura em cidades e edifícios.[15]

De acordo com o relatório do Ministério de Energia e Minas do Peru, entre 2013 a 2015 o setor de mineração tinha uma média de 107 mortes. O mesmo relatório observa que a maioria das mortes ocorrem devido a problemas de trânsito na mina, envenenamento, asfixia e absorção de gases em depósitos de minerais.

Os alunos do Centro de Tecnologia da Informação na Universidade Nacional de Engenharia desenvolveram um casco de segurança que reduziu a 33% a taxa de mortalidade em depósitos. O casco consiste em um sistema de alerta e de comunicação sem fio. Os trabalhadores de dentro da mina estarão conectados ao sistema e serão alertados sobre a proximidade de um incidente, além de receberem informações sobre a concentração de oxigênio ou a presença de gases tóxicos no local de trabalho e serão alertados para que possam sair da mina a tempo[16].

O casco de segurança ganhou o primeiro lugar na primeira maratona *hacker* Innovative Technology for Social Responsibility, no Setor Minas e Energia, organizado pela Sociedade Nacional de Mineração, Petróleo e Energia do Peru.

O México criou o Centro de Inovação, Desenvolvimento de Tecnologia e Aplicações Internet das Coisas, onde universidades, empresas privadas e centros de pesquisa se relacionam para promover projetos inovadores que utilizam a Internet das Coisas com fundos do governo. Aplicações tecnológicas e protótipos resultantes de CIIOT incidirão sobre os setores identificados como prioritários pela Agenda de Inovação mexicana: agroa-

15 Ver: SCIENCE DIRECT. Ray: Smart Indoor/Outdoor Routes for the Blind Using Bluetooth 4.0 BLE. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1877050916301843>. Acesso em: 12 set. 2017.

16 Ver: ROJAS, Yazmin. Universitarios construyen casco para disminuir accidentes en minas. RPP NOTICIAS, 02 out. 2016. Disponível em: <https://goo.gl/WCq7QT>. Acesso em: 12 set. 2017.

limentação, saúde, tecnologia da informação e indústrias de comunicação e de biotecnologia criativas. Alguns dos membros da CIIOT são o Instituto Tecnológico de Monterrey, a Luxoft, a MXP, a Intel, a IBM e a Microsoft com o apoio do IEEE.[17]

IOT PARA O FUTURO

Como demonstrado por estas iniciativas que nascem em universidades da região, a Internet das Coisas traz uma variedade de possibilidades criativas que utilizam a tecnologia como o núcleo do projeto. Inovação, empreendedorismo e pesquisa se reúnem para fornecer à indústria e à sociedade novas opções para um melhor desenvolvimento.

Ao mesmo tempo, a Internet das Coisas levanta uma série de desafios que devem ser levados em conta por todos os interessados no ecossistema da Internet e da sociedade:

- a Internet das Coisas vai gerar uma grande quantidade de dados que devem ser armazenados com a segurança necessária;
- a Internet das Coisas traz dilemas de privacidade, por exemplo: como e quando um indivíduo quer ser monitorado e estar conectado;
- a Internet das Coisas vai gerar uma demanda adicional de energia e aumentará a geração de resíduos tecnológicos;
- a Internet das Coisas exigirá o desenvolvimento do padrão Ipv,[6] pois é a única maneira de conectar tantos dispositivos à Internet;
- a Internet das Coisas será uma mudança para a sociedade, uma vez que tudo estará conectado e tudo poderá ser detectado e medido;
- a Internet das Coisas significa máquinas conectadas entre si, redes de sensores sem máquinas e máquinas sem interação humana;
- a Internet das Coisas coloca desafios semelhantes aos relacionados com *Big Data, Cloud Computing e Data Mining*;
- a Internet das Coisas deve resolver a interoperabilidade entre tecnologias e padronização.

A Internet das coisas pode ser assustadora. No entanto, já existe uma série de tecnologias que automatizam parte das atividades da indústria ou em que pessoas estão envolvidas. A incorporação maciça dessas tecnologias deve ser associada com o devido respeito à privacidade, ao ambiente e à segurança das pessoas, das organizações e das informações.

17 Ver: CONECTA. Disponível em: <http://www.itesm.mx/wps/wcm/connect/snc/portal+informativo/por+tema/investigacion/tec-ciiot>. Acesso em: 12 set. 2017.

As universidades na América Latina irão desempenhar um papel de grande importância na pesquisa de produtos e serviços que utilizam a Internet das Coisas como diferencial tecnológico e serão importantes para ajudar a indústria, o governo e as organizações na sua adoção bem-sucedida.

REFERÊNCIAS

CAF, LACNIC. Despliegue de IPV6 para el desarrollo socio económico en América Latina y el Caribe. Diciembre 2015. Disponível em: <http://portalipv6.lacnic.net/caf-lacnic/>. Acesso em: 12 set. 2017.

CAVALLI, Olga. *Internet de las Cosas en América Latina***.** Departamento de Sistemas. Facultad de Ciencias Económicas. Universidad de Buenos Aires, octubre 2015.

CENTRO DE DESARROLOO Y TRANSFERENCIA TECNOLOÓGICA. CHILE SE INSERTÓ EN EL TOP 20 DEL EMPRENDIMIENTO MUNDIAL. Disponível em: <http://inria.cl/chile-se-inserto-en-el-top-20-del-emprendimiento-mundial/>. Acesso em: 12 set. 2017.

CENTRO DE EMPRENDIMENTO INACAP. Disponível em: <http://www.redemprendimientoinacap.cl/>. Acesso em: 12 set. 2017.

COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Aportes de las Universidades. Disponível em: <http://proyecto-ciaa.com.ar/devwiki/doku.php?id=aportes_universidades>. Acesso em: 12 set. 2017.

COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Cursos Abiertos de Programación de Sistemas Embebidos (CAPSE). Disponível em: <http://proyecto-ciaa.com.ar/devwiki/doku.php?id=educacion:cursos:cursos_programacion_ciaa>. Acesso em: 12 set. 2017.

COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Disponível em: <http://proyecto-ciaa.com.ar/images/placa3b.png>. Acesso em: 12 set. 2017.

COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Disponível em: <http://proyecto-ciaa.com.ar/devwiki/lib/exe/fetch.php?media=edu-ciaa-nxp:lg_31-finales.jpg>. Acesso em: 12 set. 2017.

COMPUTADORA INDUSTRIAL ABIERTA ARGENTINA (CIAA). Objetivos del proyecto. Disponível em: <http://proyecto-ciaa.com.ar/devwiki/doku.php?id=start>. Acesso em: 12 set. 2017.

CONECTA. Disponível em: <http://www.itesm.mx/wps/wcm/connect/snc/portal+informativo/por+tema/investigacion/tec-ciiot>. Acesso em: 12 set. 2017.

CONSEJO MEXIQUENSE DE CIENCIA E TECNOLOGÍA. Disponível em: <http://comecyt.edomex.gob.mx/>. Acesso em: 12 set. 2017.

FIWARE. Disponível em:<https://www.fiware.org/>. Acesso em: 12 set. 2017.

IDC. IDC FutureScape: Worldwide Internet of Things (IoT) 2017 Predictions. Noviembre 2016. Disponível em: <http://www.idc.com/getdoc.jsp?containerId=US41910716>. Acesso em: 12 set. 2017

INACAP. Disponível em: <http://www.inacap.cl/web/2016/sites/50ideas/index.html>. Acesso em: 12 set. 2017.

INTEL. Rise of the Embedded Internet. White Paper Intel Embedded Processors. Junio 2016. Disponível em: <http://download.intel.com/newsroom/kits/embedded/pdfs/ECG_WhitePaper.pdf.>. Acesso em: 12 set. 2017

LIBELIUM. Predicting eruptions in the Masaya Volcano with wireless sensors. Disponível em: <http://www.libelium.com/predicting-eruptions-in-the-masaya-volcano-with-wireless-sensors/>. Acesso em: 12 set. 2017.

LIBELIUM. Rain forest monitoring for climate change control in Peru. Disponível em: <http://www.libelium.com/rain-forest-monitoring-for-climate-change-control-in-peru/>. Acesso em: 12 set. 2017.

MOHAM, Ram. Riesgos en Internet de las Cosas. CircleID. Septiembre 2015. Disponível em: <http://www.circleid.com/posts/20150602_internet_of_things_solving_security_challenges/>. Acesso em: 12 set. 2017

PONTIFICIA UNIVERSIDADE CATÓLICA DE CHILE. GRUPO ENGIE PREMIA ROBOT QUE LIMPIA PANELES SOLARES DESARROLLADO POR INGENIEROS UC. 20 jun. 2016. Disponível em: <https://www.ing.uc.cl/grupo-engie-premia-robot-que-limpia-paneles-solares-desarrollado-por-ingenieros-uc/>. Acesso em: 12 set. 2017.

RFID JOURNAL. That 'Internet of Things' Thing. Mayo 2015. Disponível em: <http://www.rfidjournal.com/article/print/4986>. Acesso em: 12 set. 2017

ROJAS, Yazmin. Universitarios construyen casco para disminuir accidentes en minas. RPP NOTICIAS, 02 out. 2016. Disponível em: <https://goo.gl/WCq7QT>. Acesso em: 12 set. 2017.

SCIENCE DIRECT. Ray: Smart Indoor/Outdoor Routes for the Blind Using Bluetooth 4.0 BLE. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1877050916301843>. Acesso em: 12 set. 2017.

TELEFONICA. Smart m2m Solution. Octubre 2016. Disponível em: <https://m2m.telefonica.com/telefonica-m2m/solutions/m2m-managed-connectivity/smart-m2m-solution>. Acesso em: 12 set. 2017

THE WORLD BANK. Disponível em:< http://www.worldbank.org/en/topic/water/publication/high-and-dry-climate-change-water-and-the-economy>. Acesso em: 12 set. 2017.

UIT. Internet of Things Global Standards Initiative. Disponível em: <http://www.itu.int/en/ITU-T/jca/iot/Pages/default.aspx>. Acesso em: 12 set. 2017

VERIZON. Discover how IoT is transforming business results. State of the Market: The Internet of Things 2015, ago. 2015. Disponível em: <http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf>. Acesso em: 12 set. 2017

WIKIPEDIA. Licencia BSD. Disponível em: <https://es.wikipedia.org/wiki/Licencia_BSD>. Acesso em: 12 set. 2017.

WORLD HEALTH ORGANIZATION. Visual impairment and blindness. Fact Sheet N282, ago. 2014. Disponível em: <http://www.who.int/mediacentre/factsheets/fs282/en/>. Acesso em: 12 set. 2017.

DE PRODUTOS A SERVIÇOS: A IOT E A TRANSFORMAÇÃO DA MANUFATURA

EDUARDO PEIXOTO

IOT, O QUE É?

Internet das Coisas, IoT do inglês *Internet of Things*, ou a Internet de Tudo, não se trata de mais um dispositivo ou uma plataforma, mas como bem antecipou Greenfield (2006), de uma era onde todos os objetos serão capazes de capturar, receber, transmitir, armazenar, processar e mostrar informação e, eventualmente, agir em contexto por e para nós – seres humanos –, nos orientando como assistentes inteligentes, ou tomando decisões em nosso nome.

A definição é bem ampla. Talvez para entender melhor, deveríamos voltar um pouco no tempo. Lá atrás, na década de 80, 10 anos antes da internet, algumas máquinas começavam a ser interligadas: os caixas automáticos (ATM). Talvez não tenham sido as primeiras, mas foram de amplo uso pela população. Os ATM capturavam informações do cartão, transmitiam para os computadores dos bancos, mostravam saldos, e permitiam ou não saques. Sim, primitivos e limitados, mas certamente uma das primeiras aparições da IoT para nós humanos.

A conexão dos objetos prosseguiu, e com o nome de telemetria foi usada para rastrear aviões, frotas de caminhões e, mais recentemente, acompanhar o consumo de energia em residências – medidores inteligentes –, permitindo a gestão mais eficiente de recursos.

Lá para 2010, a IoT começou a tomar outro rumo. Com a internet bem mais popularizada – e sendo usada como meio de conexão das coisas também –, os objetos passaram a capturar dados e tomar decisões bem mais perto – fisicamente ou não – da gente. É bem por aqui que a vida começava a ficar mais fácil, mais inteligente, ou simplesmente *smart*. Computadores, telefones, TVs, veículos… Todo e qualquer objeto capaz de entender algum contexto local – posição, temperatura, movimento,

humor etc. – e de enriquecê-lo através de conexões na *web* com outros objetos ou sistemas, tornou-se potencialmente um grande conselheiro, um assistente inteligente. "Pegue esta rua, ao invés daquela, para ir para casa de seus pais"; "Quando entrar no metrô, leia este livro"; "Já que está na TV, assista hoje a este filme"; "E que tal marcar seu exame preventivo (o último já faz mais de dois anos…)?".

São apenas objetos conectados? Ou sou eu, o conectado? Em 2010 nos EUA, mais de 105 milhões de pessoas já possuíam dois ou mais dispositivos conectados à internet. E, pasmem, 4,5 milhões já possuíam mais de nove. Com os *wearables* vamos literalmente nos entregar à rede. Nossa temperatura corpórea, batimentos cardíacos, nível de movimentação, açúcar no sangue, pressão e tantos outros indicadores do nosso estado de saúde poderão ser monitorados 24x7, com a séria possibilidade do medidor – vestível – não passar de uma simples tatuagem de um circuito impresso na pele.

As projeções de mercado para a IoT são gigantescas. A CISCO fala em 50 bilhões (EVANS, 2011) de coisas conectadas em 2020 – não sei se incluindo nós, 7,6 bilhões, ou não. As vacas, sim, todas serão rastreadas. Os setores impactados? Praticamente todos. Da saúde às casas, do agronegócio e das utilidades ao setor automobilístico. Os investimentos nestes setores, para capturar as oportunidades da IoT, serão gigantescos e o impacto na economia pode atingir US$ 11 trilhões até 2025 (MANYIKA; CHUI, 2015).

Nada será como antes. Nas casas podemos imaginar fogões que conversam com geladeiras, que pedem receitas que contenham os alimentos mais próximos do prazo de validade. No carro, que tal ele avisar quando é tempo de fazer a revisão? E se entrar em contato com a concessionária mais próxima de sua residência, verificar sua agenda no *smartphone* e programar a revisão com todas as partes para data mais próxima? Sim, por que não? Os cenários são milhares.

Maiores ainda são os desafios até chegarmos lá. Para nós humanos – mais velhos –, segurança e privacidade são os primeiros a saltarem aos olhos. O que faremos, ou como nos adaptaremos a um mundo nu? Nu por ter se tornado vazio em privacidade. E nu também por permitir a antecipação de muitos, senão todos, os nossos passos. Viveremos bem, sem surpresas ou imprevistos? Viveremos bem sem segredos?

DE MECÂNICOS E ISOLADOS A INTELIGENTES E CONECTADOS

Moore (1965) previu que, enquanto o número de componentes por unidade de circuito integrado (CI) cresceria numa proporção que a complexidade – capacidade de armazenamento ou performance – dobraria a cada 18 meses, o custo por unidade cairia, de forma a manter o preço do CI constante. Moore foi além, prevendo que o aumento da complexidade dos circuitos integrados produziria maravilhas como computadores domésticos, controles automáticos para carros e equipamentos de comunicação pessoal.

Não errou quase nada, mas a miniaturização contínua dos circuitos integrados e o consequente aumento de complexidade sem aumento de preço levaram os circuitos integrados e a eletrônica muito além. Circuitos integrados altamente complexos, custando perto de zero, passaram a integrar todo tipo de objeto. Moore imaginou os circuitos integrados equipando objetos de maior valor agregado, mas já encontramos hoje, objetos simples, como lâmpadas, equipadas com eles.

Até então, os objetos que nos cercavam, ou Produtos, eram sua grande maioria eletromecânicos e Isolados (PMI). Entenda isolados, por estarem acessíveis apenas quando estamos próximos o suficiente para tocá-los. Os circuitos integrados em objetos passam a conferir a eles capacidade de processamento e comunicação, e os dois combinados, inteligência! Estes objetos – desde que tenham energia – estarão sempre atentos ao nosso contexto – 24 horas, 7 dias por semana –, avaliando, orientando e tomando pequenas decisões por nós. Como por exemplo, o que comprar, quando comprar e onde comprar, ou mesmo, realizando a compra por nós. Sim, sua geladeira vai lhe poupar muito tempo!

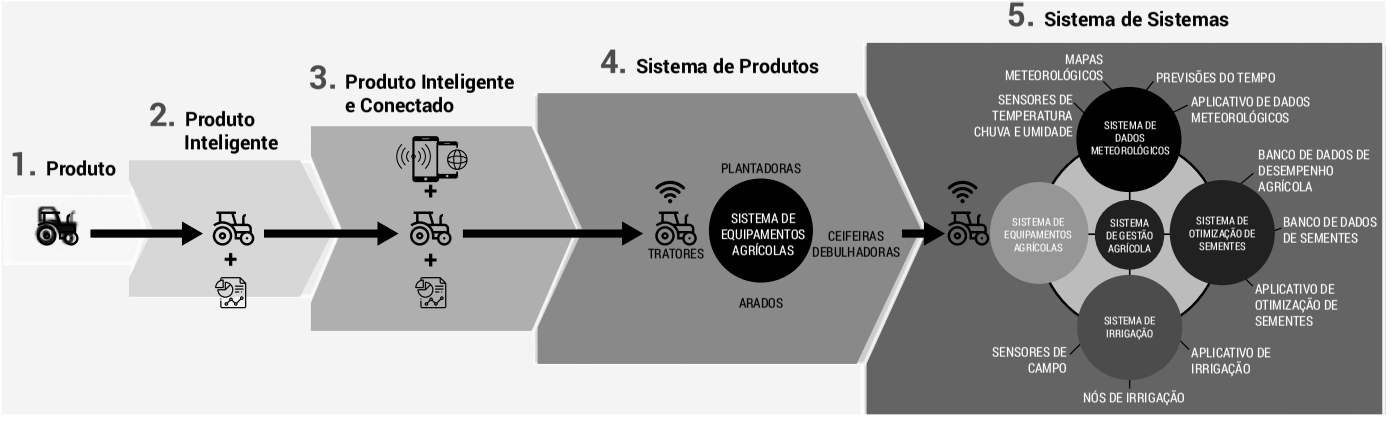
Objetos com cognição serão assistentes inteligentes e tornarão nossas vidas mais fáceis. É o que já acontece com o carro. Os mais sofisticados chegam a ter 70 unidades de processamento e possuem inteligência suficiente para reconhecer placas na estrada, nos alertar sobre limites de velocidade, ou mesmo frear por nós em situações de risco.

Com o advento da IoT, os Produtos Inteligentes – ricos em CI – serão Conectados (PIC). Eles ampliarão a capacidade de processamento na nuvem, adquirindo mais funções, cooperarão com produtos similares ou complementares e assim, melhorarão a nossa – ou deles – capacidade de decisão. O carro conectado, por exemplo, enviará informações sobre velocidade das vias em que trafega, obstáculos e acidentes no percurso para a administração pública. Enviará também, para a montadora, as condições de uso e desgaste das peças, permitindo a predição de falhas e o agendamento

antecipado de paradas para reparo. Ainda, de forma similar aos *smartphones*, o carro inteligente conectado poderá receber atualizações de software para correção de falhas ou ampliação de suas funções, ou melhorias de desempenho no produto. Segundo os PoETAS.IT (2016),

> Michael Porter e James Heppelmann (2014) apresentam uma destas mudanças na natureza dos bens através do que denominam "smart connected products" (produtos inteligentes conectados), onde ele sugere o exemplo de um trator (ver figura). Na figura, um trator isolado é apenas um produto industrial usado para aumentar a produtividade da agricultura. Adicionando-se um computador a este trator ele passa a ser reconhecido como um "produto inteligente". Se a este trator inteligente é estabelecida uma conectividade (através de qualquer dispositivo móvel), este trator é agora um "produto inteligente conectado- PIC", que pode acessar tanto diversas etapas do seu sistema produtivo quanto informação de outros sistemas produtivos, o que pode resultar na modificação do comportamento do trator no "seu" sistema. (PoETAS.IT, 2016, p. 15)

Figura 1 – Produtos Inteligentes Conectados



Fonte: Adaptação de Porter e Heppelmann (2014).

Mas a transformação para PIC pode ter ainda uma amplitude muito maior. Produtos similares conectados podem ser geridos em conjunto para aumento do desempenho do conjunto, para obtermos mais com menos. Uma frota de carros conectados pode ser gerida para minimizar o deslocamento, o tempo de atendimento do usuário e a quantidade de carros necessários rodando. No futuro, a inteligência do automóvel pode também tornar o motorista desnecessário. Se os carros forem conectados e compartilhados, demostra um estudo realizado para a cidade de Lisboa (ITF/OECD, 2015), pode-se obter praticamente a mesma mobilidade existente na cidade com apenas 10% da frota existente. Potencial enorme de ganho de espaço público, dedicado hoje para estacionamento, e uma redução sem precedentes da necessidade de produção de veículos. Este grau de otimização será possível em diversas outras indústrias.

Existe ainda uma outra forma de otimização possível para produtos em rede. Conectados a outros objetos e a sistemas na internet, os PIC podem acessar informações relevantes para ampliação do seu funcionamento. Por exemplo, equipamentos de irrigação isolados podem ter seu desempenho otimizado localmente. Porém um conjunto de equipamentos de irrigação inteligentes e conectados, coletando dados do INPE sobre pluviometria e incidência solar, e da EMBRAPA sobre o tipo de solo, podem otimizar o uso da água e, ao mesmo tempo, maximizar o resultado financeiro da safra.

ENCURTANDO A DISTÂNCIA ENTRE QUEM PRODUZ E QUEM CONSOME

Produtos de *software* são produtos virtuais, que desempenham funções específicas, executando-as sobre computadores genéricos. Os PIC também são produtos de *software*, mas que executam sobre computadores específicos – objetos como: lâmpadas, purificadores de água, bicicletas, carros etc. Como objetos híbridos – de *hardware* e *software* –, mas cada vez mais intensivos em *software*, herdam características similares aos produtos da indústria digital. E uma delas, desde a inauguração do modo Beta – permanente – pelo Google, é que a evolução do produto ocorrerá em grande parte durante o uso.

O PIC, portanto, irá eliminar a distância entre quem produz e quem faz uso do produto. Os sensores e a conectividade dos PIC podem capturar continuamente dados sobre o ambiente em que estão inseridos – temperatura, luminosidade, localização, umidade etc. –, assim como dados de uso e funcionamento – nível de ruído, consumo de energia, trepidação, velocidade, aceleração etc. – e enviá-las para a nuvem do fabricante, criando um fluxo contínuo e massivo de troca de dados – *Big Data* – entre usuário/produto e quem fabrica ou opera o produto.

Figura 2 – Fluxo de Inovação Contínua

Fonte: Centro de Estudos e Sistemas Avançados do Recife (CESAR).

Este fluxo permitirá ao fabricante ou operador do produto observar padrões de uso e desempenho, e então, corrigir falhas, modificar características que melhorem o desempenho, ou mesmo adicionar novas funcionalidades ao produto, tudo enquanto em uso – e sem que o usuário necessariamente se aperceba ou tenha consciência do que está ocorrendo. É o que já observamos nos nossos *smartphones*. O sistema operacional é atualizado periodicamente corrigindo vulnerabilidades e novas aplicações (APP) surgem a todo instante, ampliando a funcionalidade do produto. O mesmo já ocorre também com os carros. O piloto automático do Modelo S só foi lançado em 2016, mas é compatível com os carros vendidos desde 2013 – e o melhor é que ninguém precisa ir até a concessionária para atualizar o produto. Esta dinâmica, como observa o PoETAS.IT (2016), é precisamente como opera a indústria de jogos digitais:

> A título de exemplo, na chamada indústria de games (jogos digitais) para dispositivos móveis, o modelo de negócios largamente dominante é o free to play, em que não se paga para jogar mas apenas para obter certos itens (bens virtuais) dentro do jogo (Alha et al. 2014). Nesta abordagem, chamada de "Game as Service", para maximizar seu ganho, o desenvolvedor precisa compreender o comportamento e as preferências dos jogadores. Para tanto, o desenvolvedor gasta hoje apenas cerca de 20% do orçamento para lançar um produto e todo o restante (a) para adquirir e analisar grandes quantidades de dados sobre o comportamento dos jogadores e (b) para modificar o jogo de acordo com este entendimento. (PoETAS.IT, 2016, p. 16)

RUMO À ORIENTAÇÃO A SERVIÇOS[1] NA INDÚSTRIA DE BENS

A Promon Logicalis (2017) realizou pesquisa com 146 empresas de grande porte, dos mais diversos setores, das quais 33% são da vertical Serviços e 29% Manufatura. Entre as empresas brasileiras pesquisadas, entende-se por IoT "as tecnologias que possibilitam controle e automação de processos. Neste sentido a IoT vem sendo considerada por muitos entrevistados como uma evolução das tecnologias de automação industrial, incluindo telemetria, machine-to-machine (M2M) e identificação por radiofrequência (RFID)".

É certo que a IoT possibilitará um grande aumento de eficiência, mas as maiores oportunidades de inovação e ganhos estarão da porta da fábrica para fora: na inovação do produto, ou forma de comercialização dos produtos – ou sobre o que eles entregam. Os PIC reduzem a distância entre quem produz e quem usa o produto, criando um fluxo contínuo de troca de dados entre as duas pontas da cadeia de produção. Por serem intensivos em *software* – híbridos de *hardware* e *software* – facilitam o desenvolvimento de novas aplicações e a melhoria contínua de aplicações existentes – que modificam o próprio produto.

Também é esperado, com a hibridização do produto, que novos modelos de negócios, mais similares aos praticados na indústria de *software*, sejam explorados e acelerem a orientação a serviços das indústria de bens. Em estudo conduzido na Eindhoven University of Technology sobre modelos de negócios para a IoT, Dijkman *et al.* (2015) apontam para a importância do *software* nos negócios da IoT: *software* e desenvolvedores de *software* são apontados respectivamente como os tipos mais importantes nos blocos de modelo de negócios (OSTERWALDER; PIGNEUR, 2010) Parceiros Chave e Recursos Chave da pesquisa. Adicionalmente, Subscription Fee e Usage Fee aparecem como os principais tipos no bloco de Fluxos de Receita das empresas pesquisadas. São tipos de fluxos de receita que conferem ao consumidor não a posse, como a compra de um produto, mas o uso, como um serviço, do que é entregue. Tipos de fluxo de receita como estes são comuns na indústria de software, como observado no PoETAS.IT (2016):

> Outro aspecto a se notar na mudança da natureza dos bens é aquele que ocorre no seio da indústria de tecnologias de informação e comunicação – TICs, quando cada vez mais se percebe (em função das inovações tecnológicas e organizacionais) a transformação dos principais bens deste setor em serviços, tais como aqueles que compõem as principais camadas

1 Estratégia para aumentar a oferta combinada de produtos e serviços com foco nos clientes e seus negócios.

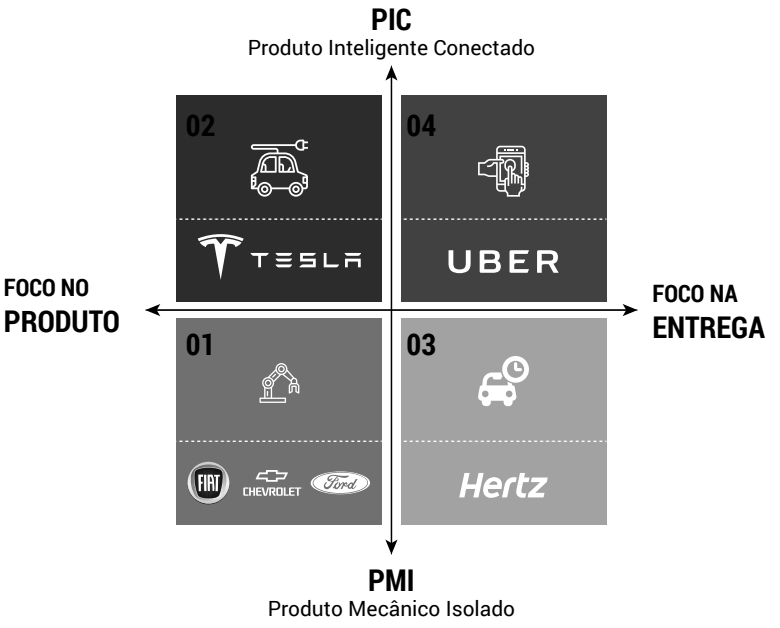
> dos modelos de negócios baseados em cloud computing (computação em nuvem): a) IaaS – Infrastructure as a Service (Infraestrutura como Serviço); PaaSPlatform as a Service (Plataforma como Serviço); e, c) SaaS- Software as a Service (Software como Serviço). (PoETAS.IT, 2016, p. 15)

As mudanças provocadas pela IoT no produto levantam questões importantes quanto ao foco a se dar nesta transição. Continuaremos pagando pelo produto em si, ou pelo que ele entrega? UBER e AIRBNB crescem exponencialmente sem possuir um único ativo que operam para entregar um serviço – transporte e hospedagem, respectivamente –, e outras como a Serttel e Brastemp exploram modelos *pay per use* com bicicletas e purificadores de água. Quem consome o que estas empresas entregam consome o que seus produtos entregam, na forma de serviços. Os produtos manufaturados, os carros, os quartos, as bicicletas e os purificadores de água são meios para que a entrega dos serviços possam ocorrer, e portanto, parte substituível e de menor valor na cadeia de entrega do serviço. Ter a IoT como um meio de aumento de eficiência, é direcionar os esforços na parte da cadeia de entrega de serviços de menor valor agregado, nas plataformas de *hardware*.

OS CENÁRIOS PARA A INDÚSTRIA DE BENS

A IoT tornará a separação entre indústrias físicas e digitais irrelevante (FLEISCH; WEINBERGER *et al.*, 2014). Ter como foco de aplicação apenas o aumento de eficiência na indústria de produção de bens, é deixar de lado a maior fatia do bolo; ignorar a possibilidade de construirmos no país serviços de alcance global. Já argumentamos anteriormente, que a inovação nos produtos provocada pela IoT marcará o futuro de produtos intensivos em serviços. No entanto, esta não é uma transformação trivial para a indústria de bens. A orientação a serviço constitui um grande desafio para essas empresas, pois seus modelos de negócio tradicionais têm foco no desenvolvimento, produção e venda de produtos. Em estudo de caso realizado na Scania, Mattos (2012) observou que para empreender um modelo de negócios com maior parcela de serviços a empresa precisou criar novas organizações, processos e métricas com foco nos clientes e novos modelos de receitas, baseados em contratos de risco e na venda de desempenho. Uma mudança nada simples para empresas estabelecidas com fluxos de receita bem definidos.

Figura 3 – Cenários para Indústria de Bens



Fonte: Centro de Estudos e Sistemas Avançados do Recife (CESAR)

Mas a IoT, assim como a internet, é um caminho sem volta. E que vai dividir o espaço de negócios das empresas com foco em produtos – venda de ativos – ou foco na entrega – venda de serviços – pelo eixo de produtos mecânicos e isolados (PMI) a produtos inteligentes e conectados (PIC), criando quatro possíveis cenários para a indústria de bens manufaturados:

1. permanecem como estão;
2. evoluem para fabricar produtos inteligentes e conectados;
3. operam serviços baseados em produtos mecânicos e isolados;
4. operam serviços por meio de produtos inteligentes e conectados

Veja na Figura 3 estes cenários aplicados à indústria automotiva. Algumas combinações destes cenários também são possíveis, como fabricar e operar produtos mecânicos e isolados. Mas cada um dos novos cenários, ou a combinação deles, apresenta diferentes desafios.

A opção pelo cenário 1 é a opção pela zona de conforto, que não é muito robusta. Além de excluir a participação da empresa no que será o maior mercado dos próximos anos, irá deixá-la vulnerável ao ataque de novos entrantes, ou de *incumbentes* mais flexíveis que evoluírem seus produtos para o cenário 2.

A transição do cenário 1 para o cenário 2 não é sem dor. Embora a fonte de receita ainda esteja calcada na venda de ativos, os produtos inteligentes e conectados são intensos em *software*. Para fazer esta migração, a indústria necessitará adquirir novos conhecimentos. Para ser capaz de desenhar, desenvolver, distribuir e manter produtos que são intensos em *software*, a indústria precisará adquirir e aprender a lidar com processos e equipes inteiras de cientistas da computação e afins, com especialização em inteligência artificial, comunicação, análise, privacidade e segurança de dados.

O cenário 3 é para quem quer deixar de ser indústria ou avançar na cadeia de valor ofertando serviços. E por que não? Talvez até por influência dos modelos praticados pela maioria das indústrias puramente digitais – Netflix, Spotify, Amazon AWS entre muitas outras –, o desejo de posse é substituído lentamente na sociedade pelo desejo de uso. As empresas tradicionais de PMI podem adicionar valor a produto pela oferta de pacotes de serviços associados.

E por fim, temos o cenário 4, que é certamente o mais difícil de todos para a indústria tradicional. Nele habita o que chamamos, em referência à indústria de *games*, de operador de produto. Além de fazer toda a mudança para atualizar sua capacidade de concepção e desenvolvimento de produtos, como no cenário 2, a indústria precisará desenvolver competências de uma empresa de serviço, pois operar um serviço baseado em produtos conectados significa saber capturar dados – do produto e do usuário –, interpretá-los, armazená-los – e lidar com todas as questões de privacidade e segurança – e continuamente evoluir o produto, além de entender e atender usuários na prestação do serviço na interface não digital.

Não será fácil, mas dependendo do setor que a indústria se encontra, não existem boas alternativas. Imaginem se forem poucos os provedores de serviços que necessitam do seu produto… Imaginem eles dominantes. Pois não só a maior parte do valor capturado estará com o provedor do serviço, como será ele quem irá determinar os volumes de produção. Manter-se na zona de conforto, achar que o cenário 1 é opção, é puro risco!

UNS POUCOS CASOS NO BRASIL

Embora ainda sejam vistas como periféricas, já é possível observar no Brasil mudanças impulsionadas na direção do cenário 4 ou empresas que se valem da IoT para atuar exclusivamente como operadoras de produtos. Citamos abaixo alguns casos, sem querer ser exaustivo, apenas para exemplificar esta narrativa:

- Serttel,[2] empresa que atua em mobilidade urbana com bicicletas. As bicicletas utilizadas no serviço foram desenhadas e produzidas pela Serttel, mas não são vendidas, são as plataformas de entrega do serviço de mobilidade;
- Aker,[3] empresa que utiliza o hardware de firewall[4] – *commodity* – para prover serviço de segurança digital com *software* proprietário;
- Brastemp, tradicional fabricante de produtos da linha branca que optou por criar um serviço de água filtrada,[5] ao invés de vender purificadores. O usuário assina o serviço, a Brastemp instala e mantém o purificar de água;
- Elcoma, que desenvolve no Brasil e produz no exterior, roteadores de alto desempenho,[6] que são comercializados como serviço para acesso a internet.

O DESAFIO PARA O BRASIL

As novas tecnologias não podem ser vistas apenas como uma forma de redução de custos. As soluções que surgirão com a IoT, no bojo de Manufatura Avançada, vão gerar redução de custos e ganhos de qualidade para a indústria. Mas a grande revolução na indústria com a IoT se dará em novos produtos, novos modelos de negócios e em uma nova cadeia e padrão de produção, nas indústrias digitais – ou no mix das tradicionais rumo à digitalização. A IoT abrirá um enorme leque de novas oportunidades para o mercado de trabalho e educação, para novas plataformas de *software*, para novas empresas e empresas maduras, que souberem transitar para novos cenários.

No entanto, assistimos nos últimos anos à criação dos Institutos SENAI de Inovação (ISI) e da Empresa Brasileira de Inovação Industrial (EMBRAPII),

2 Ver: SERTTEL. Disponível em: <http://www.serttel.com.br/>. Acesso em: 07 set. 2017.

3 Ver: OGASEC. Sobre a Aker. Disponível em: <http://www.aker.com.br/empresa/sobre-a-aker/>. Acesso em: 07 set. 2017.

4 Equipamento de rede de computadores que tem por aplicar uma política de segurança a um determinado ponto da rede. Ver: WIKIPEDIA. Firewall. Disponível em: <https://pt.wikipedia.org/wiki/Firewall>. Acesso em: 07 set. 2017.

5 Ver: MAIS QUE ÁGUA. Disponível em: <http://maisqueagua.brastemp.com.br/>. Acesso em: 07 set. 2017.

6 Ver: VAGALUME WIFI. WiFi como serviço para o seu negócio. Disponível em: <http://vagalumewifi.com.br/>. Acesso em: 07 set. 2017.

equipamentos criados para estimular a inovação na indústria tradicional, em detrimento a estímulos para fortalecer as indústrias digitais. No tocante à IoT, são ações que indicam a prioridade do MDIC, MCTIC e BNDES na direção à inovação com foco na Manufatura Avançada, ou seja, no aumento de eficiência da indústria tradicional. É o esforço Brasil para nos mantermos competitivos no cenário 1 – ver Figura 3.

Seremos mesmo capazes de criar indústrias tradicionais com capacidade de inserção em cadeias globais? Vale a pena continuar investindo nesta direção? Talvez. Mas não parece ser a nossa vocação. Com o setor de serviços no Brasil correspondendo a 72% do PIB e muitas empresas manufatureiras buscando aumentar a participação dos serviços em seus negócios (MATTOS, 2012), estimular a indústria digital no Brasil parece ser uma melhor estratégia, a estimular a indústria tradicional com novidades digitais.

Ironicamente através de parte de uma política industrial – Lei de Informática –, impulsionou-se a criação de importantes ambientes de inovação no país, fortemente voltados para a indústria digital. E como resultado, temos hoje no Brasil parques de pesquisa e inovação que cooperam com a indústria local e global, proporcionando – e exportando através dos participantes globais – soluções inovadoras construídas com conhecimento e capital humano local. Segundo Meira (2013), "o Brasil pode, sim, liderar comportamentos e mercados digitais. Nossa ligação com celulares e a propensão a aceitar e promover todo tipo de negócios e serviços digitais são um bom exemplo, assim como nosso E-COMMERCE". Mas não estamos prontos! Ainda segundo Meira, falta gente, temos poucos sistemas locais de inovação, são poucos os investimentos em inovação e empreendedorismo, nossa infraestrutura é deficiente e falta capital inteligente e conectado. Trabalhar esta lista parece ser um melhor roteiro para a formulação das novas políticas públicas rumo a uma indústria digital de inserção global.

REFERÊNCIAS

ALHA, Kati et al. Free-to-Play Games: Professionals' Perspectives. Digra Nordic '14: Proceedings of the 2014 International DiGRA Nordic Conference. Gotland, p. 1010-1010, 29 maio 2014. Disponível em: <http://www.digra.org/wp-content/uploads/digital-library/nordicdigra2014_submission_8.pdf>. Acesso em: 29 jan. 2017.

DIJKMAN, R. M. *et al.* Business models for the Internet of Things. *International Journal Of Information Management*, Eindhoven, p. 672-678, dez. 2015.

EVANS, Dave. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. 2011. Elaborada por Cisco Internet Business Solutions Group. Disponível em: <http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>. Acesso em: 29 jan. 2017.

FLEISCH, Elgar; WEINBERGER, Markus; WORTMANN, Felix. Business Models and the Internet of Things. Bosch Iot Lab White Paper, St. Gallen, p. 1-18, ago. 2014. Disponível em: <https://www.researchgate.net/publication/282572948_Business_Models_and_the_Internet_of_Things>. Acesso em: 29 jan. 2017.

GREENFIELD, Adam. *Everyware:* The Dawning Age of Ubiquitous Computing. Berkeley: New Riders, 2006.

ITF/OECD (Ed.). Urban Mobility System Upgrade: How shared self-driving cars could change city traffic. 2015. 34 p. Disponível em: <http://www.itf-oecd.org/sites/default/files/docs/15cpb_self-drivingcars.pdf>. Acesso em: 29 jan. 2017.

MAIS QUE ÁGUA. Disponível em: <http://maisqueagua.brastemp.com.br/>. Acesso em: 07 set. 2017.

MANYIKA, James; CHUI, Michael. By 2025, Internet of things applications could have $11 trillion impact. 2015. Disponível em: <http://fortune.com/2015/07/22/mckinsey-internet-of-things/>. Acesso em: 29 jan. 2017.

MATTOS, Bruno. *Impacto da servitização no modelo de negócio de empresas manufatureiras:* o caso Scania. 2012. 1010 f. Dissertação (Mestrado Profissional em Administração de Empresas, Escola de Administração de Empresas de São Paulo) – São Paulo, 2012. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/10284/Dissertacao - Bruno Lanzi de Ma>. Acesso em: 29 jan. 2017.

MEIRA, Silvio. *Novos negócios de inovadores de crescimento empreendedor no Brasil*. Rio de Janeiro: Casa da Palavra, 2013.

MOORE, Gordon. Cramming more components onto integrated circuits. Electronics, Bruxelas, p. 114-117, 19 abr. 1965. Disponível em: <http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf>. Acesso em: 29 jan. 2017.

OGASEC. Sobre a Aker. Disponível em: <http://www.aker.com.br/empresa/sobre-a--aker/>. Acesso em: 07 set. 2017.

OSTERWALDER, A.; PIGNEUR, Y. *The Business Model Generation:* a Handbook for Visionaries, Game Changers, and Challengers. Hoboken: John Wiley & Sons, 2010.

PoETAS.IT (Ed.). IoT – Uma estratégia para o Brasil 2016: consolidação de uma visão unificada para orientação e proposição de políticas sobre Internet das Coisas no Brasil. Recife, 2016. 41 p. Disponível em: <http://www.cesar.org.br/poetas.it/visionstatement>. Acesso em: 5 set. 2017.

PORTER, Michael; HEPPELMANN, James. How Smart Connected Products Are Transforming Competition. *Harvard Business Review*, 1010, v. 1010, n. 1010, p. 1010-1010, nov. 2014. Disponível em: <https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition>. Acesso em: 29 jan. 2017.

PROMON LOGICALIS (Ed.). IoT Snapshot 2016: um retrato da adoção e do potencial da Internet das Coisas no mercado brasileiro. Rio de Janeiro, 2016. 20 p. Disponível em: <http://www.br.promonlogicalis.com/globalassets/latin-america/iot-snapshot-2016_websafe.pdf>. Acesso em: 29 jan. 2017.

SERTTEL. Disponível em: <http://www.serttel.com.br/>. Acesso em: 07 set. 2017.

VAGALUME WIFI. WiFi como serviço para o seu negócio. Disponível em: <http://vagalumewifi.com.br/>. Acesso em: 07 set. 2017.

WIKIPEDIA. Firewall. Disponível em: <https://pt.wikipedia.org/wiki/Firewall>. Acesso em: 07 set. 2017.

O GÊNERO DA INTERNET DAS COISAS

BRUNA CASTANHEIRA DE FREITAS

INTRODUÇÃO

Em uma pesquisa de mercado feita pela consultoria Accenture Interactive em 2014, a respeito das tecnologias envolvendo a Internet das Coisas – do termo Internet of Things (IoT), foram divulgados alguns dados relevantes a respeito da concepção que o consumidor possui sobre esses aparatos. Feito um recorte de gênero no resultado do estudo, observou-se que (i) os homens têm o dobro de chance, em comparação às mulheres, de saberem o que é IoT, (ii) o dobro de chance de se considerarem *early adopters* da tecnologia e (iii) homens tem maior probabilidade – 16% *vs*. 10% – de já possuírem algum aparato IoT ou estarem pensando em adquirir um no próximo ano (ACCENTURE, 2014, p. 8).

Para além do mercado consumidor envolvendo IoT, vale também observar quais são as principais empresas que tem desenvolvido esta tecnologia: Amazon, Bosch, Cisco, Dell, GE, Google, Hitachi Data Systems, Huawei, IBM, AT&T, Intel, Microsoft, Oracle, PTC, Salesforce, Samsung, Siemens e Qualcomm são algumas delas (BUTLER, 2016) e, das dezoito empresas citadas, apenas uma possui CEO mulher: Ginni Rometty da IBM.

Pesquisadoras(es) tentam entender já há algum tempo o por que homens possuem maior adesão e proximidade à tecnologia do que mulheres. Gill e Grint (1995) questionam se a tecnologia é inerentemente masculina e quais tipos de pressuposições sobre gênero estão incrustadas no *design* e uso dos produtos; autoras(es) como Balsamo (1998), Burfoot (1997) e Caputi (1988) afirmam que a continuada dominância masculina sobre esse campo se deve a associação simbólica da masculinidade e tecnologia, a qual, através de imagens culturais e representações da tecnologia, convergem com o prevalecimento de representações de masculinidade e poder.

Quanto a isso, autores como Pierre Bourdieu, no livro *A Dominação Masculina* (1998) dizem que tanto o sistema de ensino quanto a cultura

originam de uma estrutura que hierarquiza o masculino em relação ao feminino, de modo que ficam configuradas dominações simbólicas permanentes, sendo reproduzidas inconscientemente nas relações sociais. Outras hipóteses (THEODORO, S.; ADAMS, M., 2016) dizem respeito a ainda predominante ideologia de que a mulher é a responsável principal pelo cuidado dos filhos e do lar, devendo deixar em segundo plano seus planos profissionais e interesses, ou então os reajustando às exigências da vida doméstica – o que geralmente implica na impossibilidade de exercer com plenitude suas ambições.

Existem também discussões a respeito da falta de incentivo para que mulheres, desde sua infância, se interessem por ciência e tecnologia, algo simbolizado, por exemplo, pelo tipo de conteúdo que é oferecido às meninas: uma socialização que envolve brinquedos que influenciam um papel social relacionado à vida doméstica, como bonecas e "casinhas", enquanto meninos são incentivados à descoberta do mundo objetivo, como com brinquedos de aventura e que envolvem mecânicas complexas (HENWOOD, 1996).

Fato é que esta problemática persiste, e não tem esboçado sinais de melhora – qual seja, a maior inclusão das mulheres no campo tecnológico tanto como entusiastas e consumidoras quanto profissionais – tão cedo. Neil Postman, na obra *Technopoly: The Surrender of Culture to Technology* (1993) já argumentava que vivemos em uma sociedade que não se limita a usar a tecnologia como um sistema de apoio, mas é moldada por ela, algo que gera consequências radicais para o significado da política, arte, educação, inteligência e até mesmo da verdade.

Caso a tecnologia tenha – *by design* – vieses de gênero, ilustra-se um cenário no qual a hierarquização do masculino sobre o feminino nas áreas tecnológicas é constantemente reforçada, de modo que a pouca diversidade de gênero se alastre cada vez mais. Também, inserir a ótica dos estudos de gênero na análise da tecnologia é algo capaz de levantar considerações a respeito do entendimento da tecnologia em si. Quanto a isso, Cockburn (1992, p. 32) afirma: "A tecnologia em si não pode ser plenamente compreendida sem referência ao gênero".[1] Assim, este artigo se propõe a analisar a inclusão da mulher no desenvolvimento da Internet das Coisas, bem como o modo como a IoT é capaz de impactar em uma maior diversidade de gênero no campo da tecnologia.

1 No original: "Technology itself cannot be fully understood without reference to gender". (tradução minha)

INTERNET DAS COISAS E AS PROBLEMÁTICAS ENVOLVENDO GÊNERO

Para realizar a presente análise, faz-se necessário especificar com qual definição de IoT o artigo trabalhará. Apesar de já ter sido anteriormente desenvolvido por outros autores,[2] esse conceito foi mais popularmente difundido pela International Telecommunication Union (ITU) em 2005, ao afirmar em um relatório que IoT é a conexão de objetos e dispositivos do cotidiano a qualquer tipo de rede. No campo da gestão e negócios, Fleisch (2010, p. 3) afirma que IoT está ligada à redução de custos de transações do "mundo real". Para ele, IoT proporciona a manutenção de sistemas de baixo custo, com dados de alta qualidade sobre o mundo físico. Assim, essa tecnologia se torna "[…] uma ferramenta que promove a forma como gerenciar organizações e sistemas complexos".[3]

Logo, tanto no campo doméstico quanto industrial, é possível imaginar diversos usos para esta tecnologia: desde o alarme que ao despertar às seis horas da manhã já se comunica com a cafeteira para preparar o café, até a fábrica que possui toda a rede de equipamentos se comunicando e se coordenando de forma autônoma. Consultorias afirmam que até 2020 o mundo terá cerca de 20.4 bilhões de coisas conectadas (GARTNER, 2017) – e caso a lacuna entre os gêneros nesse meio se mantenha, tanto o número de usuários quanto de criadores destas tecnologias será, em sua maioria, masculino.

A análise de gênero aplicada ao progresso da IoT é algo relevante de ser feito, pois é preciso avaliar se a tecnologia está se desenvolvendo de modo a atender as necessidades dos seus consumidores de forma igualitária, e também se esses aparatos estão reafirmando e perpetuando diferenciações de gênero – que são aspectos socialmente construídos (FÁVERO, 2010, p. 24). O estímulo à diversidade, em qualquer âmbito que seja, se faz de suma importância. Isso porque a criação – e aqui se destaca a tecnológica – pressupõe a circulação e debate de ideias em nível simétrico. Em um ambiente onde o conhecimento, as necessidades e as lideranças que são valorizadas são aqueles produzidas apenas por um grupo homogêneo e seleto de homens brancos, coloca-se em xeque o próprio avanço dessas tecnologias.

---

2 Ver: GERSHENFELD, N. *When Things Start to Think.* Nova York: Henry Holt, 1999; FERGUSON, G. Have your objects call my objects. *Harvard Business Review*, v. 80, n. 6, p. 138-144, 2002; WRIGHT, S.; STEVENTON, A. Intelligent Spaces - The Vision, the Opportunities and the Barriers. *BT Technology Journal*, v. 22, n. 3, p. 15-26, 2004.

3 No original: " […] a tool that advances the entire discipline of how to manage organizations and complex systems". (tradução minha)

Para exemplificar como vieses de gênero são capazes de influenciar no desenvolvimento tecnológico, tem-se a questão envolvendo algoritmos e Inteligência Artificial (I.A.). Pesquisas tem mostrado que existem vieses entranhados nos conjuntos de dados usados para ensinar habilidades de linguagem para programas de Inteligência Artificial:

> À medida que esses sistemas se tornam mais capazes e difundidos, seu ponto de vista sexista pode ter consequências negativas - por exemplo, nas buscas de trabalho. O problema resulta da forma como as máquinas são ensinadas a ler e a falar. Os cientistas da computação estão alimentando-as com enormes quantidades de linguagem escrita ou falada, e deixando-as desenhar conexões entre palavras e frases [...] Isso torna possível que uma máquina perceba conexões semânticas entre, digamos, "rei" e "rainha" e entenda que a relação entre as duas palavras é semelhante àquela entre "homem" e "mulher". Mas pesquisadores da Universidade de Boston e Microsoft Research New England também descobriram que os conjuntos de dados consideravam a palavra "programador" mais próxima da palavra "homem" do que "mulher", e que a palavra mais semelhante para "mulher" é "dona de casa" [...] Quando eles [pesquisadores] escreveram um programa projetado para ler páginas da Web e classificar sua relevância, eles descobriram que o sistema classificaria as informações sobre programadoras femininas como menos relevantes do que as suas contrapartes masculinas. (KNIGHT, 2016)

Assim, tem-se que uma vez que os programadores inserem tarefas iniciais nos programas de computador para estes realizarem, os algoritmos começam a "aprender" com aquilo que foi inserido e se desenvolvem a partir dali. Esse processo é chamado de *machine-learning* e, segundo Louridas e Ebert (2016): "No *machine-learning*, um computador primeiro aprende a executar uma tarefa, estudando um conjunto de exemplos de treinamento. O computador então executa a mesma tarefa com dados que não possuía antes".[4]

Para além do espectro envolvendo gênero, existem situações no campo tecnológico em que diferentes formas de discriminações têm se configurado: usuários descobriram que o aplicativo de fotos da Google, que aplica automaticamente legendas para as fotos inseridas nos pacotes de imagens, estava classificando imagens com pessoas negras como gorilas (BARR, 2015). Em outra situação, o programa de câmeras Nikon interpretava que pessoas asiáticas estavam piscando (LEE, 2009); e o *software* da *web* câmera da Hewlett-Packard tinha dificuldades em reconhecer pessoas com tons de pele mais escuros (CHEN, 2009).

4 No original: "In machine learning, a computer first learns to perform a task by studying a training set of examples. The computer then performs the same task with data it hasn't encountered before". (tradução minha)

Ainda, notou-se que o serviço prestado pela Amazon de entrega de encomendas no mesmo dia em que o pedido é realizado não funcionava em vizinhanças norte-americanas predominantemente negras. As áreas descriminadas eram as mesmas que foram afetadas pela crise hipotecária no meio do século 20, revelando o quanto a desigualdade sistemática é capaz de afetar a "inteligência" da tecnologia (INGOLD; SOPER, 2016). Em outra situação, pesquisadores da Carnegie Mellon University descobriram que mulheres tinham menores chances do que homens de visualizarem nos anúncios do Google ofertas de empregos que oferecessem ótimos salários (SPICE, 2015).

Também, no que se diz das vozes que são dadas para inteligências artificiais interagirem com o usuário, notou-se que geralmente quando a I.A. é criada para exercer funções de assistência – como organizar o calendário, marcar alguma reunião, encontrar algum endereço ou informação – geralmente a tecnologia ganha um nome feminino (Siri, Cortana e Alexa, por exemplo). Todavia, quando a I.A. é elaborada para exercer funções mais cognitivas, como responder dúvidas jurídicas por exemplo, é atribuído um nome masculino: é o caso da tecnologia "Ross" criada pela IBM – a mesma dona do supercomputador "Watson". Para Katherine Cross, autora do livro *An Anthropology of Robots and AI: Annihilation Anxiety and Machines*, esse cenário é um reflexo de como homens pensam sobre mulheres e que a existência de I.A. "femininas" é algo que alimenta e reforça a noção de que mulheres são naturalmente mais subservientes que os homens (LEWIS, 2015).

Todas essas situações demonstram como vieses de gênero e raciais podem ser inseridos em diversas programações de *software*, de modo que parcelas da sociedade sejam descriminadas. Em outras palavras, assim como as tecnologias anteriores, os algoritmos inseridos nas máquinas, que podem ser aparatos IoT, refletirão os valores de seus criadores e programadores. Certamente, o campo tecnológico pouco diverso nada faz além de favorecer o acontecimento de mais situações lamentáveis como essas.

Vale dizer que existem engenheiros de *software* e executivos do campo tecnológico preocupados com questões morais que envolvam suas empresas, de modo que alguns deles estão com propostas para reformular um código de ética para programadores criado em 1992. Entre as diretrizes está, por exemplo, a obrigatoriedade de que estes façam um juramento ético que guie o exercício da profissão (COREN, 2017). Todavia, na análise do documento preliminar não existe qualquer referência a questões envolvendo diversidade no corpo de funcionários das empresas ou descriminação na programação de *softwares*.[5]

5 O documento preliminar pode ser acessado em: ACM Ethics. ACM Code of Ethics and Professional Conduct. Disponível em: <https://ethics.acm.org/wp-content/uploads/2016/11/1992_and_2018Draft1_sidebyside.pdf?189db0>. Acesso em: 15 abr. 2017.

Ainda quanto a gênero, com o intuito de incentivarem a inserção de mais mulheres no campo da tecnologia, grandes empresas de tecnologia têm realizado desde 2014 levantamentos de dados em suas equipes para averiguar a quantidade de homens e mulheres contratados. Segundo Larson (2014): Facebook – 69% dos funcionários eram homens e apenas 31% mulheres; Google – 70% homens e 30% mulheres; Linkedin – 61% homens e 39% mulheres; Yahoo – 62% homens e 37% mulheres; única empresa, dentre as citadas, a possuir CEO mulher.

Todavia, passados três anos deste levantamento pouca coisa mudou. No World Economic Forum realizado em Davos em 2016, um dos relatórios –The Industry Gender Gap – revelou que as mulheres ocupam apenas 26% dos cargos no campo tecnológico (WOJCICKI, 2016). Apesar disso, empresas de tecnologia tem afirmado que não possuem problemas envolvendo diversidade no seu corpo de funcionários: 83% acham que já possuem equipes diversificadas. Talvez isso se deva ao fato de que nos últimos cinco anos várias destas empresas tenham empregado políticas internas de contratação que tentam lidar com essa questão. Mas, os resultados ainda são insuficientes e não amenizam a exclusão das mulheres do meio tecnológico (ELIAS, 2017). Ainda, empresas como HP e a IBM criaram políticas para garantir que 30% das novas contratações em áreas técnicas sejam de mulheres. Porém, é comum que as vagas não sejam preenchidas, até porque existe um número baixo de mulheres nos cursos de formação para este tipo de emprego (FELITTI, 2015).

O desenvolvimento da IoT em um cenário masculino propicia a formação de um ecossistema enviesado. Apesar de todos os dados aqui apresentados, as grandes empresas envolvidas no progresso da IoT ainda se mostram pouco diversas e estão inseridas em contextos tecnológicos que parecem pouco conscientes a respeito da gravidade do problema. Caso as lacunas de gênero em empregos no campo da tecnologia persistam, as mulheres estão sujeitas à riscos como a perda de futuras oportunidades de emprego.

No Brasil, por exemplo, segundo a Pesquisa Nacional por Amostra de Domicílio (PNAD) de 2015, realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), as mulheres ocupam apenas 20% dos cargos na área tecnológica. E, mesmo possuindo maior escolaridade que homens, as profissionais de tecnologia no Brasil ganham 30% a menos do que eles. Ainda, apenas 17% das programadoras são mulheres (CASTRO, 2013).

O cenário no qual predominantemente homens produzem tecnologia e homens a consomem, levam autoras como Faulkner, já em 2001 (p. 89), a afirmar que:

I. a tecnologia possui gênero, pois os autores-chaves dos sistemas são, predominantemente, homens;

II. existem fortes divisões de gênero nos empregos do campo tecnológico, devido a associação feita entre masculinidade e habilidades técnicas;

III. imagens culturais da tecnologia são fortemente associadas com a masculinidade hegemônica; e

IV. a tecnologia é um elemento importante na identidade de gênero dos homens que trabalham com tecnologias. A partir disso, a autora ainda afirma (p. 90) que gênero é uma parte integral da formatação social da tecnologia e que "Nós não podemos transformar relações de gênero sem nos envolver em tecnologia".[6]

CONSIDERAÇÕES FINAIS

O presente artigo se ocupou em delinear as preocupações envolvidas em relação a questões de gênero em um campo com grande predominância masculina. A presença de mulheres é bastante inferior à dos homens em qualquer área do ecossistema envolvendo o campo tecnológico: existem poucas mulheres que estudam para se tornar profissionais nas áreas, poucas que estão empregadas, poucas que produzem esse tipo de tecnologia e, se comparadas aos homens, poucas que se interessam – ou que são estimuladas a se interessar – pela tecnologia em si.

No campo específico dos algoritmos e I.A., tem-se que caso as discriminações de gênero não comecem desde cedo a serem questionadas, elas fatalmente se tornarão parte da lógica dos algoritmos mais comumente utilizados e usados em *machine-learning*, sendo apenas mais uma forma de reprodução de preconceitos e afirmação de práticas sexistas e contrárias à diversidade. Reforça-se a importância da discussão do tema, especialmente no campo da IoT que se mostra em ascensão e pouco diversificado. É necessário um ambiente no qual ideias e criações oriundas dos mais diversos interlocutores possam circular com a mesma simetria para que o desenvolvimento democrático possa ser produzido; caso um grupo seleto se aproprie dessa circulação, invariavelmente aquilo que é gerado, consumido e ditado como tendência se torna produto daquele ponto de visto homogêneo. Desse modo, as ideias e criações que poderiam provocar rupturas correm um maior risco de serem deslegitimadas, algo que gera a construção de conhecimentos, práticas e produtos enviesados.

6 No original: "We cannot transform gender relations without engaging in technology".

REFERÊNCIAS

ACCENTURE INTERACTIVE. The Internet of Things: The Future of Consumer Adoption. Disponível em: <https://www.accenture.com/t20150624T211456__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf>. Acesso em: 15 abr. 2017.

ACM Ethics. ACM Code of Ethics and Professional Conduct. Disponível em: <https://ethics.acm.org/wp-content/uploads/2016/11/1992_and_2018Draft1_sidebyside.pdf?189db0>. Acesso em: 15 abr. 2017.

BALSAMO, Anne. *Technologies of the Gendered Body:* Reading Cyborg Women. Durham: Duke University Press, 1998.

BARR, Alistair. Google Mistakenly Tags Black People as 'Gorillas,' Showing Limits of Algorithms. Disponível em: <https://blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/>. Acesso em: 15 abr. 2017.

BOURDIEU, Pierre. *A dominação masculina*. 2. ed. Rio de Janeiro: Bertrand, 1998.

BURFOOT, Annette. Through the eyes of Mary: Maternity and Modernity in Italy Canadian Women's Studies. *Les Cahiers de la Femme*, v. 18, n. 4, p. 32-38, 1997.

BUTLER, Brandon. Most powerful Internet of Things companies. Disponível em: <http://www.networkworld.com/article/2287045/wi-fi/wireless-153629-10-most-powerful-internet-of-things-companies.html#slide19>. Acesso em: 15 abr. 2017.

CAPUTI, Jane. Seeing elephants: The myths of phallotechnology. *Feminist Studies*, v. 14, n. 3, p. 487-524, 1988.

CASTRO, Bárbara. *Afogados em contratos:* o impacto da flexibilização do trabalho nas trajetórias dos profissionais de TI. 2013.Tese (Doutorado em Ciências Sociais) – Universidade Federal de Campinas, Campinas, 2013.

CHEN, Brian. HP Investigates Claims of 'Racist' Computers. Disponível em: <https://www.wired.com/2009/12/hp-notebooks-racist/>. Acesso em: 15 abr. 2017.

COCKBURN, Cynthia. *Machinery of dominance***:** Women, men and technical know-how. London: Pluto, 1985.

COREN, Michael. Silicon Valley's finest are finally developing a code of ethics. Disponível em: <https://qz.com/964159/the-president-of-y-combinator-sam-altman-is-leading-an-effort-to-develop-a-code-of-ethics-for-silicon-valley-in-response-to-president-donald-trump/>. Acesso em: 15 abr. 2017.

ELIAS, Jennifer. Silicon Valley still doesn't think it has a diversity problem, survey shows. Disponível em: <http://www.bizjournals.com/sanjose/news/2017/03/23/silicon-valley-tech-diversity.html>. Acesso em: 15 abr. 2017.

FAULKNER, Wendy. The technology question in feminism: a view from feminist technology studies. *Women's Studies International Forum*, v. 24, n. 1, p. 79–95, 2001.

FÁVERO, Maria Helena. *Psicologia do gênero:* psicobiografia, sociocultura e transformações. Curitiba: UFPR, 2010.

FELITTI, Guilherme. Por que há menos mulheres no setor de tecnologia? Disponível em: <http://epocanegocios.globo.com/Informacao/Dilemas/noticia/2015/08/por-que-ha-menos-mulheres-no-setor-de-tecnologia.html>. Acesso em: 15 abr. 2017.

FERGUSON, G. Have your objects call my objects. *Harvard Business Review*, v. 80, n. 6, p. 138–144, 2002.

FLEISCH, Elgar. What is the internet of things? An economic perspective. *Economics, management, and financial markets*, v. 5, n. 2, p. 125-157, 2010.

GARTNER. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Disponível em: <http://www.gartner.com/newsroom/id/3598917>. Acesso em: 15 abr. 2017.

GERSHENFELD, N. *When Things Start to Think.* Nova York: Henry Holt, 1999.

GRINT, Keith; GILL, Ros. *The gender-technology relation:* Contemporary theory and research. London: Taylor and Francis, 1995.

HENWOOD, Flis. (1996). Wise choices? Understanding occupational decision-making in a climate of equal opportunities for women in science and technology. *Gender and Education*, v. 8, n. 2, p. 199-214, 1996.

INGOLD, David; SOPER, Spencer. Amazon Doesn't Consider the Race of Its Customers. Should It? Disponível em: <https://www.bloomberg.com/graphics/2016-amazon-same-day/>. Acesso em: 15 abr. 2017.

ITU (2005). Internet reports – The internet of things. Disponível em: <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>. Acesso em: 15 abr. 2017.

KNIGHT, Will. Como corrigir algoritmos sexistas do Vale do Silício. Disponível em: <http://www.technologyreview.com.br/read_article.aspx?id=52451>. Acesso em: 15 abr. 2017.

LARSON, Selena. A Quick Survey Of Tech Giants Reaffirms Just How White And Male They Are. Disponível em: <http://readwrite.com/2014/06/26/google-facebook-yahoo-women-ethnic-diversity/>. Acesso em: 15 abr. 2017.

LEE, Odelia. Camera Misses the Mark on Racial Sensitivity. Disponível em: <http://gizmodo.com/5256650/camera-misses-the-mark-on-racial-sensitivity>. Acesso em: 15 abr. 2017.

LEWIS, Tanya. Rise of the fembots: why artificial intelligence is often female. Disponível em: <http://www.livescience.com/49882-why-robots-female.html>. Acesso em: 15 abr. 2017.

LOURIDAS, Panos; EBERT, Christof. Machine Learning. *IEEE Software*, v. 33, n. 5, p. 110-115, 2016.

POSTMAN, Neil. Technopoly**:** The Surrender of Culture to Technology. Nova York: Vintage Books, 1993.

SPICE, Byron. Questioning the fairness of targeting ads online. Disponível em: <http://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html>. Acesso em: 15 abr. 2017.

THEODORO, S.; ADAMS, M. O impacto das políticas públicas para as mulheres na promoção da igualdade de gênero. *Revista Gênero*, v. 17, n. 1, p. 191-213, 2016.

WOJCICKI, Susan. Closing the Tech Industry Gender Gap. Disponível em: <http://www.huffingtonpost.com/susan-wojcicki/tech-industry-gender-gap_b_9089472.html>. Acesso em: 15 abr. 2017.

WRIGHT, S.; STEVENTON, A. Intelligent Spaces - The Vision, the Opportunities and the Barriers. *BT Technology Journal*, v. 22, n. 3, p. 15-26, 2004.

O VIÉS EM *MACHINE LEARNING*: PERSPECTIVAS REGULATÓRIAS

HELENA FERREIRA MATOS

O VIÉS EM *MACHINE LEARNING*

Machine learning se tornou um dos termos mais populares na indústria da tecnologia nos últimos anos. O método – subcategoria dos estudos em inteligência artificial – representa a aplicação de um processo estatístico que se inicia com um corpo de dados e procura derivar, a partir deles, uma regra ou procedimento que possa explicar a sua incidência ou prever padrões futuros de ocorrência (LEGG; HUTTER, 2007; RUSSELL; NORVIG, 1995).

Para implementar a técnica, começa-se com um conjunto de dados de treinamento – *training set* – e outro de teste – *test set*. Elege-se, então, uma estrutura matemática que categorizará uma gama de possíveis regras para a tomada de decisões, com parâmetros ajustáveis com base nos dados de que dispõe. É, ademais, definida uma função objetiva, utilizada para avaliar a conveniência do resultado originado a partir de uma determinada seleção de parâmetros. Essa função costuma recompensar o modelo pelo uso de regras mais simples, bem como pelo alcance de resultados que se assemelhem aos dados de treinamento disponibilizados (UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2016, p. 9).

O treinamento do modelo criado significa a realização de ajustes nos seus parâmetros, de modo que a função a que se faz referência é maximizada, e os melhores resultados possíveis são alcançados. O conjunto de dados de teste serve para avaliar a precisão e eficiência do modelo treinado, objetivando que ele se torne capaz de generalização e aplicabilidade em relação não apenas aos dados de treinamento e de teste, mas também a dados futuros da forma mais precisa e correta possível (UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2016, p. 9; JAQUITH *et al.*, 2017).

De forma geral, a aplicação de técnicas de *machine learning* em processos decisórios tem como objetivo promover eficiência e imparcialidade, pelo uso de mecanismos automatizados supostamente menos vulneráveis aos vieses que são comuns nas relações sociais. No entanto, a implementação desse tipo de sistema não está livre de riscos.

De aplicativos de reconhecimento de imagens que caracterizam pessoas negras como gorilas (DOUGHERTY, 2015) a *chatbots* que exprimem mensagens abertamente racistas (ALBA, 2017), sistemas de aprendizagem automática têm, com frequência, demonstrado comportamentos nocivos. É que a criação dos modelos se dá com base nos dados disponibilizados em etapas anteriores ao momento de tomada de decisão. Se os dados utilizados para o treinamento forem dotados de vieses, a máquina os aprenderá e replicará.

Essas distorções podem ser produzidas, em primeiro lugar, em razão do uso de dados não representativos para treinar um algoritmo. Obter acesso a quantidades massivas de dados é tarefa difícil, e muitas vezes envolve o dispêndio de muitos recursos, de modo que os responsáveis pelo treinamento de sistemas costumam utilizar informações que já estão mais facilmente acessíveis (LEVENDOWSKI, 2017). Além disso, desvios podem ocorrer se os dados são coletados de determinados grupos e não de outros: a exclusão de certos conjuntos de informações nesse processo de seleção inicial pode ocasionar que o programa perca parte do que poderia saber (CAMPOLO *et al*, 2017). A isso se soma, ainda, o problema de que os *datasets* podem ser construídos de forma não transparente (ATTENBERG, 2011), com o uso de códigos tratados como "caixas pretas" (PASQUALE, 2015), o que dificulta a verificação de suas características e potenciais defeitos.

Outro problema envolve o fato de que boa parte dessas informações têm de ser previamente classificadas por humanos, para que componham os dados de treinamento, o que muitas vezes implica também a transmissão dos vieses embutidos nessas escolhas iniciais realizadas por pessoas para o sistema algorítmico, ainda que de forma não intencional (CAMPOLO *et al.*, 2017, p. 15). Assim, padrões discriminatórios podem ser reproduzidos com a aplicação do programa. Como afirmou o relatório de Stanford de 2016 (STANFORD UNIVERSITY, 2016), sobre Inteligência Artificial:

> As aplicações de IA e os dados em que se baseiam podem refletir os preconceitos de seus criadores e usuários, que especificam as fontes de dados. Isso ameaça aprofundar os preconceitos sociais existentes e concentrar os benefícios da IA de forma desigual entre os diferentes subgrupos da sociedade. Por exemplo, algumas tecnologias de reconhecimento de fala não funcionam bem para mulheres e pessoas com sotaques. À medida que

> a AI é cada vez mais utilizada em aplicações críticas, esses vieses podem fazer emergir questões de equidade a grupos diversos em sociedade [...].[1]

A confiança em dados é também um problema de muitos sistemas de algoritmos (O'NEIL, 2016). Existe a possibilidade de que esses programas "herdem os preconceitos de tomadores de decisão anteriores" (BAROCAS; SELBST, 2016, p. 674). Ou seja, se no passado havia vieses, esses programas irão mantê-los vivos ao reproduzi-los. Nesse sentido se posicionam Barocas e Selbst:

> [...] (1) se a mineração de dados tratar casos em que o preconceito tenha desempenhado algum papel como exemplos válidos para o aprendizado, essa regra pode simplesmente reproduzir o preconceito envolvido nesses casos anteriores; ou (2) se a mineração de dados realiza inferências a partir de uma amostra enviesada da população, qualquer decisão que recaia sobre essas inferências pode prejudicar sistematicamente aqueles que estão sub ou sobre-representados no conjunto de dados. Ambos podem afetar o conjunto de dados de formas que levam à discriminação [...]
> [...] onde a mineração de dados é adotada e aplicada sem cuidado, ela introduz sérios riscos de reproduzir muitas das mesmas dinâmicas problemáticas que permitiram que a discriminação persistisse na sociedade, mesmo na ausência de preconceito consciente (BAROCAS; SELBST, 2016, p. 674).[2]

Dessa forma, os dados podem refletir vieses que persistem na sociedade, e a sua análise pode descobrir e reproduzir padrões de exclusão e desigualdade. Ainda, essa preocupação tende a se agravar conforme a implementação de sistemas de Inteligência Artificial avança em diferentes áreas, muitas vezes substituindo atores humanos e métodos burocráticos, permitindo

1 No original: "[...] AI applications and the data they rely upon may reflect the biases of their designers and users, who specify the data sources. This threatens to deepen existing social biases, and concentrate AI's benefits unequally among different subgroups of society. For example, some speech recognition technologies do not work well for women and people with accents. As AI is increasingly used in critical applications, these biases may surface issues of fairness to diverse groups in society [...]." (tradução minha)

2 No original: "[...] (1) if data mining treats cases in which prejudice has played some role as valid examples to learn from, that rule may simply reproduce the prejudice involved in these earlier cases; or (2) if data mining draws inferences from a biased sample of the population, any decision that rests on these inferences may systematically disadvantage those who are under- or overrepresented in the dataset. Both can affect the training data in ways that lead to discrimination [...] where data mining is adopted and applied without care, it poses serious risks of reproducing many of the same troubling dynamics that have allowed discrimination to persist in society, even in the absence of conscious prejudice." (tradução minha)

que programas de computador interfiram em diversos aspectos da vida das pessoas (UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2016, p. 2). Quando esse tipo de tecnologia é utilizado para informar decisões em áreas sensíveis, como governo, serviços públicos, emprego ou justiça criminal, o problema do viés é ainda mais pronunciado. As instituições que operam nesses campos são responsáveis por fazer escolhas críticas que afetam severamente o interesse público e os direitos mais básicos das pessoas, e os resultados injustos decorrentes de processos discriminatórios podem ter graves consequências para indivíduos e comunidades.

PERSPECTIVAS REGULATÓRIAS E GOVERNANÇA

Parece claro que a Inteligência Artificial é uma tecnologia transformadora, com potencial para desafiar muitos aspectos regulatórios em curto, médio e longo prazo. Como o direito e a elaboração de políticas públicas poderão se adaptar aos avanços nesse campo irá depender de uma grande variedade de fatores sociais, culturais e econômicos, e é provável que diferentes jurisdições chegarão a conclusões diversas sobre o seu desenvolvimento (STANFORD UNIVERSITY, 2016, p. 45). Sobre a questão específica do viés algorítmico, como afirmaram Barocas e Selbst:

> [a]bordar as fontes desta discriminação não intencional e remediar as deficiências correspondentes na lei será difícil tecnicamente, difícil legalmente e difícil politicamente. Há uma série de limites práticos para o que pode ser realizado computacionalmente. Por exemplo, quando a discriminação ocorre porque os dados que estão sendo minados são em si mesmos um resultado da discriminação intencional passada, muitas vezes não existe um método óbvio para ajustar os dados históricos para livrá-lo dessa mancha. As medidas corretivas que alteram os resultados da mineração de dados depois de concluída adentrariam em terreno legal e politicamente controverso. Esses desafios para reforma colocam em evidência as duas principais teorias subjacentes ao direito antidiscriminatório: anticlassificação e antisubordinação. Encontrar uma solução para o impacto discrepante dos dados massivos exigirá mais do que os melhores esforços para eliminar o preconceito e o viés; exigirá um reexame completo dos significados de "discriminação" e "imparcialidade" (BAROCAS; SELBST, 2016, p. 671).[3]

3 No original: "Addressing the sources of this unintentional discrimination and remedying the corresponding deficiencies in the law will be difficult technically, difficult legally, and difficult politically. There are a number of practical limits to what can be accomplished computationally. For example, when discrimination occurs because the data being mined is itself a result of past intentional discrimination, there is frequently no obvious method to adjust historical data to rid it of this taint. Corrective

Tanto o setor privado quanto a academia e governos vêm desenvolvendo algumas iniciativas para estabelecer um diálogo quanto ao estudo da ética no uso de algoritmos de *machine learning*. Nesses estudos, apontam-se orientações para a criação de uma estrutura de implementação desses sistemas.

Em primeiro lugar, o poder estatal deve monitorar a segurança e justiça na implementação desses programas, conforme são desenvolvidos, e adaptar seus arcabouços regulatórios para que se possa promover a inovação enquanto se busca proteger o público de possíveis impactos negativos. Essa atuação deve envolver o fomento de pesquisas na área, a aplicação de sistemas direcionados ao interesse público, e a formação de profissionais capacitados de origens e perfis diversos (UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2016, p. 39).

Ademais, há a preocupação de que as tecnologias no ramo da Inteligência Artificial sejam desenvolvidas de forma a serem governáveis, abertas, transparentes e compreensíveis. Elas devem ser capazes de funcionar de forma eficiente com o público, mantendo o respeito aos valores estabelecidos em sociedade (UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2016, p. 39). Além disso, devem ser desenvolvidos planos de ação para que se incremente a diversidade dos ingressantes no mercado de trabalho nesse campo, incluindo pesquisadores e especialistas (UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2016, p. 28).

Também é necessário incentivar o estabelecimento de padrões de dados abertos em Inteligência Artificial, promovendo o uso de boas práticas nesse sentido não somente pela Administração Pública, como também pela academia e pelo setor privado (UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2016, p. 40). Ademais, deve-se buscar combinar a experiência de profissionais de diferentes áreas para a criação de mecanismos regulatórios eficientes, a partir de uma perspectiva interdisciplinar que inclua especialistas técnicos e também experts em regulação (UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2016, p. 40).

---

measures that alter the results of the data mining after it is complete would tread on legally and politically disputed terrain. These challenges for reform throw into stark relief the tension between the two major theories underlying antidiscrimination law: anticlassification and antisubordination. Finding a solution to big data's disparate impact will require more than best efforts to stamp out prejudice and bias; it will require a wholesale reexamination of the meanings of 'discrimination' and 'fairness.'" (tradução minha)

Os responsáveis pela elaboração de políticas regulatórias podem estabelecer um ciclo benéfico de *accountability* interna e externa, que favoreça a transparência e a capacitação (STANFORD UNIVERSITY, 2016, p. 49). A elaboração de políticas nesse campo deve levar em conta a capacidade de se apoiar o desenvolvimento dessas tecnologias e a distribuição dos seus benefícios de forma equânime. Ademais, como os efeitos da implementação desses sistemas não são facilmente previsíveis, essas políticas terão de ser constantemente reavaliadas, a partir do seu contexto social. Especialmente em áreas como a saúde, educação e transporte, os programas devem ser introduzidos de forma a criar confiança e proteger direitos fundamentais. Certamente, esse processo envolve a consideração das implicações éticas, de privacidade, e de segurança de sua utilização, para que a ampliação do uso desse tipo de *software* se dê de forma mais justa.

As escolhas que envolvem ganhos e perdas entre o objetivo de promover a inovação tecnológica e regular a matéria, por razões de segurança e proteção de direitos, são extremamente difíceis. No mínimo, as entidades regulatórias necessitarão de funcionários com expertise no campo para que se possa compreender adequadamente as implicações dos padrões estabelecidos pelos pesquisadores, governos e pela indústria (STANFORD UNIVERSITY, 2016, p. 45).

Autores como Campolo *et al.* (2017) sugerem que, antes de lançar sistemas de Inteligência Artificial, as empresas devem realizar testes rigorosos para garantir que eles não amplificarão vieses e erros em razão de problemas com os dados de treinamento ou outros elementos do projeto. Os métodos para tanto devem ser documentados e disponibilizados publicamente, com espaço para revisões e atualizações. Além disso, as empresas devem continuar a monitorar o funcionamento desses programas em diferentes contextos e comunidades após o seu lançamento, a partir de metodologia que também deve ser definida a partir de processos abertos. A esse respeito, especial atenção deve ser concedida às perspectivas e experiências de comunidades tradicionalmente marginalizadas (CAMPOLO *et al.,* 2017).

Para compreender e fiscalizar problemas relativos à manutenção de vieses e desvios na aplicação desses sistemas, devem ser desenvolvidos padrões para rastrear a origem e uso dos dados de treinamento, durante todo o deu ciclo de vida. Essa atividade deve, ainda, ser acompanhada de um exame contínuo dos conjuntos de dados existentes, e da tentativa de compreensão dos potenciais pontos cegos que já podem estar aí presentes. Ademais, a pesquisa sobre vieses nesse tipo de *software*, bem como o estudo das estratégias para sua mitigação, não deve ser limitada a uma abordagem técnica: para que se assegure o tratamento igualitário em contextos sociais complexos, será necessária colaboração interdisciplinar (CAMPOLO *et al.,* 2017).

É importante, também, que empresas, universidades e outros *stakeholders* que atuam no âmbito dos estudos em Inteligência Artificial divulguem informações sobre a participação de mulheres, minorias e outros grupos vulneráveis nesse campo. Esse esforço deve ser acompanhado pela criação de uma cultura mais inclusiva nos espaços da pesquisa e trabalho em tecnologia. A indústria deve contratar *experts* de outras áreas do conhecimento, além das técnicas, e garantir que eles tenham poder decisório: cientistas sociais, juristas e outros especialistas são essenciais para guiar a implementação desses programas em sistemas sociais historicamente estabelecidos. Por fim, os códigos de ética criados para o desenvolvimento e aplicação de *software* de Inteligência Artificial deve ser acompanhado de fiscalização e de mecanismos eficazes de *accountability* (CAMPOLO *et al.,* 2017).

CONCLUSÕES

Nos últimos anos, sistemas de *machine learning* têm sido cada vez mais utilizados para informar processos de tomada de decisão. A técnica detecta padrões estatísticos em conjuntos de dados de treinamento, a fim de determinar o comportamento do *software*. Se por um lado se alega que esses programas ajudam a promover a eficiência e a imparcialidade, por representarem mecanismos aparentemente menos vulneráveis aos vieses que permeiam as relações sociais, por outro, eles também não estão livres destes.

O viés algorítmico com frequência decorre da má-qualidade dos dados de treinamento. Se o critério utilizado pelo algoritmo para orientar sua atividade é derivado de inferências estatísticas extraídas do conjunto de informações que lhe é dado, não há dúvida de que os problemas nos conjuntos de dados podem levar a uma implementação problemática da tecnologia. Assim, os algoritmos de aprendizado são capazes de refletir padrões discriminatórios, que decorrem principalmente de preconceitos sociais pré-existentes que foram realizados nos dados utilizados para o treinamento.

Além disso, quando esse tipo de tecnologia é utilizado para informar decisões em áreas sensíveis, como governo, serviços públicos, emprego ou justiça criminal, o problema do viés é ainda mais pronunciado. As instituições que operam nesses campos são responsáveis por fazer escolhas críticas que afetam severamente o interesse público e os direitos mais básicos das pessoas. A discriminação leva a resultados injustos e, nesses casos, qualquer falha pode ter graves consequências para indivíduos e comunidades.

Portanto, para enfrentar os novos desafios apresentados com a introdução de algoritmos em processos de tomada de decisão, é necessária a criação de políticas de governança e regulação para o desenvolvimento e implementação de sistemas de *machine learning*. Sobretudo, deve-se promover o amplo debate sobre os métodos utilizados, a transparência no emprego dos algoritmos, *accountability* dos responsáveis pela criação dos sistemas e um sistema de proteção aos afetados pelas novas tecnologias, com a adoção de estratégias de mitigação dos riscos nocivos da sua implementação.

REFERÊNCIAS

ALBA, Davey. It's Your Fault Microsoft's Teen Ai Turned into Such a Jerk. Wired, 25 mar. 2016. Disponível em: <https://www.wired.com/2016/03/fault-microsofts--teen-ai-turned-jerk/>. Acesso em: 21 out. 2017.

ATTENBERG, Josh *et al.* Selective Data Acquisition for Machine Learning. Cost-sensitive Machine Learning, 2011. p. 101-155. Disponível em: <https://pdfs.semanticscholar.org/4c29/940ef7665ed5a6d9be72260eba488473461d.pd>. Acesso em: 4 nov. 2017.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. *California Law Review*, v. 104, 2016. p. 671, 674, 681 e 732. Disponível em: <https://pdfs.semanticscholar.org/1d17/4f0e3c391368d0f3384a144a6c7487f2a143.pdf>. Acesso em: 4 nov. 2017.

CAMPOLO *et al.* AI Now 2017 Report. p. 1-2. Disponível em: <https://assets.contentful.com/8wprhhvnpfc0/1A9c3ZTCZa2KEYM64Wsc2a/8636557c5fb-14f2b74b2be64c3ce0c78/_AI_Now_Institute_2017_Report_.pdf>. Acesso em: 26 out. 2017.

DOUGHERTY, Conor. Google Photos Mistakenly Lables Black People 'Gorillas'. The New York Times, 1 jul. 2015. Disponível em: <https://bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas/?_r=1>. Acesso em: 21 out. 2017.

JAQUITH, Todd *et al.* Understanding Machine Learning, Futurism. Disponível em: <https://futurism.com/images/understanding-machine-learning-infographic/>. Acesso em: 3 nov. 2017.

LEGG, Shane; HUTTER, Marcus. Universal Intelligence: A Definition of Machine Intelligence. *Minds and Machines*, v. 17, n. 4, p. 391-444, 2007. Disponível em: <https://arxiv.org/pdf/0712.3329.pdf>. Acesso em: 29 out. 2017.

LEVENDOWSKI, Amanda. How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem. Washington Law Review, Forthcoming. p. 27. Disponível em: <https://ssrn.com/abstract=3024938>. Acesso em: 4 nov. 2017.

O'NEIL, Cathy. *Weapons of Math Destruction:* How Big Data Increases Inequality and Threatens Democracy. Nova York: Crown, 2016.

PASQUALE, Frank. *The black box society:* The secret algorithms that control money and information. Cambridge, EUA: Harvard University Press, 2015.

RUSSELL, Stuart; NORVIG, Peter. *Artificial Intelligence:* A Modern Approach. Englewood Cliffs: Prentice-Hall, 1995.

STANFORD UNIVERSITY. Artificial Intelligence And Life In 2030: One Hundred Year Study On Artificial Intelligence (AI100) Report, 2016. p. 45-49. Disponível em: <https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf>. Acesso em: 4 nov. 2017.

UNITED STATES NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Preparing for the Future of Artificial Intelligence, 2016. p. 2-40. Disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf>. Acesso em: 29 out. 2017.

SOBRE A ÉTICA HUMANA E A ÉTICA DOS ALGORITMOS

RENATO ROCHA SOUZA

Um dos poucos pontos em que concordam a grande maioria das análises contemporâneas sobre a sociedade diz respeito aos excessos informacionais e as tecnologias que os promovem. As últimas décadas nos trouxeram a internet, a *web*, as redes sociais, impulsionadas pelos dispositivos móveis e a Internet das Coisas. Se pensarmos a relação da sociedade com estes estoques de informações disponíveis, poderíamos imaginar processo inegável de democratização, tanto pela maior disponibilidade e acesso aos meios de comunicação, através da popularização das tecnologias; quanto pelo alcance a uma gama mais significativa e diversificada da produção cultural da humanidade. Tal panorama, em tese dificultaria o controle das informações, pois as fontes hoje são tantas e tão variadas que os vieses deveriam ser mais explícitos e facilmente contornáveis. Paradoxalmente, é cada vez mais complexo estabelecer parâmetros para julgamento da qualidade da informação, exatamente porque nenhuma amostra é mais significativa diante do todo, e o fenômeno da rápida obsolescência torna o conhecimento produzido cada vez mais datado. Paralelamente, as bolhas e os silos, advindos da manipulação das informações, produzem e multiplicam sociedades fragmentadas em termos de ideias e valores, um tanto amortecidas e passivamente acríticas sobre as grandes discussões em curso, sobre as consequências dos caminhos sendo desenhado, que se dão em metiês altamente seletivos, distantes dos indivíduos comuns. Sujeitas às manipulações midiáticas, às guerras de narrativas e ao fenômeno da "pós-verdade", percebemos um contexto que se assemelha a uma mistura de aspectos de duas distopias, *O admirável mundo novo*, de Huxley, e *1984*, de Orwell.

Em seu livro *As consequências da modernidade*, Giddens já apontava a confiança nos sistemas especialistas como uma características distintiva da alta modernidade. Em termos de comportamento, a ubiquidade da rede e a característica pervasiva de seus produtos em nossas vidas têm moldado a sociedade e instilado a necessidade de conexão permanente. O

entretenimento é baseado em tecnologias de *streaming*,[1] constantemente obrigando à reinvenção dos modelos de negócios dos canais tradicionais.[2] Os repositórios de informações são digitais. A mobilidade urbana depende de sistemas de navegação, GPSs e de informações capturadas pelo uso coletivo dos próprios sistemas, como o Waze. A gestão de cidades inteligentes engendra monitoramento permanente de transporte público, acompanhamento de eventos com câmeras e drones e o uso de *smart grids* para gestão e distribuição de energia.[3] A comunicação entre indivíduos é fluida em uma miríade de canais que competem entre si, acoplados às redes sociais. A medicina se baseia em imagens e mensurações para diagnósticos cada vez mais precisos[4], e a estes, somam-se os algoritmos capazes de prever doenças com mais acurácia que os médicos.[5] E estamos assistindo apenas o começo. O fato de participarmos desta época é suficiente para que soframos constante vigilância, através de câmeras, sensores e o monitoramento dos dados que produzimos diariamente, seja em redes sociais, ou através do uso dos dispositivos conectados à Internet das coisas (IoT). Neste caso, violenta-se o conceito de privacidade, através de cláusulas em letras minúsculas[6] nos termos de uso de produtos e serviços.[7]

---

1 PWC. Streaming the Future. Disponível em: <http://www.pwc.com/us/en/industry/entertainment-media/publications/assets/pwc-streaming-the-future-february-2016.pdf>. Acesso em: 12 set. 2017.

2 WAGNER, Kurt. How the NFL juggles the future of streaming, the decline of TV, and billions of dollars. Disponível em: <https://www.recode.net/2017/5/1/15386694/nfl-live-stream-amazon-prime-thursday-night-football-ratings>. Acesso em: 12 set. 2017.

3 SCIENTIFIC AMERICAN. What Is the Smart Grid? 10 maio 2010. Disponível em: <https://www.scientificamerican.com/report/smart-electricity-grid/>. Acesso em: 12 set. 2017.

4 MIT TECHNOLOGY REVIEW. The Future of Medical Visualisation. Disponível em: <https://www.technologyreview.com/s/428134/the-future-of-medical-visualisation/>. Acesso em: 12 set. 2017.

5 MURPHY, Kate. One Day, a Machine Will Smell Whether You're Sick. The New York Times, 1 maio 2017. Disponível em: <https://www.nytimes.com/2017/05/01/health/artificial-nose-scent-disease.html>. Acesso em: 12 set. 2017.

6 HESS, Amanda. How Privacy Became a Commodity for the Rich and Powerful. The New York Times, 9 maio 2017. Disponível em: <https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html>. Acesso em: 12 set. 2017.

7 FREE DOCUMENTARIES. Terms and Conditions May Apply. Disponível em: <https://freedocumentaries.org/documentary/terms-and-conditions-may-apply>. Acesso em: 12 set. 2017.

Alimentada pelos excessos informacionais, necessários para alimentar algoritmos preditivos, surge recrudescida, após um aparente fracasso nos anos 1980, a inteligência artificial.[8] É fato evidente que suas tecnologias e artefatos derivados têm revolucionado a vida humana;[9] uma revolução silenciosa, que acontece na medida em que estes dispositivos se integram e interagem,[10] de forma invisível em nosso dia a dia. Sua "inteligência" reside em supercomputadores nas nuvens, mas também em dispositivos prosaicos, como telefones celulares, relógios de pulso, televisões domésticas, geladeiras e brinquedos infantis.[11] Cada vez mais integrados ao nosso fazer cotidiano, assistimos ao poder dos algoritmos aprendendo nossos hábitos[12] e ditando o preço dos produtos no comércio eletrônico,[13] sugerindo o

8 MORAVEC, Hans. Rise of the Robots--The Future of Artificial Intelligence. Scientific American, 23 mar. 2009. Disponível em: <https://www.scientificamerican.com/article/rise-of-the-robots/>. Acesso em: 12 set. 2017.

9 LABS, Mate. Why do we need the Democratization of Machine Learning? Start Up Grind, 27 abr. 2017. Disponível em: <https://medium.com/startup-grind/why-do-we-need-the-democratization-of-machine-learning-80104e43c76f>. Acesso em: 12 set. 2017.

10 WHITTAKER, Zack. Hundreds of privacy-invading apps are using ultrasonic sounds to track you. ZD Net, 3 maio 2017. Disponível em: <http://www.zdnet.com/article/hundreds-of-apps-are-using-ultrasonic-sounds-to-track-your-ad-habits/>. Acesso em: 12 set. 2017.

11 FREYTAS-TAMURA, Kimiko. The Bright-Eyed Talking Doll That Just Might Be a Spy. The New York Times, 17 fev. 2017. Disponível em: <https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html>. Acesso em: 12 set. 2017.

12 AMAZON. The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World. Disponível em: <https://www.amazon.com/The-Master-Algorithm-Ultimate-Learning/dp/0465065708>. Acesso em: 12 set. 2017.

13 USSEM, Jerry. How Online Shopping Makes Suckers of Us All. The Atlantic, maio 2017. Disponível em: <https://www.theatlantic.com/magazine/archive/2017/05/how-online-shopping-makes-suckers-of-us-all/521448/>. Acesso em: 12 set. 2017.

que devemos assistir,[14] comer,[15] comprar[16] e para onde viajar. Assistentes pessoais nos ajudam a locomover-nos,[17] a buscar informações – muitas vezes decidindo[18] o que devemos ou não ler.[19] Por vezes, ocupam espaços afetivos,[20] e logo deixarão o teste de Turing[21] para trás como um dos desafios de tempos mais românticos, em que os humanos ainda costumavam competir com máquinas em jogos como Trívia, Poker, Xadrez ou GO.[22]

Na medida em que estes dispositivos "artificialmente sencientes" ganham espaço, podemos desenhar cenários que paulatinamente abandonam o campo da ficção científica.[23] Temos de volta a figura dos robôs, muito presentes no imaginário coletivo daqueles que viveram na década de 1970; o

---

14 VAN BUSKIRK, Eliot. HOW THE NETFLIX PRIZE WAS WON. Wired, 22 set. 2009. Disponível em: <https://www.wired.com/2009/09/how-the-netflix-prize-was-won/>. Acesso em: 12 set. 2017.

15 DAHL, Melissa. The Future of Dieting Is Personalized Algorithms Based on Your Gut Bacteria. The Future, 2 out. 2015. Disponível em: <http://nymag.com/scienceofus/2015/10/future-of-dieting-is-personalized-algorithms.html>. Acesso em: 12 set. 2017.

16 FINKELSTEIN, Sydney. Algorithms are making us small minded. BBC, 13 dez. 2016. Disponível em: <http://www.bbc.com/capital/story/20161212-algorithms-are-making-us-small-minded>. Acesso em: 12 set. 2017.

17 POITRAS, Colin. The rise of self-driving cars. PHYS.ORG, 21 mar. 2017. Disponível em: <https://phys.org/news/2017-03-self-driving-cars.html>. Acesso em: 12 set. 2017.

18 TED. Beware online "filter bubbles". Disponível em: <https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles>. Acesso em: 12 set. 2017.

19 NEW SCIENTIS. Why Facebook Have na Important Button. Disponível em: <https://www.newscientist.com/blogs/culturelab/2011/06/why-facebook-have-an-important-button.html>. Acesso em: 12 set. 2017.

20 CALVIN, Aaron Paul. Can Amazon's Alexa Be Your Friend? Digg, 30 mar. 2017. Disponível em: <http://digg.com/2017/amazon-alexa-is-not-your-friend>. Acesso em: 12 set. 2017.

21 THE ALAN TURING INTERNET SCRAPBOOK. Could a computer think?Disponível em: <http://www.turing.org.uk/scrapbook/test.html>. Acesso em: 12 set. 2017.

22 McCONNELL, Michael. The AIs Are Winning: 5 Times When Computers Beat Humans. Make Use Of, 10 maio 2016. Disponível em: <http://www.makeuseof.com/tag/ais-winning-5-times-computers-beat-humans/>. Acesso em: 12 set. 2017.

23 LANTZ, Janessa. Killer Robots and the Many Ways in Which AI Could Go Wrong. Medium, 3 maio 2017. Disponível em: <https://thinkgrowth.org/killer-robots-and-the-many-ways-in-which-ai-could-go-wrong-31e31a221bd6>. Acesso em: 12 set. 2017.

que desperta sentimentos divergentes sobre o futuro de nossa relação com estas criações tecnológicas antropomorfizadas.[24] Frequentemente ganham a mídia a expressão dos temores de que estas máquinas tomem o espaço e os empregos humanos,[25] sendo que para algumas profissões, a extinção é uma grande probabilidade,[26 27] para um futuro muito próximo.[28] E o temor não é exclusividade das velhas gerações, mas atinge também aqueles que estão entrando no mercado de trabalho.[29] Mais do que os temores sobre a perda de empregos, questiona-se o que motivaria as nossas vidas em um mundo onde não precisássemos trabalhar.[30]

Neste panorama, parece de extrema importância perguntar sobre a pretensa imputabilidade dos algoritmos que animam os dispositivos de inteligência artificial. As decisões que a eles delegamos vão além do meramente pragmático e invadem o campo da ética e mesmo da filosofia. Em tempos mais românticos, as três leis básicas do comportamento dos robôs, enunciadas por Isaac Asimov[31] deveriam ser suficientes para moldar parâmetros seguros, mas talvez não abarquem a complexidade dos casos de uso atuais.

---

24 THE GUARDIAN. Why are we reluctant to trust robots? Disponível em: <https://www.theguardian.com/science/head-quarters/2017/apr/24/why-are-we-reluctant-to-trust-robots>. Acesso em: 12 set. 2017.

25 KAFKA, Peter. Robots want half of your jobs. Recode, 14 jan. 2017. Disponível em: <https://www.recode.net/2017/1/14/14273630/robots-replace-half-jobs-16-trillion-mckinsey>. Acesso em: 12 set. 2017.

26 LOHR, Steve. A.I. Is Doing Legal Work. But It Won't Replace Lawyers, Yet. The New York Times, 19 mar. 2017. Disponível em: <https://www.nytimes.com/2017/03/19/technology/lawyers-artificial-intelligence.html>. Acesso em: 12 set. 2017.

27 YANG, Andrew. Silicon Valley Is Right—Our Jobs Are Already Disappearing. Medium, 14 mar. 2017. Disponível em: <https://thinkgrowth.org/silicon-valley-is-right-our-jobs-are-already-disappearing-c1634350b3d8>. Acesso em: 12 set. 2017.

28 FAIRCHILD, Caroline. Will AI's impact on jobs finally force Silicon Valley to grow up? LinkedIn. Disponível em: <https://www.linkedin.com/pulse/ais-impact-jobs-finally-force-silicon-valley-grow-up-fairchild>. Acesso em: 12 set. 2017.

29 ENGELBERT, Cathy. Job-Stealing Robots? Millennials See Hope, Fear in Automation. Disponível em: <https://www.linkedin.com/pulse/job-stealing-robots-millennials-see-hope-fear-cathy-engelbert>. Acesso em: 12 set. 2017.

30 THE GUARDIAN. The meaning of life in a world without work. Disponível em: <https://www.theguardian.com/technology/2017/may/08/virtual-reality-religion-robots-sapiens-book>. Acesso em: 12 set. 2017.

31 WIKIPEDIA. Three Laws of Robotics. Disponível em: <https://en.wikipedia.org/wiki/Three_Laws_of_Robotics>. Acesso em: 12 set. 2017.

Como exemplo, podemos pensar em um carro auto dirigível na iminência de um acidente, tendo que escolher entre proteger os passageiros ou os transeuntes. Deveríamos esperar que minimizasse as perdas humanas, ou protegesse seu proprietário? De quem é a culpa quando acontecem acidentes; fabricantes ou proprietários? Da mesma forma, um drone que identificasse e atacasse terroristas; deveria aceitar um número controlado de baixas civis para atingir seus objetivos? São questões difíceis de ignorar. Por outro lado, há uma grande gama de argumentos do porquê algumas decisões deveriam ser deixadas para os computadores que – novamente, em teoria – não seriam afetados por vieses cognitivos, não modificariam o comportamento programado sob estresse, pressão ou fadiga e, em princípio, poderiam ser modelados a partir dos mais elevados padrões morais. Mas, como sabemos, as definições de ética são culturalmente e diacronicamente condicionadas, e escapam aos programadores e designers mais bem intencionados.[32] Uma outra face do problema surge quando examinamos a forma com que estes algoritmos aprendem. Os vieses que observamos em programas e aplicativos[33] são inerentes às desigualdades sociais e clivagens tendenciosas presentes nos dados que produzimos, em nosso contexto e tecido sociais. Fonte primordial de aprendizado destes algoritmos, estes dados são produzidos no seio das atividades humanas, reproduzindo e perpetuando preconceitos e lacunas de compreensão.[34] A aura de objetividade da matemática é, neste caso, um pretenso mito, e a neutralidade, suspeita. Tanto pior, o esforço para fazer os assistentes pessoais – Alexa, Google, Cortana, Siri, etc. – parecerem mais humanos,[35] pode exacerbar seus comportamentos enviesados.

---

32 DIGNAN, Larry. Can AI really be ethical and unbiased? ZD Net, 16 out. 2016. Disponível em: <http://www.zdnet.com/article/can-ai-really-be-ethical-and-unbiased/>. Acesso em: 12 set. 2017.

33 GARVIE, Clare; FRANKLE, Jonathan. Facial-Recognition Software Might Have a Racial Bias Problem. The Atlantic, 7 abr. 2016. Disponível em: <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/>. Acesso em: 12 set. 2017.

34 McGLINCHEY, Lori; TOOMEY, Jenny. "Weapons of Math Destruction": Data scientist Cathy O'Neil on how unfair algorithms perpetuate inequality. Ford Foundation, 11 out. 2016. Disponível em: <https://www.fordfoundation.org/ideas/equals-change-blog/posts/weapons-of-math-destruction-data-scientist-cathy-o-neil-on-how-unfair-algorithms-perpetuate-inequality/>. Acesso em: 12 set. 2017.

35 PEREZ, Sarah. Alexa learns to talk like a human with whispers, pauses & emotion. Disponível em: <https://techcrunch.com/2017/04/28/alexa-learns-to-talk-like-a-human-with-whispers-pauses-emotion/>. Acesso em: 12 set. 2017.

Nas análises mais radicais, já se desenha uma nova forma de religião, o "dataísmo",[36] que reifica a preponderância dos algoritmos na tomada de decisões. Da mesma forma que a autoridade divina foi legitimada pela religião e a mitologia, e a autoridade humana se impôs através das ideologias humanistas, os gurus da alta tecnologia e os profetas do vale do silício estão criando uma nova narrativa universal, alimentada pelo *Big Data*.

A superação destes dilemas depende de muitas variáveis. Como condição *sine qua non*, a compreensão do problema pelo grande público e, em última instância, os grandes usuários destas tecnologias. Infelizmente, o que se observa é a amplificação do *digital divide* para o campo dos algoritmos e da inteligência artificial. Faz-se mister a reformulação dos currículos das escolas e a reorganização das pautas de discussão na sociedade. Não basta apenas "aprender a programar", como defendem muitas campanhas de reformulação de currículos escolares. Para se equacionar o problema dos algoritmos, devemos estimular abordagens holísticas e interdisciplinares, que promovam o debate, a apropriação social de questões como ética, privacidade e dados.

Humanos, é a vossa vez de mover as peças!

REFERÊNCIAS

AMAZON. The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World. Disponível em: <https://www.amazon.com/The-Master-Algorithm-Ultimate-Learning/dp/0465065708>. Acesso em: 12 set. 2017.

CALVIN, Aaron Paul. Can Amazon's Alexa Be Your Friend? Digg, 30 mar. 2017. Disponível em: <http://digg.com/2017/amazon-alexa-is-not-your-friend>. Acesso em: 12 set. 2017.

DAHL, Melissa. The Future of Dieting Is Personalized Algorithms Based on Your Gut Bacteria. The Future, 2 out. 2015. Disponível em: <http://nymag.com/scienceofus/2015/10/future-of-dieting-is-personalized-algorithms.html>. Acesso em: 12 set. 2017.

DIGNAN, Larry. Can AI really be ethical and unbiased? ZD Net, 16 out. 2016. Disponível em: <http://www.zdnet.com/article/can-ai-really-be-ethical-and-unbiased/>. Acesso em: 12 set. 2017.

ENGELBERT, Cathy. Job-Stealing Robots? Millennials See Hope, Fear in Automation. Disponível em: <https://www.linkedin.com/pulse/job-stealing-robots-millennials-see-hope-fear-cathy-engelbert>. Acesso em: 12 set. 2017.

36 HARARI, Yuval Noah. Yuval Noah Harari on big data, Google and the end of free will. Financial Times, 26 ago. 2016. Disponível em: <https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c>. Acesso em: 12 set. 2017.

FAIRCHILD, Caroline. Will AI's impact on jobs finally force Silicon Valley to grow up? LinkedIn. Disponível em: <https://www.linkedin.com/pulse/ais-impact-jobs-finally-force-silicon-valley-grow-up-fairchild>. Acesso em: 12 set. 2017.

FINKELSTEIN, Sydney. Algorithms are making us small minded. BBC, 13 dez. 2016. Disponível em: <http://www.bbc.com/capital/story/20161212-algorithms-are-making-us-small-minded>. Acesso em: 12 set. 2017.

FREE DOCUMENTARIES. Terms and Conditions May Apply. Disponível em: <https://freedocumentaries.org/documentary/terms-and-conditions-may-apply>. Acesso em: 12 set. 2017.

FREYTAS-TAMURA, Kimiko. The Bright-Eyed Talking Doll That Just Might Be a Spy. The New York Times, 17 fev. 2017. Disponível em: <https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html>. Acesso em: 12 set. 2017.

GARVIE, Clare; FRANKLE, Jonathan. Facial-Recognition Software Might Have a Racial Bias Problem. The Atlantic, 7 abr. 2016. Disponível em: <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/>. Acesso em: 12 set. 2017.

HARARI, Yuval Noah. Yuval Noah Harari on big data, Google and the end of free will. Financial Times, 26 ago. 2016. Disponível em: <https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c>. Acesso em: 12 set. 2017.

HESS, Amanda. How Privacy Became a Commodity for the Rich and Powerful. The New York Times, 9 maio 2017.

KAFKA, Peter. Robots want half of your jobs. Recode, 14 jan. 2017. Disponível em: <https://www.recode.net/2017/1/14/14273630/robots-replace-half-jobs-16-trillion-mckinsey>. Acesso em: 12 set. 2017.

LABS, Mate. Why do we need the Democratization of Machine Learning? Start Up Grind, 27 abr. 2017. Disponível em: <https://medium.com/startup-grind/why-do-we-need-the-democratization-of-machine-learning-80104e43c76f>. Acesso em: 12 set. 2017.

LANTZ, Janessa. Killer Robots and the Many Ways in Which AI Could Go Wrong. Medium, 3 maio 2017. Disponível em: <https://thinkgrowth.org/killer-robots-and-the-many-ways-in-which-ai-could-go-wrong-31e31a221bd6>. Acesso em: 12 set. 2017.

LOHR, Steve. A.I. Is Doing Legal Work. But It Won't Replace Lawyers, Yet. The New York Times, 19 mar. 2017. Disponível em: <https://www.nytimes.com/2017/03/19/technology/lawyers-artificial-intelligence.html>. Acesso em: 12 set. 2017.

McCONNELL, Michael. The AIs Are Winning: 5 Times When Computers Beat Humans. Make Use Of, 10 maio 2016. Disponível em: <http://www.makeuseof.com/tag/ais-winning-5-times-computers-beat-humans/>. Acesso em: 12 set. 2017.

McGLINCHEY, Lori; TOOMEY, Jenny. "Weapons of Math Destruction": Data scientist Cathy O'Neil on how unfair algorithms perpetuate inequality. Ford Foundation, 11 out. 2016. Disponível em: <https://www.fordfoundation.org/ideas/equals-change-blog/posts/weapons-of-math-destruction-data-scientist-cathy-o-neil-on-how-unfair-algorithms-perpetuate-inequality/>. Acesso em: 12 set. 2017.

MIT TECHNOLOGY REVIEW. The Future of Medical Visualisation. Disponível em: <https://www.technologyreview.com/s/428134/the-future-of-medical-visualisation/>. Acesso em: 12 set. 2017.

MORAVEC, Hans. Rise of the Robots--The Future of Artificial Intelligence. Scientific American, 23 mar. 2009. Disponível em: <https://www.scientificamerican.com/article/rise-of-the-robots/>. Acesso em: 12 set. 2017.

MURPHY, Kate. One Day, a Machine Will Smell Whether You're Sick. The New York Times, 1 maio 2017. Disponível em: <https://www.nytimes.com/2017/05/01/health/artificial-nose-scent-disease.html>. Acesso em: 12 set. 2017.

NEW SCIENTIS. Why Facebook Have na Important Button. Disponível em: <https://www.newscientist.com/blogs/culturelab/2011/06/why-facebook-have-an-important-button.html>. Acesso em: 12 set. 2017.

PEREZ, Sarah. Alexa learns to talk like a human with whispers, pauses & emotion. Disponível em: <https://techcrunch.com/2017/04/28/alexa-learns-to-talk-like-a-human-with-whispers-pauses-emotion/>. Acesso em: 12 set. 2017.

POITRAS, Colin. The rise of self-driving cars. PHYS.ORG, 21 mar. 2017. Disponível em: <https://phys.org/news/2017-03-self-driving-cars.html>. Acesso em: 12 set. 2017.

PWC. Streaming the Future. Disponível em: <http://www.pwc.com/us/en/industry/entertainment-media/publications/assets/pwc-streaming-the-future-february-2016.pdf>. Acesso em: 12 set. 2017.

SCIENTIFIC AMERICAN. What Is the Smart Grid? 10 maio 2010. Disponível em: <https://www.scientificamerican.com/report/smart-electricity-grid/>. Acesso em: 12 set. 2017.

TED. Beware online "filter bubbles". Disponível em: <https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles>. Acesso em: 12 set. 2017.

THE ALAN TURING INTERNET SCRAPBOOK. Could a computer think?Disponível em: <http://www.turing.org.uk/scrapbook/test.html>. Acesso em: 12 set. 2017.

THE GUARDIAN. The meaning of life in a world without work. Disponível em: <https://www.theguardian.com/technology/2017/may/08/virtual-reality-religion-robots-sapiens-book>. Acesso em: 12 set. 2017.

THE GUARDIAN. Why are we reluctant to trust robots? Disponível em: <https://www.theguardian.com/science/head-quarters/2017/apr/24/why-are-we-reluctant-to-trust-robots>. Acesso em: 12 set. 2017.

USSEM, Jerry. How Online Shopping Makes Suckers of Us All. The Atlantic, maio 2017.

VAN BUSKIRK, Eliot. HOW THE NETFLIX PRIZE WAS WON. Wired, 22 set. 2009. Disponível em: <https://www.wired.com/2009/09/how-the-netflix-prize-was-won/>. Acesso em: 12 set. 2017.

WAGNER, Kurt. How the NFL juggles the future of streaming, the decline of TV, and billions of dollars. Disponível em: <https://www.recode.net/2017/5/1/15386694/nfl-live-stream-amazon-prime-thursday-night-football-ratings>. Acesso em: 12 set. 2017.

WHITTAKER, Zack. Hundreds of privacy-invading apps are using ultrasonic sounds to track you. ZD Net, 3 maio 2017. Disponível em: <http://www.zdnet.com/article/hundreds-of-apps-are-using-ultrasonic-sounds-to-track-your-ad-habits/>. Acesso em: 12 set. 2017.

WIKIPEDIA. Three Laws of Robotics. Disponível em: <https://en.wikipedia.org/wiki/Three_Laws_of_Robotics>. Acesso em: 12 set. 2017.

YANG, Andrew. Silicon Valley Is Right—Our Jobs Are Already Disappearing. Medium, 14 mar. 2017. Disponível em: <https://thinkgrowth.org/silicon-valley-is-right-our-jobs-are-already-disappearing-c1634350b3d8>. Acesso em: 12 set. 2017.

editoraletramento
editoraletramento
grupoletramento
editoraletramento.com.br
company/grupoeditorialletramento
contato@editoraletramento.com.br

casadodireito.com
casadodireitoed
casadodireito

Grupo
Editorial
LETRAMENTO

O campo de estudos em Direito, Tecnologia e Sociedade é amplo e controverso, sujeito a mudanças constantes que trazem, muitas vezes, mais perguntas do que respostas. Os debates deste campo tratam de objetos que transformarão a vida cotidiana no futuro, mas que também já produzem efeitos no presente. É para explorar essa realidade multifacetada que o presente livro reúne especialistas de diversos setores para debater transformações tecnológicas, políticas públicas, desafios regulatórios, posicionamentos da sociedade civil, preocupações, soluções e oportunidades, dentro e além do Direito.

Grupo Editorial LETRAMENTO

ISBN: 978-85-9530-081-1

9 788595 300811