Data protection and digital humanities in Brazil: black boxes

Proteção de dados e humanidades digitais no Brasil: caixas-pretas

Luiz Paulo Carvalho[1], Jonice Oliveira[2]

[1]Programa de Pós-graduação em Informática, Universidade Federal do Rio de Janeiro
[2]Laboratório de Computação Social e Análise de Redes Sociais,
Instituto de Matemática, Universidade Federal do Rio de Janeiro

luiz.paulo.carvalho@ppgi.ufrj.br, jonice@dcc.ufrj.br

Recebido: 4/12/2019 Aceito: 8/12/2019 Publicado: 10/12/19

Abstract. *The effervescence of the theme of privacy and data protection around the world is growing, ranging from the preservation of the right to personality to the preservation of democratic principles as we traditionally know. Works have been developed seeking compliance with laws and regulations related to this theme, not observing a socio-technical epistemological side of digital humanities. In this paper I expose black boxes that communications make clear, serving as guide for further interdisciplinary research.*

Keywords: *General personal data protection law. Post-colonialism. Sociotechnical.*

Resumo. *É crescente a efervescência do tema de privacidade e proteção de dados pelo mundo, contemplando desde a preservação do direito à personalidade até a preservação dos princípios democráticos como tradicionalmente conhecemos. Trabalhos vem sendo desenvolvidos buscando conformidade com as legislações e normativas relacionadas com este tema, não observando um lado epistemológico socio técnico de humanidades digitais. Neste trabalho exponho caixas-pretas que as comunicações deixam perceber, e que podem servir como norte para pesquisas interdisciplinares posteriores.*

Palavras-chave: *Lei geral de proteção de dados pessoais. Pós-colonialismo. Sociotécnica.*

1. Introdução

Em 14 de Agosto de 2020 entrará em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira[1], regulamentando a proteção de dados operacionalizada pelo tratamento

[1] http://bit.ly/2PeKgcj. Acesso em 01/12/2019

de dados de pessoas naturais brasileiras, em âmbito digital ou físico, seja internamente, nas fronteiras nacionais, ou externamente, em alcance transnacional.
Neste trabalho busco tensionar alguns pontos opacos sobre a LGPD, como esboço de uma agenda de pesquisa com um viés socio técnico sob o prisma de Humanidades Digitais. Pelo foco direcionado deste trabalho não me aprofundarei em detalhes na LGPD ou na legislação de proteção de dados da União Europeia (UE), a Regulamentação Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR) [2].

Estas tensões surgem de "fios soltos" no labirinto das epistemologias políticas das tecnologias, que levam para caixas-pretas a partir de uma perspectiva de formação de uma rede semiótica-materialista. Utilizo então a abordagem da Teoria Ator-Rede (*Actor-Network Theory* – ANT) (LATOUR, 2005) (LATOUR, 1987), onde analiso os atores não-humanos, assim como humanos, como atuantes e participantes nos sistemas legais e jurídicos associados com a proteção de dados no Brasil. Nesta pesquisa me interessam as caixas-pretas, de acordo com a ANT são atores ou associações de atores, até redes inteiras, opacos e não-identificáveis, propositadamente ou não.

As raízes da aprovação final da LGPD estão associadas com casos internacionais de manipulação digital inescrupulosa de dados pessoais, como Brexit e as eleições presidenciais estadunidenses de 2016; assim como casos brasileiros, como as eleições presidenciais de 2018 (BIONI, 2019). Em determinados casos não há nem a necessidade de compartilhamento de desinformação, vulgarmente generalizada como *fake news*, uma abordagem com viés de psicologia informacional associada com o perfil de interesse da parte pode ser o bastante para conduzi-la ao comportamento esperado, mesmo que este seja o de inação [3]. Por exemplo, fomentar no eleitor a intenção de ausentar-se de um processo eleitoral.

A LGPD é genérica ao ponto de abstrair meios e canais, influenciando tanto plataformas digitais como fichas de cadastro de clientes em papel de pequenas empresas. Considerando capacidades de processamento, a ênfase é na categoria computadorizada, operando sobre dezenas de dimensões simultaneamente, e não na categoria humana, que apresenta dificuldades algébricas e de representação gráfica ao se ultrapassar três dimensões (SUMPTER, 2018). A importância do tipo de mídia será aprofundada adiante.

Como tenho observado algumas comunicações utilizando termos errôneos ou dúbios, caracterizo como necessário um esclarecimento sobre Privacidade e Proteção de Dados. Pelas comunicações podem ser encontradas falas que misturam os dois termos ou citam a LGPD como "lei da privacidade", o que é uma infidelidade semântica. Deveres e obrigações legais são relacionados com o direito positivo; a não-interferência de uns em relação aos direitos de outros é relacionada com o direito negativo. Como esclarece Bioni (2019), Privacidade tem aspecto negativo, vem à tona apenas quando se percebe violada; Proteção de Dados tem aspecto positivo, é dever e obrigação do Estado e da Sociedade protegê-lo e preservá-lo. Uma das maneiras de preservar a privacidade é com a proteção de dados, mas a proteção de dados não provêm da privacidade. A partir do momento que alguém decide compartilhar seus dados, seja preenchendo um cadastro pessoal, a privacidade é violada, mesmo que o compartilhamento seja apenas entre esta pessoa e a organização que lhe garantiu determinada

[2] http://bit.ly/35OtKWW. Acesso em 01/12/2019
[3] http://bit.ly/2ODFpCc. Acesso em 01/12/2019

segurança ou proteção de dados. Por exemplo, a GDPR utiliza o princípio de "*Data Protection by Design*" e não "*Privacy by Design*", não há nenhuma citação desta última na redação base da GDPR, mesmo que algumas comunicações, escritas ou verbais, se enganem em citar diferente [4].

Considerados os rumos da pesquisa, estruturo o trabalho da seguinte forma: Seção 2 apresenta breve histórico de proteção de dados na UE e na América Latina; Seção 3 apresenta a tensão principal deste trabalho, o aprofundamento no viés de Humanidades Digitais do cenário brasileiros de proteção de dados, como viés pós-colonial, influências negativas para efetividade da legislação, oportunismo pancapitalista sobre legisladores, dentre outros; Seção 4 apresenta a conclusão.

2. Breve histórico de proteção de dados

No Brasil consideram-se alguns pontos anteriores à LGPD como precursores da proteção de dados, dentre eles os artigos 43º e 44º do Código de Defesa do Consumidor (CDC) [5], de 1990; Marco Civil da Internet (MCI) [6], de 2014. Sobre este último há o Artigo 7º, que foi complementado antes de aprovação final recebendo itens específicos para proteção de dados pessoais pela Internet. A "injeção de proteção de dados" no MCI foi influência, como resposta brasileira, das revelações de Snowden sobre iniciativas de espionagem antiética e ilegal do governo estadunidense (BIONI, 2015), não apenas sobre cidadãos de outros países, como também de chefes de governo. Os incisos I e II do MCI demonstram preocupação explícita com sigilo de comunicações e seus respectivos fluxos.

A primeira lei propriamente direcionada à proteção de dados no Brasil é a LGPD. Seu início remonta o ano de 2010, onde foi aberto o debate sobre o tema para toda sociedade. Após um período de latência é retomada em 2015, onde uma nova plataforma de colaboração foi utilizada (BIONI, 2015). O termo "geral" de LGPD se dá não apenas pela amplitude multisetorial que a legislação perpassa, como também pela rica colaboração multisetorial que culminou na redação final de legislação, com ampla e democrática participação de parcela da sociedade interessada e engajada, não apenas legisladores e juristas (BIONI, 2019).

Em países muito próximos, geográfica e geopoliticamente, do Brasil já se encontravam leis próprias e dedicadas para proteção de dados, por exemplo: Argentina, 2001; Chile, 2002; Uruguai, 2008; e Colômbia, 2012 (DLA PIPER, 2019). Estes países possuem também entidades operacionais e atuantes de controle das respectivas legislações, diferente do Brasil. No Brasil a entidade que zela pela proteção de dados, à luz da LGPD, é a Autoridade Nacional de Proteção de Dados (ANPD), já em vigor pela própria LGPD, só que não composta e instituída *de facto*, seus membros ainda não foram todos definidos até este momento.

O Mercado Comum do Sul (Mercosul) foi fundado em 1991, o último país a acessar o bloco foi a Venezuela, em 2012; este mesmo país se encontra em suspensão desde 2016. O Mercosul é formado por cinco membros plenos: Argentina, Brasil, Uruguai, Paraguai e

[4] https://glo.bo/2sAncgl. Acesso em 01/12/2019

[5] http://bit.ly/2RcOQKv. Acesso em 01/12/2019

[6] http://bit.ly/2CBJrVk. Acesso em 01/12/2019

Venezuela; cinco países associados: Chile, Bolívia, Colômbia, Equador e Peru. Por associação simples, o Mercosul seria o equivalente à União Europeia da América do Sul.

Na Europa o histórico relacionado com proteção de dados é mais longínquo. Data de 1981 com a Convenção de Proteção de Dados (*Data Protection Convention* – DPC); em 1995 com a Diretiva Europeia de Proteção de Dados (*European Data Protection Directive* – EDPD). Em 2012 a GDPR vem à luz e é colocada em debate multisetorial pela sociedade europeia, sendo aprovada 4 anos depois, em 2016, e entrando em vigor em 2018. A GDPR abrange todos os países membros da UE. Vários tratados formaram a UE como é configurada hoje, desde o Tratado de Roma, em 1957, até o Tratado de Lisboa, em 2007. Em 2013 a Croácia se tornou o último país a ingressar na UE, sendo o 28º.

3. Humanidades digitais e proteção de dados no Brasil

A GDPR autoriza que apenas países com legislações que proporcionem rigor comparável de proteção de dados possam tratar dados pessoais ou dados sensíveis de cidadãos da UE. Neste contexto retornarmos às mídias físicas e digitais, caso um cidadão da UE intencione hospedagem no Brasil, mesmo que o negócio específico utilize cadastro físico, totalmente em papel, ele ainda precisa estar em conformidade com a GDPR.

O *Brussels Effect* (BRADFORD, 2012) nos auxilia a perceber o fenômeno de pós colonialismo da influência colonizadora legal nos países periféricos ou semiperiféricos, através da visão geopolítica, em países que apresentam dependência de negociação com a UE. Isto é, a UE exporta não apenas a sua legislação de proteção de dados, também seus princípios, valores e epistemologias conceituais sobre o tópico (SCOTT; CERULUS, 2018); como entendemos e operacionalizamos proteção de dados é como a UE entende e operacionaliza proteção de dados.

São importados os mecanismos e operacionalizações legais, artefatos jurídicos, de outro contexto, onde não necessariamente consideram-se os desafios e problemas da proteção de dados brasileiros. Observo que comunicadores sobre o tema não apenas debruçam-se sobre a GDPR para qualquer tema negligenciado ou não coberto pela LGPD, como também assim o recomendam aos demais: "caso não consigamos resolver este item à luz da LGPD, voltamo-nos à GDPR, impactos e aplicações, para buscar bases e exemplos de como agir aqui". Não apenas importamos o artefato jurídico em sua essência, como também importamos informações complementares em avanço, decidimos questões particulares nacionais aos olhos de uma comunidade sociocultural muito diferente. Aspectos contextuais europeus são diferentes ou incompatíveis com os brasileiros, como econômicos, socioculturais ou o nível de maturidade tecnológica digital (MOOR, 2005).

Seguindo neste âmbito, Couldry e Mejias (2019) abordam pós colonialismo e descolonização ao se tratar de dados e suas influências, citando o Brasil e sua relação com a GDPR. A primeira caixa-preta está relacionada com a escolha do modelo de legislação proposto pela UE para proteção de dados. Considerando que: (i) outros países muito mais próximos, geograficamente ou geopoliticamente localizados no sul global, periféricos ou semiperiféricos, já tinham legislações para proteção de dados bem estabelecidas, com suas determinadas entidades reguladoras e muitos anos de efetividade prática; (ii) a UE construiu

sua legislação como um bloco unificado, deixando em aberto para que cada país do bloco complementasse a GDPR com seus aditivos contextuais; (iii) a GDPR, desde sua aprovação em 2016 já reconhecia o Uruguai e a Argentina como países com iniciativas de proteção de dados em conformidade com seu rigor; (iv) a preocupação com a proteção de dados, físicos ou digitais, data da décadas atrás, intensificada nas décadas de 1970 e 1980 na Europa e nos Estados Unidos, e é inicialmente esboçada no CDC brasileiro em 1993; observo: (a) o Mercosul não construiu sua própria legislação de proteção de dados consolidada, mesmo que antropofagizada (MEDINA *et al.*, 2014), baseada nas legislações já vigentes em seus países integrantes; (b) o Brasil não recorreu às legislações da Argentina ou Uruguai para construir ou embasar a maior parte da sua própria. Parece que a GDPR, e seu item de restrição transnacional de operação de dados, que realmente motivaram este tópico, não as disposições do Art. 1º da LGPD; (c) sendo primariamente uma precaução pancapitalista (ESCOBAR, 2018) às sanções europeias e eventuais multas, então não há uma preocupação material com privacidade, liberdade, proteção de dados ou o conceito de boa-fé que for. Seguindo o raciocínio do item (c) podemos seguir a jusante (LATOUR, 2016) desta rede ainda em formação antecedendo que a LGPD poderá, de fato, agir sobre os mercados e negócios superficialmente, negligenciando outros efeitos colaterais danosos ao tecido social democrático, como manipulação de dados por baixo dos panos para influenciar resultados de eleições, a partir de operações que utilizam como insumo dados pessoais, como *profiling* (PINTO, 2018). Isto é, a lei servirá apenas para "europeu ver", construindo uma fachada de "sim, como país, estamos em conformidade".

Outro ponto além do *Brussels Effect* (BRADFORD, 2012) pode ser visto em uma colonização técnico-linguística. Na LGPD são considerados papéis com responsabilidades específicas, sendo os dois com maior envolvimento no tratamento de dados o encarregado e o controlador. Lê-se: "controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;" e "operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;". A GDPR considera o papel do *Data Protection Officer* (DPO), por analogia simples seria o equivalente ao controlador na LGPD. Desde a sanção da LGPD, diversos atores, especialmente advogados, tem se intitulado DPO, apesar deste papel não ter nenhuma associação com a LGPD, sendo apenas vigente na GDPR. Uma busca rápida pelo termo *Data Protection Officer* no Google expõe o ambiente predatório e sedutor para oportunistas que percebem o papel europeu como socialmente mais bem capitalizado do que o brasileiro, de controlador, mesmo que isso seja inefetivo *de facto* (CARVALHO *et al.*, 2019).

Com um viés tecnológico (MARQUES, 2016) a importação majoritária da GDPR à LGPD nos apresenta outra caixa-preta, das aparelhagens tecnológicas que irão operacionalizar os conceitos da LGPD. Considerando que o discurso dominante da prática é de recorrer à GDPR, podemos caminhar neste raciocínio para os respectivos aparelhos tecnológicos já existentes. Quem detém a propriedade destes aparelhos que adequam a conformidade ou estão em conformidade com a GDPR? A UE, sejam os aparelhos de recursos humanos especializados, potenciais consultorias; sejam os aparelhos tecnológicos computadorizados, como Sistemas de Gerenciamento de Banco de Dados (SGBD) configurados para os requisitos técnicos provindos da LGPD ou GDPR.

Sendo um tópico polêmico em relação à proteção de dados, o reconhecimento facial pode servir de exemplos para outra caixa-preta, do monopólio dos aparelhos tecnológicos de tratamento de dados pessoais por organizações privadas. Por exemplo, as organizações públicas não são proprietárias de algoritmos de reconhecimento facial. Nos Estados Unidos, várias das maiores empresas de tecnologia, como Amazon e Microsoft, com soluções de reconhecimento facial estão pressionando o Governo para criação de leis que regulem o uso delas [7]. Estas empresas não apenas clamam por regulamentações sobre o tema, como rascunham suas próprias redações e conceituações para estas mesmas regulamentações [8], demonstrando, explicitamente, a intenção de dominar o discurso legal sobre o tema. O raciocínio se deduz com simplicidade: (1) tecnologias de reconhecimento facial estão sendo banidas ou percebidas com infâmia pela Sociedade [9]; (ii) maiores empresas de tecnologia suspendem o lançamento ou espalhamento das suas tecnologias de reconhecimento facial, alegando que são apenas as fornecedoras dos serviços e que os usufrutuários do mesmos que estão errados; (3) as mesmas empresas pressionam a Sociedade, em especial os atores legislativos, a pensar em "freios legais" que "controlem" o uso das tecnologias que elas mesmas desenvolvem e disponibilizam; (4) legisladores, lobistas ou não, clamam por assistência tecnológica especializada e empírica sobre o tema; (5) quem detém o *know how* especializado e empírico sobre a tecnologia de reconhecimento facial? As mesmas empresas que as desenvolvem e disponibilizam; (6) próximo passo dessas empresas? Rascunhar suas próprias regulamentações sobre o tema, como que de boa-fé. Zuboff (2019) vai classificar esta "boa-fé" como inconcebível, pelos preceitos do capitalismo de vigilância.

Esta ilustração do percurso ou itinerância do que tem acontecido com o reconhecimento facial nos Estados Unidos pode ser associado com a GDPR e LGPD, assim como com alguma futura regulamentação para reconhecimento facial que o norte global venha a adotar. Desta forma, por exemplo, um prelúdio pela GDPR pode ser, no futuro, que a Amazon restrinja a comercialização da sua aparelhagem tecnológica de reconhecimento facial apenas para países que apresentem legislações comparáveis com aquelas que considere ideais, podendo este fenômeno se tornar um comportamento disseminado às demais empresas do ramo.

Um dos casos de proteção de dados, reconhecimento facial e vício de consentimento tensionados é o de implementação de câmeras desta tecnologia em Igrejas [10], ou ambientes onde haja uma relação de poder implícita, um currículo doutrinário oculto. Como qualquer legislação ou poder público poderá competir em influência com uma suposta "determinação sagrada" através de uma possível "palavra divina" que ordena aos membros daquela comunidade que cedam o consentimento do tratamento de dados da sua imagem à instituição religiosa? Em outro cenário, como um funcionário, desprivilegiado em poder, vai denunciar o uso tratamento indevido de seus dados pessoais ou dados sensíveis na instituição na qual trabalha? Como um candidato à uma vaga de emprego vai realizar uma denúncia porque o processo de seleção tentou coletar dados não condizentes com a finalidade da função para a qual é pleiteado o acesso? Um desafio está em construir mecanismos e operacionalizações que coíbam esses falsos legítimos interesses ou consentimentos predatórios inescrupulosos,

[7] https://engt.co/33Fu8Wm. Acesso em 01/12/2019
[8] http://bit.ly/2DCgqZA. Acesso em 01/12/2019
[9] https://nyti.ms/35QujPX. Acesso em 01/12/2019
[10] http://bit.ly/2P0tGfW. Acesso em 01/12/2019

empoderando o titular dos dados, sem expô-lo ao dano. A preservação deste titular de dados é, também, prerrogativa da LGPD.

Finalizando, faço um último tensionamento em paralelo ao olhar sociotécnico (CUKIERMAN, 2007) em relação ao *Credit Score* chinês, conjuntamente ao *Social Credit System* (SOARES, 2018). Na China os dados pessoais e dados sensíveis são coletados por super plataformas, como da empresa Alibaba. Assim como no Brasil, os aparelhos tecnológicos de vigilância de dados são detidos por organizações privadas, que cedem dados ao Estado, devido ao modelo do país. O Estado, então, pode construir pontuações e quantificar cidadãos de acordo com seus dados e suas ações específicas. A intenção da LGPD é, principalmente, impedir este fenômeno de vigilância total sobre a vida das pessoas. Apesar disso o governo parece andar na contramão, tentando construir o Cadastro Nacional de Informações Sociais (CNIS), através dos decretos 10.046 e 10.047/2019 [11]. Esse cadastro em base de dados única conflita profundamente com o propósito da LGPD, que é garantir da forma mais ampla possível o direito à privacidade através da proteção de dados consentida pela pessoa natural. Estes dois decretos buscam coletar dados pessoais e dados sensíveis de toda população brasileira, sem finalidade ou demais informações disponíveis específicas, com a justificativa de "fomentar interoperabilidade", "compartilhar bases de dados" e "ampliar informações". Dito isto, o Estado terá todas as informações possíveis e imagináveis para construir uma solução de vigilância total, contendo desde o endereço até os dados da retina de uma pessoa. O próprio Estado, através de um suposto poder de atuação, viola completamente a privacidade de todos os cidadãos brasileiros, em apenas dois decretos seguidos.

4. Conclusão

A LGPD finalmente traz o tema de Privacidade e de Proteção de Dados "à mesa" do brasileiro. Faltando menos de um ano para a lei entrar efetivamente em vigor, ânimos estão exaltados e o contorno dos discursos está tomando forma, explícita ou implicitamente, a favor ou contra a lei. Como comunicações onde autores priorizam acriticamente elementos como "competitividade", "inovação" e "progresso tecnológico" [12], inserindo várias conjunções adversativas após enunciarem as vantagens e benefícios da proteção de dados no Brasil. Faz-se necessário uma inspeção criteriosa nas comunicações, que tentem parecer neutras e impessoais ou próprias, e nos respectivos discursos. Uma abordagem é utilizar balões de falas, como em quadrinhos, para rastrear os atores e suas redes (LATOUR, 2016).

Já me posicionando totalmente favorável à intenção da lei, considero também que não podemos renunciar a um aprofundamento nas caixas-pretas que compõe o aspecto socio técnico deste cenário, de seus atores e suas respectivas redes. É inegável que há um fator de colonização no ato de importar a maioria do artefato jurídico (ESCOBAR, 2018), porque não apenas importando a lei, estamos importando as normas, costumes e percepções da realidade de outro contexto. E, concomitantemente, precisamos ficar atentos quanto às iniciativas de vigilância inescrupulosa do mesmo Estado que aprovou e fará valer uma legislação dedicada à proteção de dados e que, supostamente, preserva o direito à privacidade.

[11] http://bit.ly/2Lb2oCD. Acesso em 01/12/2019

[12] http://bit.ly/33HR2w1. Acesso em 01/12/2019

Financiamento

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Referências

BIONI, B. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. ed. 2. São Paulo: Forense, 2019.

_____. **Xeque-Mate: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015.

BRADFORD, A. **The Brussels Effect**. Northwestern University Law Review. 107 (1). SSRN 2770634, Columbia Law and Economics Working Paper n. 533, 2012.

CARVALHO, L.P.; CAPPELLI, C.; OLIVEIRA, J. **Proteção de Dados no Brasil, uma visão Sociotécnica em Sistemas de Informação**. 2º Encontro do INCT.DD. Salvador, Bahia. DOI 10.13140/RG.2.2.13999.89765. 2019.

COULDRY, N.; MEJIAS, U. **Making data colonialism liveable: how might data's social order be regulated?** Internet Policy Review, 8 (2). DOI 10.14763/2019.2.1411. 2019.

CUKIERMAN, H.L.; TEIXEIRA, C.; PRIKLADNICKI, R. **Um Olhar Sociotécnico sobre a Engenharia de Software**. RITA, v. XIV, n. 2, 2007.

DLA PIPER. **DATA PROTECTION LAWS OF THE WORLD, Full Handbook**. Disponível em: https://www.dlapiperdataprotection.com/. 2019.

ESCOBAR, A. **Designs for the Pluriverse: Radical Interdependence, Autonomy, and the Making of Worlds**. Londres: Duke University, 2018.

LATOUR, B. **Cogitamus: seis cartas sobre as humanidades científicas**. São Paulo: Editora 34, 2016.

_____ . **Reassembling the Social: An Introduction to Actor-Network-Theory**. Oxford: Oxford UP, 2005.

_____. **Science in Action: How to Follow Scientists and Engineers Through Society**. Londres: Open University Press, 1987.

MARQUES, I. **História das Ciências, Estudos CTS e os Brasis**. Abertura do IX Congresso Scientiarum Historia. Rio de Janeiro, 2016.

MEDINA, E.; MARQUES, I.; HOLMES, C. **Beyond Imported Magic. Essays on Science, Technology, and Society in Latin America**. EUA: MIT Press, 2014.

MOOR, J. **Why we need better ethics for emerging technologies. Ethics and Information Technology**. v. 7 (3), pp. 111–119. DOI 10.1007/s10676-006-0008-0. 2005.

PINTO, R. **SOBERANIA DIGITAL OU COLONIALISMO DIGITAL? Novas tensões relativas à privacidade, segurança e políticas nacionais**. Disponível em: https://sur.conectas.org/soberania-digital-ou-colonialismo-digital/. 2018. Acesso em 01/12/2019.

SCOTT, M.; CERULUS, L. **Europe's new data protection rules export privacy standards worldwide**. Disponível em: https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/. 2018. Acesso em 01/12/2019.

SOARES, G. **Rumo à governança algorítmica - análise sociotécnica dos algoritmos de credit score: o caso chinês**. XI Congresso Scientiarum Historia. Rio de Janeiro, 2018.

SUMPTER, D. **Outnumbered: From Facebook and Google to Fake News and Filter-bubbles – The Algorithms That Control Our Lives**. EUA: Bloomsbury Sigma, 2018.

ZUBOFF, S. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. EUA: PublicAffairs, 2019.