PUCRS

ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO
MESTRADO EM DIREITO

BRUNO SCHIMITT MORASSUTTI

REGULAÇÃO DE TECNOLOGIAS E ARQUITETURA DE SISTEMAS: UM ESTUDO SOBRE O PRIVACY BY DESIGN E A TRANSPARÊNCIA APLICADA A ALGORITMOS COMPUTACIONAIS

Porto Alegre
2019

PÓS-GRADUAÇÃO - *STRICTO SENSU*

Pontifícia Universidade Católica
do Rio Grande do Sul

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL

ESCOLA DE DIREITO

BRUNO SCHIMITT MORASSUTTI

REGULAÇÃO DE TECNOLOGIAS E ARQUITETURA DE SISTEMAS

UM ESTUDO SOBRE O *PRIVACY BY DESIGN* E A TRANSPARÊNCIA APLICADA A ALGORITMOS COMPUTACIONAIS

Porto Alegre

2019

BRUNO SCHIMITT MORASSUTTI

REGULAÇÃO DE TECNOLOGIAS E ARQUITETURA DE SISTEMAS

UM ESTUDO SOBRE O *PRIVACY BY DESIGN* E A TRANSPARÊNCIA APLICADA A ALGORITMOS COMPUTACIONAIS

Dissertação apresentada como requisito para a obtenção o grau de Mestre pelo Programa de Pós-Graduação da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

Orientador: Prof. Dr. Juarez Freitas

Porto Alegre

2019

Ficha Catalográfica

M829r Morassutti, Bruno Schimitt

Regulação de Tecnologias e Arquitetura de Sistemas : Um estudo sobre o privacy by design e a transparência aplicada a algoritmos computacionais / Bruno Schimitt Morassutti . – 2019.

182 f.

Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, PUCRS.

Orientador: Prof. Dr. Juarez Freitas.

1. regulação. 2. algoritmos computacionais. 3. transparência. 4. privacy by design. I. Freitas, Juarez. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da PUCRS
com os dados fornecidos pelo(a) autor(a).
Bibliotecária responsável: Salete Maria Sartori CRB-10/1363

BRUNO SCHIMITT MORASSUTTI

REGULAÇÃO DE TECNOLOGIAS E ARQUITETURA DE SISTEMAS

UM ESTUDO SOBRE O *PRIVACY BY DESIGN* E A TRANSPARÊNCIA APLICADA A ALGORITMOS COMPUTACIONAIS

Dissertação apresentada como requisito para a obtenção o grau de Mestre pelo Programa de Pós-Graduação da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

Aprovada em: 19 de junho de 2019.

BANCA EXAMINADORA

Prof. Dr. Juarez Freitas – PUCRS

Prof. Dr. Eugênio Facchini Neto – PUCRS

Prof. Dr. Darci Guimarães Ribeiro – UNISINOS

Prof. Dr. Martin Perius Haeberlin - UNIRITTER

Porto Alegre

2019

Dedico este trabalho à minha família,
pelo incentivo, carinho e inspiração
que fazem de mim a pessoa que sou.
Dedico também aos meus amigos, pois
sem eles a vida não teria
tantas cores

AGRADECIMENTOS

Este trabalho é resultado da colaboração de uma série de pessoas que, pela sua contribuição, consciente ou não, tornaram possível escrever estas linhas. Sendo assim, gostaria de agradecer:

- Ao meu orientador, Professor Doutor Juarez Freitas. Desde os primeiros anos de graduação, sua permanente disposição em estudar temas novos e complexos me instigaram e desafiaram a manter sempre viva minha curiosidade e vontade de buscar por novos conhecimentos. Sem sua cuidadosa orientação este trabalho não teria chegado até aqui.
- Aos meus pais, Paulo e Regina, pelo permanente apoio, compreensão e amor que jamais deixaram de dar durante toda a minha vida. Pelo orgulho que sinto de ser seu filho e pelo exemplo que são todos os dias, obrigado.
- Às minhas irmãs, Bianca e Alana, pelo amor, compreensão, provocações e companheirismo que, mesmo um pouco distante, sempre estiveram presentes. Contem sempre comigo.
- À Amanda Zamboni, por caminhar comigo durante esta aventura, pelo carinho de cada dia, compreensão e apoio constante. Tua dedicação, humor, perseverança e, sobretudo, torcida permanente fizeram toda a diferença. Obrigado por tudo, meu amor!
- Ao meu grande amigo e colega Alexander Pibernat, pelas contínuas conversas e permanente debate. Suas críticas, desafios e provocações ajudaram, com café ou cerveja, a amadurecer diversas ideias neste trabalho. Tmj.
- Aos meus amigos Ivonei Trindade, Diego Canabarro, Maura Polidoro e Rodrigo Aguiar pelas várias leituras e ajuda com revisões e ideias. Cada ponto que fizeram neste texto foi levado em conta.
- Ao Pedro Benz e Carlo Mazo, pelas hilárias conversas no Observatório Social e camaradagem cuja história sendo escrita no grande livro da amizade.
- Ao Lucas, Leonardo, Pedro e Ivonei, pela amizade do grupo do "Kadetchê". Ter um lugar pra conversar e rir sempre ajuda a tocar o dia.
- À toda minha família, amigos e demais pessoas que, mesmo não estando aqui listadas, fizeram e fazem parte da minha vida. Sem vocês, eu não estaria aqui.

Os infortúnios são causados pela negligência (FUNAKOSHI, Gichin)

RESUMO

O significativo desenvolvimento e disseminação das tecnologias de informação e comunicação tem acarretado profundos efeitos em nossa sociedade, afetando direitos fundamentais de grupos e indivíduos. Este cenário de mudanças incrementais e disruptivas suscita cada vez mais a necessidade de estudar as tensões existentes entre Direito, Ciência, Tecnologia e Inovação. Diante deste panorama, a regulação de sistemas eletrônicos e algoritmos computacionais tem recebido significativa atenção de estudiosos e agentes reguladores, os quais passaram a propor novas metodologias para a proteção de direitos. Dentre essas novas metodologias se encontra o instituto do *privacy by design*, o qual propõe adoção do princípio da transparência como um de seus elementos informadores. Em razão da novidade do tema no Brasil, o presente trabalho busca estudar o relacionamento entre o princípio da transparência e a proteção da privacidade no contexto da regulação de tecnologias. Para tanto, são examinadas as contribuições da doutrina jurídica estadunidense a respeito da regulação de tecnologias de informação e comunicação, identificando as reflexões trazidas por diferentes estágios doutrinários. Igualmente, busca-se estudar o desenvolvimento normativo do *privacy by design* e sua operacionalização de acordo com os diplomas mais recentes. Por fim, procura-se estudar especificamente a aplicação do *privacy by design* no que se refere à transparência de algoritmos computacionais de forma delimitar seu alcance e limites. Conclui-se que sob o ponto de vista tecnológico, a transparência de algoritmos possui limitações decorrente de barreiras enfrentadas pela própria Ciência da Computação. Desta forma, faz-se necessário ampliar a transparência sob o ponto de vista organizacional para fins de estimular o desenvolvimento responsável de novas tecnologias e proteger direitos fundamentais constitucionalmente assegurados.

Palavras-chave: regulação; algoritmos computacionais; transparência; *privacy by design*

ABSTRACT

The remarkable development and propagation of information technology has resulted in profound outcomes in our society, affecting fundamental rights of groups and individuals. This scenario of incremental and disruptive shifts stimulates the need to study the stresses between Law, Science, Technology and Innovation. In light of this situation, the regulation of electronic systems and computer algorithms has received considerable attention from scholars and regulatory agents who started to propose new methodologies for the protection of fundamental rights. Among these new methodologies is the privacy by design, which proposes the adoption of transparency as one of its foundational principles. Because of the novelty of the subject in Brazil, this research seeks to study the relationship between the transparency principle and privacy protection in the context of technology regulation. For that matter, the contributions of US the law doctrine about technology regulation are studied, in order to identify the reflections brought by different doctrinal phases. Likewise, the normative development of privacy by design was studied as well as its operationalization according to recent legislation. Finally, the enforcement of privacy by design with regard to computer algorithm transparency was studied in order to identify its reach and boundaries. It was concluded that under a technological point of view, algorithmic transparency faces limitations encountered by Computer Science itself. Because of that, a further increase in organizational transparency is needed in order to promote the responsible development of new technologies and to protect constitutionally assured fundamental rights.

Keywords: regulation; computer algorithms; transparency; privacy by design

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

ACM – Association for Computing Machinery

ARPA – Advanced Research Projects Agency

ARPANET – Advanced Research Projects Agency Network

CEO – Chief Executive Officer

DARPA – Defense Advanced Research Projects Agency

DNS – Domain Name System

DoD – Department of Defense

EDPS – European Data Protection Supervisor

EFF – Electronic Frontier Foundation

EUA – Estados Unidos da América

GDPR – General Data Protection Regulation

IAB – Internet Activities Board

IANA – Internet Assigned Numbers Authority

IBM – International Business Machines Corporation

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IP – Internet Protocol

IPTO – Information Processing Techniques Office

ISO – International Organization for Standardization

ITU – International Telecommunications Union

MIT – Massachusetts Institute of Technology

NBR – Norma Técnica Brasileira

NSF – National Science Foundation

NSFNET – National Science Foundation Network

OECD – Organization for Economic Co-operation and Development

OSI – Open Systems Interconnection

PET – Privacy-Enhancing Technologies

RAND – Research ANd Development Corporation

RFC – Request for Comments

TCP – Transmission Control Protocol

SUMÁRIO

1 INTRODUÇÃO

Na atualidade, o trânsito transfronteiriço de dados e informações se tornou um elemento indissociável da economia mundial. Diante da crescente complexidade de uma sociedade urbana e interconectada, cada vez mais pessoas e organizações públicas e privadas produzem, coletam e utilizam este "novo petróleo" cotidianamente para auxiliar a tomada de todo tipo de decisões. Neste cenário, os dados e informações pertinentes à vida e ao cotidiano de indivíduos também passaram a receber uma maior atenção por parte dos mais diversos setores econômicos.

De fato, conhecer os interesses e as preferências das pessoas se tornou algo vital para qualquer agente econômico que deseje efetivamente competir de forma eficiente num mercado global onde produtos e serviços podem ser produzidos e fornecidos com relativa facilidade em qualquer lugar do mundo. Nesse contexto, atividades diárias que até então não exigiam qualquer fornecimento de informações pessoais para serem realizadas passaram a requerer como condição para a sua realização o fornecimento desses dados, os quais passaram a alimentar bancos de armazenamento cada vez maiores e abrangentes.

Juntamente a este crescimento do uso de dados pessoais, o avanço tecnológico também proporcionou um incremento na utilização de sistemas eletrônicos para coletar e tratar estes dados. Paulatinamente, programas de computador passam a contar com algoritmos sofisticados, os quais permitem, inclusive de forma automatizada, o tratamento de informações a serem utilizadas para apoiar processos decisórios, os quais passaram a levar em conta detalhes individuais cujo conhecimento até então não era possível.

Todavia, apesar deste desenvolvimento tecnológico apresentar facetas positivas em virtude do aprimoramento da eficiência e eficácia dos processos decisórios, possui também consequências negativas. De modo cada vez mais marcante, o aumento indiscriminado da coleta e tratamento de dados, particularmente por meio de tecnologias de informação e comunicação, tem ocasionado uma crescente redução da privacidade de grupos e indivíduos. Com efeito, mesmo pessoas que procuram preservar detalhes de sua vida do conhecimento de terceiros acabam por frequentemente se deparar com casos em que essas informações são de alguma forma obtidas e utilizadas por outros agentes interessados sem o seu consentimento. Por sua vez, esta circunstância tem desencadeado um gradativo processo de perda da autonomia dos indivíduos, o que tem chamado a atenção de estudiosos e reguladores preocupados em estabelecer mecanismos capazes de proteger direitos fundamentais ameaçados por novas

tecnologias. Tendo em vista o protagonismo dos EUA no desenvolvimento de tecnologias de informação e comunicação, estudiosos daquele país protagonizaram debates particularmente importantes no que tange à regulação de tecnologias e arquiteturas de sistemas eletrônicos.

Dessa discussão doutrinária, marcada por diversos estágios e posicionamentos distintos quanto à postura a ser adotada quanto à regulação tecnológica, diversas propostas foram elaboradas com a finalidade de atender às necessidades de proteção da privacidade de indivíduos, muitas delas inclusive passando a ser adotadas por leis ou outras espécies de atos normativos de países ocidentais do hemisfério norte. Dentre essas ideias, o instituto do *privacy by design*, proposto inicialmente na metade da década de 90, passou a receber significativa atenção de entes públicos e privados preocupados com a proteção de dados pessoais especialmente após a edição do *General Data Protection Regulation* pela União Europeia em 2016.

Entre os vários problemas que busca atender quanto à proteção da privacidade, o *privacy by design* também almeja aprimorar o atual cenário de reduzida transparência com a qual dados e informações pessoais são tratados por algoritmos desenvolvidos e utilizados por entidades públicas e privadas. Entretanto, a despeito do maior foco que este instituto tem recebido no exterior, ainda é escassa a literatura a seu respeito no Brasil, particularmente no que tange a reflexões jurídicas a seu respeito e seu papel no que tange à proteção de direitos fundamentais. Por certo, diante da edição da recente Lei Geral de Proteção de Dados em nosso país, a qual estabeleceu significativa regulamentação voltada a impactar o desenvolvimento tecnológico, justifica-se com ainda mais importância o estudo da matéria diante tensões existentes entre direito, ciência, tecnologia e inovação. Assim sendo, o objeto desta investigação será a relação do princípio da transparência com instituto do *privacy by design*. Desse modo, convertendo-se o objeto numa questão central, buscar-se-á responder à pergunta: "qual é a relação do *privacy by design* com a transparência de algoritmos computacionais?".

Tendo em vista a necessidade de estabelecer objetivos parciais que permitam responder à pergunta central, este trabalho terá como objetivos: a) compreender a evolução da discussão doutrinária sobre regulação de tecnologias de informação e comunicação; b) entender como se operacionaliza o *privacy by design*; c) estudar a transparência de algoritmos e seu enquadramento dentro do contexto do *privacy by design.*

No que se refere à sua estrutura, o presente texto será dividido em três seções, cada uma voltada a atender, numa ordem lógica, cada um dos objetivos vinculados à solução da pergunta

central desta dissertação. Deste modo, a Seção **2** iniciará a discussão deste trabalho com o objetivo de realizar uma análise da evolução da discussão acerca da regulação de tecnologias de informação e comunicação. Para tanto, serão examinados cada estágio do debate doutrinário estadunidense, buscando extrair deles os principais elementos necessários para compreender a regulação neste complexo setor. Na sequência, a Seção **3** buscará se aprofundar especificamente no estudo do *privacy by design*, tendo como objetivos identificar sua origem e desenvolvimentos iniciais, evolução normativa e como se operacionaliza, com especial foco para o *General Data Protection Regulation* e, quando possível, para a Lei Geral de Proteção de Dados brasileira. Por último, estabelecidas as premissas necessárias para o adequado entendimento do tema nas seções anteriores, a Seção **4** terá como finalidade examinar o problema central desta pesquisa. Assim, inicialmente esta última seção buscará delimitar o conceito de transparência e sua localização no âmbito da proteção da privacidade. Logo após, buscar-se-á examinar o alcance e limites da transparência de algoritmos computacionais como solução voltada à proteção de dados, dando atenção para as técnicas de abertura do código-fonte e explicação de algoritmos. Por fim, tomando por base os elementos até então levantados, serão avaliadas as possíveis estratégias a serem utilizadas por uma política de *privacy by design* a fim de proporcionar maior transparência ao processo de coleta e tratamento de dados e proporcionar o acesso a informações sobre o tema pelos titulares de dados.

Para tanto, será utilizado o método sistemático de interpretação jurídica com o intuito de analisar o tópico sob seu viés axiológico, buscando assim uma melhor compreensão acerca do relacionamento entre privacidade e transparência no âmbito da regulação da arquitetura de tecnologias de informação e comunicação. Nessa senda, considerando a já referida escassez de estudos sobre o tema no Brasil, a literatura revista neste estudo será preponderantemente em Língua Inglesa, principalmente de autores estadunidenses, porquanto as discussões naquele país se encontram mais amadurecidas do que em nosso país[1]. Tendo em vista o constante e intenso diálogo entre estudiosos e agentes reguladores estadunidenses e europeus, também foram utilizadas fontes sobre o objeto da pesquisa no âmbito da União Europeia.

Finalmente, é necessário fazer a ressalva de que, não obstante o presente trabalho se tratar de uma dissertação de mestrado na área das Ciências Jurídicas e Sociais, buscar-se-á quando eventualmente necessário ou pertinente para o objeto de estudo trazer subsídios da Tecnologia de Informação para o melhor entendimento da matéria. Assim, procurar-se-á manter ao mínimo

[1] Sobre o papel da Língua Inglesa na área da tecnologia de informação em geral, vide: MCCULLOCH, Gretchen. Coding is for Everyone – As Long as You Speak English. **Wired**, 08 apr. 2019. Não paginado.

a terminologia técnica, evitando confundir o leitor não familiarizado com a matéria. Por fim, espera-se que este texto possa contribuir para as discussões atualmente realizadas pela doutrina jurídica brasileira, permitindo avançar a compreensão sobre a regulação de tecnologias de informação e comunicação e o *privacy by design* em nosso país.

2 REGULAÇÃO E TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO: A EVOLUÇÃO DO DEBATE NA DOUTRINA ESTADUNIDENSE

Durante a história da humanidade, o avanço e o desenvolvimento de tecnologias mais eficientes para o compartilhamento, armazenamento e processamento de informações sempre impactaram de forma significativa a sociedade. Com efeito, o manuseio e utilização mais efetivos da informação possibilitou e possibilita progressos tanto no campo social quanto científico[2]. Não obstante, devido a essa capacidade transformadora, tecnologias de informação e comunicação são objeto de significativa atenção e debates por parte de agentes públicos e privados no que diz respeito às questões regulatórias a elas relacionadas[3].

Este cenário de expansão tecnológica acaba inevitavelmente por influenciar o Direito enquanto fenômeno que afeta a sociedade e é por ela reciprocamente afetado, pois novas tecnologias podem não apenas modificar, criar ou extinguir direitos, como também podem modificar, extinguir ou criar formas de ameaçá-los ou danificá-los. Entretanto, como alertam Carlos Alberto Molinaro e Ingo Sarlet, o Direito possui extrema dificuldade em se adequar a esse processo de inovação: em certas ocasiões, vê aquilo que não mais existe; noutras, é incapaz de ver o que está à sua frente[4]. Além disso, a existência de vocabulários e gramáticas completamente distintos torna difícil ou mesmo inexistente a comunicação entre o Direito e campos relacionados às tecnologias de informação e comunicação, tais como a Ciência da Computação e Sistemas de Informação[5].

Por certo, sendo o propósito do presente trabalho estudar o *privacy by design* e sendo a finalidade desse instituto regular tecnologias de informação e comunicação, forçoso reconhecer que a compreensão das teorias por trás desta modalidade de regulação é relevante para entendê-la adequadamente. Nesse sentido, a presente seção buscará realizar uma aproximação a respeito

---

[2] UNITED NATIONS. **Technology and Innovation Report 2018:** Harnessing Frontier Technologies for Sustainable Development. Switzerland: United Nations, 2018. p 108.

[3] Nesse sentido, vide: ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Science, Technology and Innovation Outlook 2016.** Paris: OECD, 2016. p. 17-19.

[4] MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. "Não existe o que panoramicamente vemos no céu": o ponto-cego do direito (políticas públicas sobre regulação em ciência e tecnologia. In.: SAAVEDRA, Giovani Agostini; LUPION, Ricardo (orgs.). **Direitos Fundamentais:** direito privado e inovação. Porto Alegre: EdiPUCRS, 2012. p. 12.

[5] CHACON, Eduarda Moraes. Resistência do Direito à Tecnologia: uma análise teubiana de comunicação e regulação. **The Law, State and Telecommunications Review**, v. 10, n. 2, p. 67-102, oct. 2018. p. 97.

do tema relativo ao fenômeno da regulação[6] [7] das tecnologias de informação e comunicação utilizando como base, de forma preponderante, a produção acadêmica da doutrina estadunidense, em especial as reflexões realizadas por Lawrence Lessig e as análises críticas feitas acerca de sua obra por outros autores.

Evidentemente, sendo o presente trabalho produzido no Brasil, é razoável e pertinente se questionar o motivo da utilização de reflexões jurídicas estrangeiras num estudo acadêmico brasileiro. Com efeito, de acordo Jaap Hage, uma das funções do direito comparado é contribuir para a explicação e compreensão do conteúdo do direito, possibilitando explicar desenvolvimentos legais quando estes forem inspirados em institutos jurídicos estrangeiros[8]. Nesse mesmo sentido, Jan Smits aduz que sendo objetivo comum dos sistemas jurídicos buscar as melhores soluções legais para determinados problemas, é provável que alguns cheguem a estas soluções antes ou melhores que outros[9].

A escolha feita aqui é deliberada e encontra sua razão de ser em dois principais fatores: 1) desde a segunda metade do Século XX, os Estados Unidos da América se situam em posição de liderança no desenvolvimento de tecnologias de informação e comunicação; 2) em virtude dessa colocação de destaque, debates acadêmicos e judiciais envolvendo a regulação de tecnologias de informação e comunicação ocorrem naquele país pelo menos desde o final da

---

[6] Com efeito, embora o termo "regulação" seja frequentemente utilizado sem maiores preocupações, é importante deixar claro que esta palavra é utilizada com vários significados distintos. Nesse sentido, pode ser vista como "leis que servem a grupos de interesse" (STIGLER, George J. The Economic Theory of Regulation. **The Bell Journal of Economics and Management Science,** v. 2, n. 1, p. 3-21, 1971. p. 3), "um produto alocado de acordo com princípios básicos de oferta e demanda" (POSNER, Richard A. Theories of Economic Regulation. **The Bell Journal of Economics and Management Science**, v. 5, n. 2, p. 335-258, 1974. p. 344), "a intervenção estatal no domínio privado" (ORBACH, Barak. What is Regulation? **Yale Journal on Regulation Online**, v. 30, n. 1, p. 1-10, 2012. p. 10), "uma regra ou ordem prescrita para administração ou governo" (BLACK, Henry Campbell. **Black's Law Dictionary.** 4. ed. rev. Saint Paul: West Publishing, 1968. p. 1450), entre outros. De fato, entende-se que este conceito, em razão de sua abertura, é mais apto a descrever a regulação indireta realizada por intermédio de "códigos", conforme se estudará abaixo.

[7] Para fins de estabelecer um acordo semântico e tornar claro o sentido do termo aqui utilizado, o presente trabalho utilizará "regulação" como significando "o efeito conformador de alguma ação ou política estabelecida, de forma intencional ou não, por alguém" (LESSIG, Lawrence. The New Chicago School. **The Journal of Legal Studies**, v. 27, n. 2, p. 661-691, 1998. p. 662). De fato, entende-se que este conceito, em razão de sua abertura, é mais apto a descrever a regulação indireta realizada por intermédio de "códigos", conforme se estudará abaixo. Em sentido relativamente próximo ao de Lessig, Prosser afirma que "regulation is the ustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification" (PROSSER, Tony. Two Visions of Regulation. **Regulation in the Age of Crisis.** Dublin: University Colledge Dublin, 2010. p. 2-3).

[8] HAGE, Jaap. **Comparative Law as Method and the Method of Comparative Law**. Maastricht European Private Law Institute Working Paper, n. 11, mar. 2014. p. 10.

[9] SMITS, Jan M. Comparative Law and its Influence on National Legal Systems. In.: REIMANN, Mathias; ZIMMERMANN, Reinhard (eds.), **The Oxford Handbook of Comparative Law**. Oxford: Oxford University Press, 2006. p. 16.

década de 80[10]. Assim, antes de adentrar na análise do tema propriamente dita, será apresentado um breve relato histórico sobre alguns dos eventos determinantes para que os EUA conquistassem a posição em que se encontram atualmente.

No estágio em que atualmente se encontra, é possível afirmar que o progresso realizado no campo da Ciência da Computação é o principal responsável pela drástica evolução observada no âmbito das tecnologias de informação e comunicação. Em 1965, Gordon Moore, então diretor de pesquisa e desenvolvimento da *Fairchild Semiconductor*, projetou que os computadores passariam a ser sucessivamente mais poderosos em razão da taxa "complexidade de circuitos" *versus* "custo mínimo de produção" praticamente dobrar a cada ano[11]. Esta projeção, posteriormente chamada de "Lei de Moore", se demonstrou correta, permitindo que quantidades cada vez maiores de dados pudessem ser processadas por computadores cada vez mais poderosos[12].

Entretanto, não apenas foi apenas o processamento de dados que progrediu exponencialmente, mas também a sua capacidade de transmissão e comunicação sofreu uma inimaginável evolução. De fato, até a primeira metade do Século XX computadores eram máquinas isoladas que, embora já estivessem gerando impactos profundos na sociedade, ainda não conversavam entre si. Todavia, após o lançamento da *Sputinik I* em 1957 pela União das Repúblicas Socialistas Soviéticas, ficou evidente para os Estados Unidos da América de que era necessário fortalecer a capacidade tecnológica do país para fazer frente ao avanço comunista.

Assim, dentre uma série de medidas voltadas a fortalecer estrategicamente os EUA, em 1958 o então presidente Dwight Eisenhower criou a *Advanced Research Projects Agency (ARPA)*[13], vinculada ao *Department of Defense* (*DoD),* cujo propósito era justamente promover e executar pesquisas avançadas voltadas às necessidades de segurança nacional. Ainda que não tenha sido a única instituição envolvida no financiamento e promoção das tecnologias que permitiram o desenvolvimento e criação da internet nos moldes em que atualmente se conhece,

---

[10] Por exemplo: EGER, John M. The Global Phenomenon of Teleinformatics: an Introduction. **Cornell International Law Journal**, v. 14, n. 2, p. 203-236, 1981. GILBERT, Jonathan. Computer Bulletin Board Operator Liability for User Misuse. **Fordham Law Review**, v. 54, n. 3, p. 439-454, 1985.

[11] MOORE, Gordon E. Cramming More Components onto Integrated Circuits. **Electronics**, p. 114-117, april. 1965. p. 2.

[12] SNEED, Annie. Moore's Law Keeps Going, Defying Expectations. **Scientific American**, 19. maio. 2015. Não paginado.

[13] UNITED STATES OF AMERICA. **Public Law 85-325.** Washington: Office of the Law Revision Counsel, 1958. Posteriormente, a agência estadunidense passou a ser denominada *Defense Advanced Research Projects Agency* (DARPA), nome que mantém até o presente momento.

a *ARPA* desempenhou um papel vital nesse processo, sendo possível afirmar que sua criação é um dos fatores históricos que explicam a predominância estadunidense no setor das tecnologias de informação e comunicação até os dias atuais[14].

Em 1962, quatro anos após a criação da *ARPA*, Joseph Licklider foi nomeado para ser o primeiro diretor do recém-criado *Information Processing Techniques Office* (*IPTO*), o qual tinha a finalidade de concentrar os esforços da agência voltados à criação de departamentos de ciência da computação em universidades, estabelecimento de técnicas para compartilhamento de tempo[15] e desenvolvimento de redes. Embora não tivesse conhecimento técnico sobre como criar e operacionalizar uma rede de computadores, Licklider reconhecia a importância que tal tecnologia representaria para o desenvolvimento das atividades voltadas à pesquisa. Assim, em 1963, por intermédio de um memorando, propôs aos seus colegas que avaliassem as possíveis implicações que o intercâmbio de informações por intermédio de uma rede de computadores traria para suas atividades[16]. O conceito por trás da *Intergalactic Computer Network* proposta por Licklider permitia aos usuários compartilhar informações e recursos entre si de uma forma até então não experimentada pela ciência da computação, sendo atualmente considerado como sendo o esboço do que se tornou a internet[17]. Ainda que Licklider tenha deixado o *IPTO* em 1964, seu pensamento influenciou profundamente os futuros diretores do órgão, dentre eles Ivan Sutherland e Robert Taylor[18], os quais também desempenharam papel relevante ao financiar o desenvolvimento da primeira rede de computadores, a *ARPANET*.

No mesmo período em Licklider teorizava sobre o funcionamento de sua *Intergalactic Computer Network* e influenciava a comunidade científica da época[19], diversos avanços cruciais para o desenvolvimento de uma rede de computadores foram sendo obtidos. Entre 1961 e 1964 Leonard Kleinrock, do *Massachusett Institute of Technology* (MIT), Paul Bauran, da *RAND*

---

[14] ACKERMAN, Evan. 60 Years of DARPA's Favorite Toys: The Past and Future of Cutting-edge technology was on display at DARPA's 60th anniversary conference. **IEEE Spectrum**, 26 set. 2018. Não Paginado.

[15] Em resumo, trata-se de uma técnica computacional que buscava permitir que vários usuários utilizassem ao mesmo tempo o mesmo computador, compartilhando seus recursos. Em virtude do elevado custo de produção, instalação e manutenção de um computador nos primórdios da computação, esta técnica buscava aproveitar os recursos computacionais que de outra forma seriam desperdiçados se o equipamento ficasse ocioso. Durante parte significativa do tempo de utilização, a capacidade de processamento de um computador não é efetivamente utilizada em sua capacidade máxima, pois um único usuário gastava a maior parte do tempo apenas introduzindo ou visualizando dados no computador e não efetivamente realizando operações. Posteriormente, esse conceito foi utilizado para permitir o compartilhamento de recursos computacionais em rede.

[16] LICKLIDER, Joseph Carl Robnett. **Memorandum for Members and Affiliates of the Intergalactic Network.** Washington: Advanced Research Projects Agency, 1963. Não paginado.

[17] LEINER, Barry M. *et alli*. **Brief History of the Internet.** Reston: Internet Society, 1997. p. 3.

[18] Idem, p. 3.

[19] ROBERTS, Lawrence G. The Evolution of Packet Switching. **Proceedings of the IEEE**, v. 66, n. 11, p. 1307-1313, nov. 1978.

Corporation, e Donald Davies, do *National Physical Laboratory*, publicaram os primeiros trabalhos sobre comunicação utilizando comutação de pacotes. Crucial para o funcionamento da internet até os dias de hoje, esta tecnologia permite que a comunicação entre computadores ocorra através da transmissão de sucessivos pacotes de informação ao contrário de um único circuito contínuo como nas redes de telefonia até então existentes, permitindo que a troca de dados ocorra de forma muito mais estável e segura[20].

Estabelecidos os protocolos essenciais para o funcionamento da rede, em 1969 foi realizada a primeira troca de mensagens entre dois computadores, localizados em universidades distintas, por meio do financiamento e troca de experiências proporcionado pela *ARPA*. Com efeito, a partir do sucesso de sua primeira comunicação, a *ARPANET* rapidamente foi crescendo em número de usuários e computadores conectados. Esta crescente complexidade acarretou o desenvolvimento de novos protocolos destinados a resolver desafios de escala trazidos pela expansão da rede, tais como o *Transmission Control Protocol* (*TCP*) e o *Internet Protocol* (*IP*), em 1974[21], e o *Domain Name System* (*DNS*), em 1983[22]. Concomitantemente a essa expansão, gradativamente o uso de tecnologias de comunicação em rede foi deixando de ser uma exclusividade militar. Assim, incentivado pela *National Science Foundation (NSF),* o uso de redes de computadores com finalidades acadêmicas se disseminou, possibilitando a interconexão entre universidades e centros pesquisas por intermédio da *NSFNET*. Enfim, a partir final da década de 80 e início da década 90, em razão de diversas políticas públicas de incentivo ao mercado por autoridades estadunidenses, do desenvolvimento da *world wide web*[23] e do lançamento dos primeiros *softwares* de navegação, o emprego da internet para fins privados e comerciais se popularizou, permitindo que um número cada vez maior de pessoas tivesse acesso à rede mundial de computadores.

Conforme se pode perceber desta breve narrativa apresentada, o cenário das tecnologias de informação e comunicação, especialmente no que se refere ao desenvolvimento da internet, é

---

[20] LEINER, op. cit., p. 5.

[21] Em síntese, os protocolos TCP e IP, além de permitirem o controle sobre o fluxo e transmissão de pacotes dados, também permitem a existência de uma rede de computadores de maior complexidade, porquanto estabelecem um sistema de endereçamento lógico que permite aos computadores que utilizam estes protocolos se localizarem e trocarem dados (CERF, Vinton G.; KAHN, Robert E. A Protocol for Packet Network Intercommunication. **IEEE Transactions on Communications**, v. 22, n. 4, p. 637-648, may. 1974. p. 12).

[22] Numa rápida explicação, o *Domain Name System* consiste num protocolo que permite um gerenciamento mais eficiente dos recursos de numeração do protocolo IP por intermédio da criação de endereços alfanuméricos chamados de "nomes de domínio" (MOCKAPETRIS, Paul. **Request for Comments 882:** Domain Names – Concepts and Facilities. [s.l.]: Network Workink Group, 1983. p. 2-3).

[23] BERNERS-LEE, Tim. **Information Management:** a Proposal. Geneva: *Conseil Européen pour la Recherche Nucléaire*, 1989. Não paginado.

fortemente marcado pela predominância de atores estadunidenses. Por certo, apesar de existirem diversos pesquisadores e instituições em outros países envolvidos no desenvolvimento e estudos na área da ciência da computação durante a segunda metade do Século XX, a forte interação entre atores do governo, academia e indústria existente nos EUA fez com que este país se tornasse a mais importante potência mundial neste setor. Dessa maneira, não é particularmente surpreendente que a interação entre o Direito e as tecnologias de informação e comunicação tenha ocorrido de forma mais precoce naquele país, suscitando debates relevantes na academia jurídica estadunidense que até hoje influenciam os demais sistemas jurídicos, mesmo quando não estruturados sob a *common law*.

Assim sendo, para que o leitor possa se situar e compreender adequadamente o objeto estudado neste trabalho, esta seção terá como objetivo examinar o debate doutrinário a respeito da regulação de tecnologias de informação e comunicação, examinando as principais etapas que o delimitam, seus principais autores, teses e argumentos defendidos. Igualmente, é importante fazer a ressalva de que embora a presente seção **2** se dedique a descrever os estágios da discussão doutrinária, a ordem em que esses são apresentados não segue rigorosamente uma cronologia sucessiva[24]. De fato, ainda que seja possível identificar um intervalo de tempo relativamente determinado que concentre a publicação de artigos em defesa de argumentos representativos de cada um dos estágios descritos nas subseções seguintes, alguns autores seguiram defendendo seus posicionamentos já durante o estágio subsequente, embora já respondendo às críticas feitas por outros estudiosos. Assim, buscou-se reunir em cada estágio aqueles autores cujos posicionamentos possuem certo alinhamento de premissas e/ou conclusões de modo a facilitar a compreensão do tema.

Desta forma, concluída a breve contextualização histórica e feitas as devidas ressalvas, resta informar a ordem em que serão apresentados os cada um dos estágios do debate doutrinário estadunidense: a subseção **2.1** apresentará aquele que pode ser caracterizado como sendo o primeiro estágio da discussão na doutrina dos EUA, o qual foi profundamente marcado por argumentos que transitavam entre a impossibilidade, a ilegitimidade ou mesmo desnecessidade de regulação. Logo a seguir, a subseção **2.2** descreverá a etapa subsequente do debate doutrinário, já delineado com posições menos otimistas sobre os efeitos das tecnologias

[24] Não obstante, é necessário informar que, principalmente no que diz respeito à delimitação das características dos dois primeiros estágios, os artigos *Cyberspace 2.0* de Neil Weinstock Netanel (NETANEL, Neil Weinstock. Cyberspace 2.0. **Texas Law Review**, v. 79, p. 447-491, dez. 2000) e *The New Chicago School* de Lawrence Lessig (LESSIG, Lawrence. The New Chicago School. **The Journal of Legal Studies**, v. 27, n. 2, p. 661-691, 1998). serviram de inspiração para esta delimitação.

de informação e comunicação sobre a sociedade e o relacionamento destas com a regulação estatal. Nesse sentido, embora este estágio doutrinário possa ser identificado em vários autores, se dedicará a subseção **2.2.1** para apresentar e analisar com mais atenção as reflexões feitas por Lawrence Lessig, em especial o modelo regulatório por ele delineado em seu livro *Code and Other Laws of Cyberspace*. Finalmente, a subseção **2.3** examinará o terceiro estágio da discussão doutrinária, no qual a academia jurídica, fortemente influenciada pelo trabalho de Lessig, realiza uma releitura do marco teórico do autor, apresentando críticas ao seu trabalho e delineando pontos não abordados em sua obra.

2.1 DO PRIMEIRO ESTÁGIO DO DEBATE DOUTRINÁRIO: A IMPOSSIBILIDADE, A ILEGITIMIDADE E A DESNECESSIDADE DE REGULAÇÃO DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

Embora recebessem investimentos massivos de entes estatais, a comunidade de cientistas responsáveis pela criação e desenvolvimento dos primeiros protocolos, equipamentos e demais tecnologias voltadas ao cenário das tecnologias de informação e comunicação sempre gozou de uma significativa liberdade em suas atividades[25]. De fato, durante a primeira metade da década de 90, em inúmeros momentos personagens importantes do setor técnico demonstraram de forma enfática seu posicionamento contrário a uma interferência do Estado, suas normas, burocracia e formalismos.

O primeiro exemplo ilustrativo que pode ser citado é a apresentação feita em 1992 por David Dana Clark, ex-diretor da *Internet Activities Board* (*IAB*), no 24ª congresso da *Internet Engineering Task Force* (*IETF*), na qual cunhou a famosa frase: "*We reject: kings, presidents and voting. We believe in: rough consensus and running code*"[26] [27]. Posteriormente elevada a um *status* de lema não-oficial da comunidade técnica da internet, esta frase representa um sentimento daquele grupo de que processos formais e complexos para a tomada de decisão

[25] Curiosamente, a presença de dinheiro público ou mesmo agentes públicos no setor de alta tecnologia é um fenômeno identificado em diversos países. Sobre o assunto, exemplificativamente: BALDING, Christopher; CLARKE, Donald C. Who Owns Huawei. **SSRN**, 17 apri. 2019.

[26] Original em Inglês. Tradução livre: "Nós rejeitamos: reis, presidentes e votações. Nós acreditamos em consenso grosseiro e código que funcione" (CLARK, David D. **Views of the Future:** A Cloudy Crystal Ball – Visions of the Future. [s.l.]: Internet Engineering Task Force, 1992. p. 19).

[27] Em razão da NBR 10520:2002, que normaliza o tema referente a citações em documentos, não fazer qualquer menção expressa a respeito do assunto, o presente trabalho optará por citar o texto em sua língua original, fornecendo a tradução livre, feita pelo autor, no rodapé.

representam um empecilho para o desenvolvimento de sistemas e códigos eficazes e eficientes. Verdadeiramente, esta constatação não deixa de possuir alguma correção quando se constata que um fator frequentemente citado para a vitória do protocolo TPC/IP contra o protocolo OSI foi justamente a informalidade dos processos de decisão da comunidade técnica da internet[28]. Esta ausência de estrutura definida lhe conferia uma eficiência e eficácia na elaboração de tecnologias incapaz de ser superada pelo lento e burocrático processo da *International Standard Organization* (*ISO*) e da *International Telecommunications Union* (*ITU*)[29], responsáveis pelo desenvolvimento do protocolo OSI.

Contudo, não foi apenas David Clark que demonstrou publicamente sua opinião quanto à "inadequação" de preocupações jurídicas clássicas no contexto de tecnologias. Em 1994, Jonathan Bruce Postel, ou simplesmente Jon Postel, desempenhava pessoalmente as atividades relacionadas à *Internet Assigned Numbers Authority* (*IANA*)[30] e possuía tamanho respeito e importância entre seus colegas ao ponto de ser chamado de "Czar/ Deus da internet" [31]. Assim, buscando organizar o sistema de delegação e estrutura do DNS, editou a RFC 1591, na qual afirmou que: *"Concerns about 'rights' and 'ownership' of domains are inappropriate. It is appropriate to be concerned about 'responsibilities' and 'service' to the community"* (grifos no original)[32]. Ora, desviar de preocupações sobre "direitos" e "propriedade" era crucial pois implicava um distanciamento do Estado, cuja ausência, conforme asseverava Vinton Cerf, foi justamente o que permitiu à internet se expandir[33].

Estando imersos numa comunidade cujo foco principal era desenvolver tecnologias cada vez mais robustas, Clark, Cerf e Postel tinham a preocupação de que a intervenção de interesses

---

[28] CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória da Internet no Brasil:** Do Surgimento das Redes de Computadores à Instituição dos Mecanismos de Governança. 2006. 239 f. Dissertação (Mestrado em Ciências de Engenharia de Sistema e Computação) – Faculdade de Engenharia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. p. 49. RUSSEL, Andrew L. OSI: The Internet that Wasn't. **IEEE Spectrum**, 30 jul, 2013. Não paginado.

[29] Nesse sentido: RUSSEL, Andrew L. 'Rough Consensus and Running Code' and the Internet-OSI Standards War. **IEEE Annals of the History of Computing**, v. 28, n. 3, p. 48-61, jul./set. 2006. p. 53.

[30] Essencial para o funcionamento da Internet, a *IANA* tem como funções a designação de protocolos técnicos para o funcionamento da rede, a distribuição e controle dos recursos de numeração do protocolo IP e a administração da zona raiz do DNS (INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. **The IANA Functions:** an Introduction to the Internet Assigned Numbers Authority (IANA) Functions. Los Angeles: Internet Corporation for Assigned Names and Numbers, 2015. p. 4).

[31] Original em Inglês. Tradução livre: "Preocupações sobre 'direitos' e 'propriedade' de domínios são inapropriadas. É apropriado se preocupar com 'responsabilidades' e 'serviço' à comunidade"(POSTEL, Jon. **Request for Comments 349:** Proposed Standard Socket Numbers. Los Angeles: Network Working Group, 1972. p. 1. 'God of the Internet' is dead. **BBC News**, London, 19 oct. 1998. Não paginado).

[32] POSTEL, Jon. **Request for Comments 1591:** Domain Name Structure and Delegation. Marina Del Rey: Network Working Group, 1994. p. 5.

[33] CERF, Vinton G. Building an Internet Free of Barriers. **New York Times**, New York, 27 jul. 1997. Não paginado.

estranhos – principalmente estatais, mas também empresariais – prejudicaria suas criações. Para além da comunidade exclusivamente técnica, outros atores relevantes também demonstravam posicionamento igualmente cético quanto à intervenção regulatória estatal. Desses, John Perry Barlow, fundador da *Electronic Frontier Foundation* (*EFF*)[34], talvez tenha sido responsável pelas manifestações mais emblemáticas quanto ao tema.

Primeiramente, em seu ensaio *The Economy of Ideas*[35], Barlow buscou avaliar as implicações que o novo modelo econômico trazido pela internet[36] e pela era digital traria para o regime clássico da propriedade – especialmente a propriedade intelectual – frente à sua função como estímulo à produção de conhecimento. Nesse sentido, dentre outras questões, o autor aduziu que a inexperiência dos juristas frente a uma economia "imaterial" acarretaria uma equivocada tentativa de aplicar leis antigas a este novo cenário. Tendo em vista que o "Contrato Social" no ciberespaço ainda estaria sendo redigido, a melhor conduta a ser adotada pelo Direito seria se manter afastado, deixando aos agentes envolvidos nesta área desenvolver seus próprios códigos, práticas e sistemas éticos[37], os quais surgiriam em razão da natureza detestar o vácuo[38]. Na opinião extremamente crítica desse pensador, "*Faith in law will not be an effective strategy for high-tech companies. Law adapts by continuous increments and at a pace second only to geology"*[39]. Assim, Barlow concluiu este seu primeiro ensaio prevendo, em especial, que: a) as proteções aos direitos dependeriam mais da ética e de soluções tecnológicas do que do sistema jurídico; b) criptografia seria a base técnica para muitas dessas proteções; c) a economia do futuro seria baseada no relacionamento e não na posse.

Embora o trabalho anteriormente referido tenha trazido reflexões importantes, uma das mais significativas e influentes obras do autor foi a sua "Declaração de Independência do

[34] Fundada em 1990, a *EFF* é uma entidade civil não-governamental sem fins lucrativos cuja finalidade é defender e promover as liberdades civis no mundo digital. Para atingir seus objetivos, a *EFF* patrocina ou auxilia em processos judiciais, realiza mobilizações políticas, entre outras ações (ELECTRONIC FRONTIER FOUNDATION. **About EFF.** San Francisco: Electronic Frontier Foundation, 2018. Não paginado).
[35] BARLOW, John Perry. The Economy of Ideas. **Wired**, 01 mar. 1994. Não paginado.
[36] Para uma análise introdutória mais detida sobre a economia da internet em seus primórdios, vide: MCKNIGHT, Lee W.; BAILEY, Joseph P. An Introduction to Internet Economics. **Journal of Electronic Publishing** v. 1, n. 1&2, jan. 1995. Não paginado.
[37] BARLOW, op. cit., 1994. Não paginado.
[38] Idem.
[39] Idem. Original em Inglês. Tradução livre: "A fé no direito não será uma estratégia efetiva para companhias de alta tecnologia. O direito se adapta incrementalmente, numa velocidade superada apenas pela geologia".

Ciberespaço"[40]. Neste manifesto endereçado em 1996 aos "Governos do Mundo Industrial", Barlow afirmou que[41]:

> […] *I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us.* ***You have no sovereignty where we gather.*** [...]. *I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us.* ***You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.*** […]. *You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts.* ***Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means.*** *We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.* [...] ***Your legal concepts of property, expression, identity, movement, and context do not apply to us.*** *They are all based on matter, and there is no matter here. Our identities have no bodies, so, unlike you,* ***we cannot obtain order by physical coercion****. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions.* ***The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.*** (**grifou-se**)

Escrita num momento o Congresso estadunidense havia acabado de aprovar a *Telecommunications Act of 1996*[42], a qual teve profundo impacto no setor de infraestrutura da internet, a mensagem de Barlow representava uma ideia comum entre os usuários de tecnologias de informação e comunicação da época: a de que o Estado deveria permanecer fora desse ecossistema, pois seus próprios membros seriam capazes de resolver seus problemas. Esta

---

[40] BARLOW, John Perry. **A Declaration of the Independence of Cyberspace.** Davos: [.s.n.], 1996. Não paginado.

[41] Original em Inglês. Tradução livre: "[...] Eu venho do Ciberespaço, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem a sós. Vocês não são bem-vindos entre nós. Vocês não têm soberania onde nos reunimos. [...]. Eu declaro o espaço social global que estamos construindo naturalmente independente das tiranias que vocês buscam nos impor. Vocês não têm direito moral de nos governar nem tampouco possuem quaisquer métodos de imposição que tenhamos motivos para temer. [...]. Vocês alegam que existem problemas entre nós que vocês precisam resolver. Vocês usam esta alegação como uma desculpa para invadir nossos lares. Muitos destes problemas não existem. Onde existam conflitos reais, onde existam injustiças, nós iremos identifica-los e resolvê-los por nossos meios. Nós estamos formando nosso próprio Contrato Social. Esta governança irá surgir de acordo com as condições de nosso mundo e não do seu. Nosso mundo é diferente. [...]. Seus conceitos jurídicos de propriedade, expressão, identidade, movimento e contexto não se aplicam a nós. Eles são todos baseados em matéria e não há matéria aqui. Nossas identidades não possuem corpos, então, ao contrário de vocês, nós podemos obter ordem pela coerção física. Nós acreditamos que da ética, interesses pessoais esclarecidos e o bem comum nossa governança irá emergir. Nossas identidades podem estar distribuídas ao redor de muitas jurisdições. A única lei que todas as nossas culturas constituintes poderiam geralmente reconhecer é a Regra de Ouro. Nós esperamos que sejamos capazes de construir nossas próprias soluções com base nela. Mas não podemos aceitar as soluções que vocês estão tentando impor " (Idem).

[42] UNITED STATES OF AMERICA. **Public Law 104-104.** Washington: Government Publishing Office, 1996. Posteriormente, esta lei teve parte de seu Título V, destinado a regulamentar comunicações "indecentes e obscenas", julgado inconstitucional pela Suprema Corte no caso *Reno v American Civil Liberties Union* em razão de violar os direitos de liberdade de expressão protegidos pela 1ª Emenda à Constituição (SUPREME COURT. **Reno v. American Civil Liberties Union.** 521 U.S. 844 (1997)).

concepção ecoada pelo autor identificava no ente estatal uma incapacidade de compreender esse novo cenário de desenvolvimento tecnológico, o qual seguia tentando resolver problemas novos – alguns que talvez até não fossem problemas – com ferramentas ultrapassadas, pertencentes a uma "era" anterior[43].

Todavia, embora a mensagem de Barlow tenha recebido grande atenção, ela ainda parecia mais baseada numa ideia de ilegitimidade derivada da baixa popularidade do *Telecommunications Act,* da suposta "falta de consentimento" e da violação aos direitos de expressão[44] dos usuários da rede do que em aspectos efetivamente práticos sob o ponto de vista tecnológico. Assim, dentre outros autores que buscaram compreender melhor a questão, David Post pode ser indicado como sendo um dos mais importantes estudiosos desse período[45]. Realmente, ele concordava com a assertiva de que naquele momento as regras que governavam as tecnologias de informação e comunicação ainda não eram claras. Porém, para este estudioso era igualmente necessário perquirir *quem* faria estas regras e *como* elas seriam fiscalizadas[46], porquanto essas questões possuiriam precedência lógica frente outras matérias de direito substantivo.

Desse modo, examinando as características e a natureza das redes de computadores, Post chamou atenção para uma primeira grande constatação: redes não são "simplesmente" regidas pelos protocolos de funcionamento estipulados pelo seu administrador, elas efetivamente *não existem* fora desses protocolos[47]. Portanto, os "controladores" da rede, responsáveis pela

---

[43] DYSON, Esther *et alli*. Cyberspace and the American Dream: A Magna Carta for the Knowledge Age. **The Information Society**, v. 12, n. 3, p. 295-308, 1996. p. 308.

[44] Curiosamente, embora a liberdade de expressão tenha inicialmente fosse utilizada como fundamento libertário contra atos arbitrários do Estado, este argumento gradativamente tem sido utilizado por grandes empresas de tecnologia de informação para evitar a redução de seus poderes de mercado (EDWARDS, Haley Sweetland. How the First Amendment Became a Tool for Deregulation. **Time**, 19 jul. 2018. Não paginado).

[45] Seja individualmente ou em conjunto com David R. Johnson, David Post possui um significativo acervo de obras dedicadas ao tema das tecnologias de informação e comunicação, a saber: POST, David G. Anarchy, State, and the Internet: an Essay on Law-Making in Cyberspace. **Journal of Online Law**, 1995. POST, David G. Governing Cyberspace. **Wayne Law Review**, v. 43, p. 155-171, 1996. JOHNSON, David R.; POST, David. Law and Borders: The Rise of Law in Cyberspace. **Stanford Law Review**, v. 48, p. 1367-1402, 1996. JOHNSON, David R.; POST, David. And How Shall the Net be Governed? A Meditation on the Relative Virtues of Decentralized Emergent Law. In: KAHIN, Brian; KELLER, James H (eds.). **Coordinating the Internet.** Cambridge: MIT Press, 1997. JOHNSON, David R.; POST, David. Chaos Prevailing in Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems. **Chicago-Kent Law Review**, v. 73, n. 4, p. 1055-1099, 1998. JOHNSON, David R.; POST, **David. The New 'Civic Virtue' of the Internet:** A Complex Systems Model for the Governance of Cyberspace. [s.l.]: The Emerging Internet, 1998. POST, David G. What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace. **Stanford Law Review**, v. 52, p. 1439-1459, may. 2000. POST, David G. Against "Against Cyberanarchy". **Berkeley Technology Law Journal**, v. 17, p. 1366-1387, 2002.

[46] POST, David G. Anarchy, State, and the Internet: an Essay on Law-Making in Cyberspace. **Journal of Online Law**, 1995. Não paginado.

[47] Idem.

definição destas especificações técnicas, exerceriam um papel relevante na definição de um "direito do ciberespaço"[48]. Igualmente, estes mesmos controladores também seriam um ponto focal importante para o estabelecimento de obrigações regulatórias destinadas ao ciberespaço.

Além desses aspectos, o autor refletiu que, sendo a efetividade de uma sanção inversamente proporcional à capacidade de "fuga" do indivíduo sancionado, a facilidade que os usuários de redes possuiriam para trocar de ambiente afetaria fortemente a capacidade do Estado de exercer a sua soberania[49]. Para ele, o fato da arquitetura da internet ser descentralizada e da informação armazenada em uma jurisdição poder facilmente ser transferida para outra acarretaria consequências importantes no que diz respeito à capacidade de regulação pelos entes estatais[50]. Em virtude desses fatores, existiria uma espécie de competição entre redes individuais, as quais competiriam para implementar arquiteturas e protocolos mais compatíveis com a preferência individual dos usuários. Em termos sistêmicos, este "mercado por protocolos" acarretaria um inevitável "dilema do prisioneiro"[51] no qual administradores e controladores de redes seriam obrigados a desenvolver mecanismos de coordenação, sob pena de serem incapazes de conter as externalidades negativas desse cenário[52].

Esse autor gradativamente refinou seus argumentos normativos em defesa da importância de se encontrar uma metodologia para a definição de regras aceitáveis na seara das tecnologias de informação e comunicação. Inicialmente, o foco de sua atenção se fixou para o fato de que a "territorialidade", enquanto critério de aplicação de leis[53] e até mesmo enquanto elemento do conceito de Estado[54], já não era capaz de responder adequadamente aos problemas trazidos pela

---

[48] Idem.
[49] Idem.
[50] De fato, trata-se de exemplo típico do fenômeno chamado de "arbitragem regulatória" (em alusão ao instituto da "arbitragem" estudado pelas Ciências Econômicas), o qual ocorre quanto sujeitos regulados possuem mobilidade suficiente em suas operações a ponto de poder escolher sob quais regimes regulatórios desejam ser sujeitados (MURRAY, Andrew; SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. **Modern Law Review**, v. 65, n. 4. P. 491-516, jul. 2002. p. 494. FROOMKIN, Micheal A. The Internet as a Source of Regulatory Arbitrage. **Symposium on Information, National Policies, and International Infrastructure**, jan. 1996. Não paginado).
[51] Estudado no âmbito da teoria dos jogos, o "dilema do prisioneiro" é um modelo de jogo de uma rodada no qual duas partes precisam escolher, de forma independente, entre cooperar ou competir. Neste modelo, os incentivos são estruturados da seguinte forma: a) se ambas cooperarem, as duas saem beneficiadas; b) se ambas competirem, as duas saem prejudicadas; c) se apenas uma parte competir, esta será mais beneficiada do que se cooperasse. Em virtude destes fatores, existe probabilidade de ambas as partes, ao decidirem individualmente por obter o melhor benefício para si, acabarem por obter o pior resultado possível (BURK, Dan L. Virtual Exit in the Global Information Economy. **Chicago-Kent Law Review**, v. 73, n. 4, p. 943-995, 1998. p. 971).
[52] POST, David G. Anarchy, State, and the Internet: an Essay on Law-Making in Cyberspace. **Journal of Online Law**, 1995. Não paginado.
[53] POST, David G. Governing Cyberspace. **Wayne Law Review**, v. 43, p. 155-171, 1996. p. 157.
[54] POST, David G. The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed. **Indiana Journal of Global Legal Studies**, v. 5, n. 2, p. 521-543, 1998. p. 543.

expansão de redes de computadores localizadas nos mais diversos locais do mundo. Levando em conta os protocolos então existentes para o armazenamento e – principalmente – para o tráfego de dados entre redes, era irrelevante a existência de fronteiras geográficas[55]. Não sendo um sistema feito para a "conveniência de advogados", a internet teria seus efeitos sentidos em diversos locais da rede, de modo praticamente simultâneo[56]. Assim, postulou que embora o Direito, enquanto debate racional de um grupo acerca de seus valores essenciais, continuasse a existir, ele não seria mais, nem poderia ou deveria ser o mesmo Direito aplicável a territórios físicos e geograficamente definidos[57].

Entretanto, talvez uma das ideias mais interessantes de David Post, em conjunto com David Johnson, para o estudo da regulação das tecnologias de informação e comunicação tenha sido a proposta de utilização de elementos da teoria dos sistemas complexos[58] para melhor explicar a governança da rede mundial de computadores[59]. Para tanto, os autores observaram que a internet possui as características de um sistema complexo, a saber: a) os indivíduos que a compõem possuem características e estados heterogêneos; b) as mudanças de estado sofridas por cada indivíduo acarretam efeitos no estado dos demais; c) o estado de cada indivíduo é definido como uma função do estado dos demais indivíduos[60]. Assim, a inclusão sucessiva de indivíduos e variáveis no sistema aumentaria exponencialmente a dificuldade para encontrar soluções utilizando mecanismos "clássicos", tais como o Estado e a regulação centralizada. Desse modo, os autores sustentaram a necessidade de abandono desses mecanismos, porquanto seriam incapazes de fornecer respostas adequadas aos problemas enfrentados num mundo global e sem fronteiras físicas[61].

---

[55] POST, David G. Governing Cyberspace. **Wayne Law Review**, v. 43, p. 155-171, 1996. p. 161.
[56] Idem, 162.
[57] JOHNSON, David R.; POST, David. Law and Borders: The Rise of Law in Cyberspace. **Stanford Law Review**, v. 48, p. 1367-1402, 1996. p. 1402.
[58] De forma extremamente sintética, a teoria dos sistemas complexos é uma área do conhecimento que busca compreender o funcionamento dos "sistemas complexos", definidos como sistemas compostos por muitas partes que interagem entre si, cujo comportamento e funcionamento tornam difícil de formular modelos descritivos ou preditivos (GARE, Arran. Systems Theory and Complexity Introduction. **Democracy & Nature**, v. 6, n. 3, p. 327-339, 2000. p. 329-332. GIUDICE, James M. Through the Lens of Complex Systems Theory: Why Regulators Must Understand the Economy and Society as a Complex System. **University of Richmond Law Review**, v. 51, p. 101-119, 2016. p. 103-105).
[59] JOHNSON, David R.; POST, David. Chaos Prevailing in Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems. **Chicago-Kent Law Review**, v. 73, n. 4, p. 1055-1099, 1998.
[60] Idem, p. 1060-1061.
[61] JOHNSON, David R.; POST, David. **The New 'Civic Virtue' of the Internet:** A Complex Systems Model for the Governance of Cyberspace. [s.l.]: The Emerging Internet, 1998. Não paginado.

Utilizando a teoria dos sistemas complexos como argumento normativo em prol de suas conclusões[62], Post e Johnson afirmaram que: a) a decisão por modelos descentralizados poderia funcionar de forma eficiente para a definição de regras, porquanto indivíduos poderiam facilmente migrar entre cada sistema de acordo com as suas preferências; b) a divisão do processo decisório em mecanismos menores e locais poderia acarretar em decisões melhores em razão de existir menos assimetria informacional sobre questões locais nestes espaços. Em resumo, os autores acreditavam que embora a competição entre sistemas menores pudesse gerar resultados que, numa perspectiva menor, fossem ineficientes, numa perspectiva global o sistema completo seria mais eficiente do que pela utilização de outras técnicas, ocasionando um melhor encaixe dos diversos interesses envolvidos[63].

Conquanto houvesse consenso entre os autores desse primeiro estágio do debate doutrinário de que a regulação estatal deveria permanecer afastada do âmbito das novas tecnologias de informação e comunicação, havia uma certa discordância sobre se, em virtude das sucessivas inovações tecnológicas, seria necessária a criação de um novo ramo do Direito aplicável a esta área. Para o juiz estadunidense Frank Easterbrook, a resposta era não[64].

Com efeito, embora não criticasse que juristas estudassem outras áreas do conhecimento, Easterbrook era extremamente contrário à proposta de criação de áreas específicas das Ciências Jurídicas destinadas ao estudo de um suposto "ramo especial" do Direito, em particular na seara tecnológica. Para o autor, ideias voltadas ao desenvolvimento de novos ramos jurídicos seriam tão inúteis quanto a criação de um "direito dos cavalos", porquanto somar o conhecimento de duas áreas sobre as quais se sabe pouco a respeito apenas resultaria no pior de dois mundos[65]. Assim, considerando que as noções eventualmente obtidas acerca de tecnologias rapidamente se tornam ultrapassadas, o ideal seria que o jurista focasse seus estudos em disciplinas e princípios gerais do Direito, já que, na sua opinião, a maior parte dos comportamentos neste ecossistema seria facilmente classificável dentro de regimes já existentes[66]. Ademais, os operadores do direito, generalistas e com pouco conhecimento e

---

[62] I JOHNSON, David R.; POST, David. Chaos Prevailing in Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems. **Chicago-Kent Law Review**, v. 73, n. 4, p. 1055-1099, 1998, p. 1089.
[63] JOHNSON, David R.; POST, David. **The New 'Civic Virtue' of the Internet:** A Complex Systems Model for the Governance of Cyberspace. [s.l.]: The Emerging Internet, 1998. Não paginado.
[64] EASTERBROOK, Frank H. Cyberspace and the Law of the Horse. **The University of Chicago Legal Forum**, p. 207-216, 1996.
[65] Idem, p. 207.
[66] Idem, p. 208-210.

treinamento para coletar dados e analisar hipóteses empiricamente[67], não deveriam intervir naquilo que desconhecem, mas sim deixar os agentes envolvidos no setor realizar seus próprios acordos.

Como é possível verificar, Easterbrook se filiava à concepção de que o Estado e a regulação dele decorrente deveriam adotar uma posição de deferência frente às soluções concebidas pelos próprios personagens envolvidos no setor de tecnologias de informação e comunicação[68]. Desse modo, defendia que os juristas se limitassem a estabelecer um ambiente propício e seguro à realização de negócios jurídicos mediante o foco em três objetivos[69]: a) criar regras mais claras; b) criar direitos de propriedade onde estes não existem; c) facilitar a formação de instituições de incentivo a negócios jurídicos. Com estas medidas, restariam estabelecidas as condições necessárias para o desenvolvimento e evolução desse novo ecossistema.

2.2 DO SEGUNDO ESTÁGIO DO DEBATE DOUTRINÁRIO: A ARQUITETURA DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO COMO MECANISMO REGULATÓRIO

Conforme se relatou na primeira parte desta seção, durante o primeiro estágio do debate doutrinário prevaleceu entre os autores o entendimento segundo o qual a regulação estatal deveria permanecer afastada do cenário das tecnologias de informação e comunicação no mínimo em razão da inabilidade dos legisladores de compreender as vicissitudes dessa seara. Não obstante, a disseminação das novas tecnologias e o amadurecimento da discussão permitiu não apenas uma melhor análise sobre os argumentos da "primeira geração" da doutrina estadunidense, mas também o desenvolvimento de reflexões mais críticas sobre o funcionamento, o impacto e as consequências desse novo paradigma[70].

---

[67] EASTERBROOK, Frank H. Cyberspace versus Property Law. **Texas Review of Law and Politics**, v. 4, p. 103-113, 1999. p. 109-110.

[68] No mesmo sentido: GIBBONS, Llewellyn Joseph. No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. **Cornell Journal of Law and Public Policy**, v. 6, n. 3, p. 475-551, 1997. p. 544.

[69] EASTERBROOK, op. cit., 1996, p. 216.

[70] Resumindo a ideia por trás desta releitura quanto à regulação de tecnologias, David Post assevera que "*The other view reports that the imminent death of the state is greatly exaggerated* (POST, David G, op. cit., 1998, p. 522). Original em inglês. Tradução livre: "A outra posição relata que a morte iminente do Estado foi demasiadamente exagerada".

Mesmo que na segunda metade da década de 90 a internet, provavelmente a mais importante das novas tecnologias de informação e comunicação, ainda não possuísse a quantidade de usuários que na atualidade, sua utilização por um número significativo de pessoas já começava a trazer novos desafios e problemas desconhecidos pela até então pequena comunidade de pioneiros e cientistas. Com efeito, ainda que a retórica em prol de soluções "privadas" permanecesse presente inclusive em manifestações de autoridades governamentais estadunidenses[71], o crescente número de conflitos em diversos setores econômicos demonstrava que continuar a tratar o ciberespaço como um *commons*[72] – dominado pelo princípio *first-come, first-served*[73] – já não era uma alternativa viável[74]. Assim, no segundo estágio do debate doutrinário, diversos autores passaram a propugnar um retorno de uma concepção realista frente ao tratamento regulatório das novas tecnologias. De acordo com eles, apesar da atuação e coordenação de atores privados ser possível e desejável num momento inicial, esse espírito cooperativo se tornaria inviável com o massivo ganho de escala e efeitos de rede trazidos pela utilização da internet por mais pessoas. Desta maneira, o sucesso preliminar dos esforços coletivos desses agentes correria o risco de ser perdido sem a interação com entes estatais, os quais seriam capazes de criar válvulas de escape e mediar conflitos nas situações em que mecanismos de auto-governança não tivessem habilidades de fazê-lo[75].

Nesse sentido, buscando aprofundar o estudo e as reflexões sobre a primeira geração de autores, Neil Weinstock Netanel reuniu os argumentos favoráveis à autonomia do ciberespaço

---

[71] De fato, durante o mandato do presidente Bill Clinton, entre os anos de 1993 a 2001, o governo estadunidense passou a adotar progressivamente a divulgar uma agenda pública em favor da "privatização" de diversos setores relacionados à internet (UNITED STATES OF AMERICA. **Memorandum for the Heads of Executive Departments and Agencies:** Electronic Commerce. Washington: Office of the Press Secretary, 1997. Não paginado. UNITED STATES OF AMERICA. **Memorandum for the Heads of Executive Departments and Agencies:** Successes and Further Work on Electronic Commerce. Washington: Office of the Press Secretary, 1998. Não paginado).

[72] Em síntese, um "commons" pode ser considerado como sendo um recurso não regulado de uso compartilhado entre os usuários. Em um dos principais ensaios sobre o tema, Garret Hardin denominou de *Tragedy of the Commons* o fenômeno da inevitável destruição de um recurso compartilhado em virtude de seus usuários, num modelo clássico de racionalidade, perceberem proporcionalmente menos o prejuízo causado pela utilização nociva do recurso compartilhado do que o respectivo benefício (HARDIN, Garret. The Tragedy of the Commons. **Science**, v. 162, n. 3859, p. 1243-1248, dec. 1968. p. 1244).

[73] Em síntese, o princípio do "*first-come, first served"* corresponde a um regime que privilegia a posição jurídica do agente que reivindicar primeiro sua relação jurídica (geralmente a propriedade, mas também a posse) sobre a coisa, sem a necessidade de análises profundas quanto ao mérito da reivindicação. Para uma definição mais específica quanto ao tema no âmbito do registro de nomes de domínio, vide a RFC 8126 (COTTON, Michelle. *et alli*. **Request for Comments 8126:** Guidelines for Writing an IANA Considerations Section in RFC. Los Angeles: Internet Engineering Task Force, 2017. p. 19-20).

[74] RADIN, Margaret Jane; WAGNER, R. Polk. The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace. **Chicago-Kent Law Review**, v. 73, p. 1295-1317, 1998. p. 1301.

[75] Idem, p. 1317.

em três rótulos[76]: a) os "ciberpopulistas", cujos argumentos estavam centrados no fato de que as novas tecnologias permitiriam o desenvolvimento de uma democracia direta, sem a necessidade da intermediação por representantes; b) os "cibersindicalistas", que defendiam a tese de que a interação entre os grupos nestes novos meios de comunicação permitiria a criação de ambientes nos quais o consenso entre os participantes seria suficiente para a organização social, sem a necessidade de mecanismos externos; c) os "ciberanarquistas", que sustentavam que a ampla liberdade de saída e escolha entre diversas opções de sistemas permitiria a criação de um verdadeiro "livre mercado" entre as alternativas existentes.

Embora também partilhasse de um ideal democrático e libertário, acreditando que as novas tecnologias possuíam uma incrível capacidade para modificar a realidade existente, Netanel adotava uma postura crítica com relação às teses dos grupos que identificou. Para ele, havia grandes problemas por trás do que defendiam os argumentos e ideais ciberpopulistas, cibersindicalistas e ciberanarquistas. Em primeiro lugar, apontou que apesar de serem razoáveis muitas das críticas feitas à democracia representativa, os estudiosos do primeiro estágio doutrinário se equivocavam ao defender que essa seria simplesmente uma segunda opção diante de uma democracia direta[77]. Em segundo, o autor também se demonstrou reticente frente à crença de que as novas tecnologias de informação e comunicação seriam capazes de possibilitar a existência de modelos de auto-governança, sem a necessidade de mecanismos de intermediação ou governos. Em terceiro, referiu que a "liberdade de escolha" entre diversos sistemas existentes no mercado criado pelas novas tecnologias também estaria sujeita às mesmas espécies de restrições e defeitos trazidos por assimetrias informacionais e de poder verificadas no mercado. Por último, aduziu que ainda que as novas tecnologias fossem efetivamente instrumentos capazes de permitir maior liberdade de ação aos indivíduos, elas não estariam disponíveis a todas as pessoas, o que faria com que uma nova democracia baseada nestes instrumentos tecnológicos fosse um privilégio de poucos.

No primeiro estágio doutrinário, em virtude da postura refratária à intervenção dos entes estatais, existia um certo consenso entre os estudiosos desse período de que caberia aos atores privados envolvidos nesse meio estabelecer mecanismos de cooperação aptos a desenvolver soluções para os problemas enfrentados no setor. Devido a essas características, muitos identificavam uma certa semelhança entre o fenômeno da regulação de tecnologias por atores

---

[76] NETANEL, Neil Weinstock. Cyberspace Self-Governance: a Skeptical View from a Liberal Democracy Theory. **California Law Review**, v. 88, n. 2, p. 395-498, 2000. p. 404.
[77] Idem, p. 405.

privados e o advento das normas de direito dos comerciantes – a *lex mercatoria* – cuja criação se deu justamente num cenário histórico de ausência de um poder central capaz de estabelecer um regramento uniforme e cogente[78].

Examinando esta questão, Joel Reidenberg concordava com a existência de semelhanças entre o cenário da *lex mercatoria* e o novo paradigma experimentado em decorrência da evolução das tecnologias de informação e comunicação[79]. Igualmente, reconhecia que a crescente permeabilidade das fronteiras nacionais ocasionada pela expansão da infraestrutura global de informações afetava a soberania do Estado no que diz respeito à sua capacidade de formular e aplicar a regulação estatal[80]. Porém, indo mais além, asseverou que não apenas as fronteiras legais territoriais haviam se tornado mais ambíguas, mas os próprios limites substantivos entre disciplinas jurídicas se tornaram mais confusos. Conforme observou, matérias que anteriormente possuíam arcabouços normativos distintos, tais como telecomunicação e serviços financeiros, privacidade e propriedade intelectual, entre outros, passaram a sofrer um processo de conexão e sobreposição, gerando um aumento significativo de incerteza e insegurança jurídica[81]. Além disso, tomando um passo que representou um amadurecimento frente ao primeiro estágio da doutrina, Reidenberg reconheceu que o papel desempenhado pelas escolhas relacionadas à arquitetura de sistemas e capacidades tecnológicas merecia uma análise e tratamentos distintos, a qual denominou de *lex informatica*[82].

Inicialmente, o autor identificou que naquele estágio de evolução do ecossistema de redes de informação existiria três matérias que demandariam atenção crítica por parte daqueles responsáveis pela formulação de políticas, a saber: a) o tratamento de conteúdo; b) o tratamento de informações pessoais; c) a preservação de direitos de propriedade. Todavia, ao invés de buscar propor soluções estritamente jurídicas para a solução de problemas envolvendo as matérias referidas, demonstrou a existência de diversas medidas tomadas no campo do desenvolvimento de tecnologias e arquitetura de sistemas voltadas a resolver tais questões[83]. Assim, chamou atenção para o fato de que os desenvolvedores e engenheiros de computação,

---

[78] Por exemplo: JOHNSON, David R.; POST, David. Law and Borders: The Rise of Law in Cyberspace. **Stanford Law Review**, v. 48, p. 1367-1402, 1996. p. 1389. VALAUSKAS, Edward J. Lex Networkia: Understanding the Internet Community. **First Monday**, v. 1, n. 4, não paginado, oct. 1996.
[79] REIDENBERG, Joel R. Lex Informatica: The Formulation of Information Policy Rules through Technology. **Texas Law Review**, v. 76, n. 3, p. 553-593, fev. 1998. p. 554.
[80] REIDENBERG, Joel R. Governing Networks and Rule-Making in Cyberspace. **Emory Law Journal**, v. 45, p. 911-930, 1996. p. 913-915.
[81] Idem, p. 916.
[82] REIDENBERG, op. cit., 1998, p. 555.
[83] Idem, p. 557-568.

ao decidirem por implementar determinadas estratégias ou mecanismos na arquitetura de seus sistemas, acabavam por adquirir e compartilhar características importantes com outros atores políticos[84].

Entretanto, Reidenberg também pontuou que as decisões políticas tomadas por desenvolvedores de sistemas funcionariam de forma distinta daquelas tomadas por reguladores "clássicos", principalmente no que diz respeito ao fluxo de informações. Nesse sentido, no momento de definição da configuração, a arquitetura de um sistema poderia ter seu estado padrão definido de modo a estabelecer políticas que poderiam ser tanto imutáveis quanto flexíveis sob a perspectiva do usuário[85]. Igualmente, sistemas também poderiam ser estruturados de maneira a restringir ou completamente excluir determinadas condutas do campo de ação dos usuários ou mesmo permitir que estes personalizem determinadas configurações conforme as suas necessidades ou vontades[86]. De uma forma ou de outra, não haveria uma margem real de interpretação por parte dos usuários: sua amplitude de ação estaria adstrita aos parâmetros definidos pelos desenvolvedores dos sistemas[87].

Além desses aspectos, o autor fez outra importante constatação no que tange à efetividade das políticas definidas por intermédio da *lex informatica*: diferentemente das normas jurídicas, cuja efetividade depende primordialmente de mecanismos *ex post* por intermédio do Poder Judiciário, regras imbuídas na arquitetura de sistemas, quer em nível local ou em nível de rede, poderiam ser desenhadas para possuir efetividade automática, autônoma e *ex ante*[88]. Por certo, ainda que falhas nos códigos ou defeitos na arquitetura não permitiriam concluir pela perfeição da *lex informatica*, essa circunstância alteraria de forma substancial o relacionamento dos agentes regulados para com as normas às quais estão sujeitos.

Diante de todas essas observações, Reidenberg adotou uma postura distinta dos autores do primeiro estágio doutrinário, porquanto considerava que a regulação estatal poderia desempenhar um papel importante na elaboração e desenvolvimento da *lex informatica*[89]. Com efeito, o autor considerava que o Estado poderia contribuir neste cenário mediante o estabelecimento de sanções, positivas ou negativas, destinadas tanto a usuários quanto a desenvolvedores, para fortalecer políticas públicas cuja implementação não fosse eficiente ou

---

[84] Idem, p. 556.
[85] Idem, p. 568.
[86] Idem, p. 569-571.
[87] Idem, p. 571-572.
[88] Idem, p. 572.
[89] Idem, p. 583.

eficaz quando da utilização de medidas regulatórias clássicas. Para tanto, julgava necessário e crucial que os entes estatais se engajassem e buscassem influir no processo de estabelecimento de padrões técnicos através de mecanismos de regulação indireta. Assim, por exemplo, mencionou que haveria seis abordagens que poderiam ser utilizadas pelo Estado para esta finalidade[90]: 1) ameaçar intervir em caso de inércia dos agentes privados em adotar algum padrão técnico; 2) participar diretamente em entidades de padronização técnica; 3) financiar projetos voltados ao desenvolvimento de padrões técnicos; 4) direcionar a política de compras e contratações públicas para favorecer determinado padrão técnico; 5) regular e sancionar negativamente comportamentos contrários ao padrão técnico desejado; 6) determinar o formato de padrões técnicos específicos.

Para ele, o avanço inevitável da *lex informatica* representou uma importante mudança institucional no que se refere ao relacionamento do Estado para com os atores envolvidos no desenvolvimento de tecnologias de informação e comunicação. Dado à sua importância, entidades e mecanismos responsáveis pelo estabelecimento de padrões técnicos se tornaram efetivos centros políticos[91]. Desta forma, ainda que de forma involuntária, essa mudança trouxe à comunidade técnica, além de uma maior influência, uma inegável responsabilidade política[92]. Igualmente, ainda que culturas organizacionais distintas [93] tragam dificuldades e sejam recebidas com resistência[94], reguladores estatais passariam a se ver obrigados a interagir mais com esta comunidade e seus fóruns não tradicionais para conseguir fazer avançar seus objetivos.

No que diz respeito ao estudo sobre a capacidade regulatória de tecnologias de informação e comunicação, Lawrence Lessig seguramente pode ser considerado um dos mais influentes e conhecidos especialistas jurídicos sobre o tema[95]. Até 2018, publicou cinco livros e mais de cinquenta e cinco artigos sobre o assunto[96]. Além disso, foi o perito judicial em dois importantes casos judiciais estadunidenses envolvendo a temática: *United Stated v. Microsoft* e *A&M Records v. Napster*. De fato, os esforços do professor da Faculdade de Direito de

---

[90] Idem, p. 588.
[91] Idem, p. 591.
[92] Idem, p. 592.
[93] Para um ilustrativo relato a respeito do funcionamento e organização da *Internet Engineering Task Force*, órgão responsável pelo estabelecimento dos protocolos técnicos da internet, vide: BORSDOK, Paulina. How Anarchy Works. **Wired**, 01 oct. 1995. Não paginado.
[94]
[95] De fato, o autor figura entre os 10 professores de direito mais citados nos EUA no período entre 2010 e 2014 (ADLER, Jonathan H. Most-cited law faculty, 2010-2014. **The Washington Post**, 19 may. 2016. Não paginado). Mesmo no Brasil, uma simples busca pelo termo "Lessig" em 10/06/2018 na base de periódicos da Revista dos Tribunais (https://revistadostribunais.com.br) já revela 29 resultados.
[96] De acordo com a edição mais recente de seu currículo (Disponível em: <http://lessig.org/wp-content/uploads/2015/150807_CV_updated.pdf>. Acesso em: 10 maio. 2018).

Harvard para tornar mais claro aos juristas os efeitos regulatórios do "código" sobre os indivíduos são percebidos até mesmo no Poder Legislativo brasileiro[97].

Por certo, pode-se dizer que sua principal obra foi o livro *Code and Other Laws of Cyberspace* (doravante *Code*), cuja primeira edição foi publicada em 1999 e a segunda em 2006, na qual avaliou questões relacionadas a "regulabilidade" de tecnologias de informação e comunicação, a regulação feita por intermédio dessas tecnologias, ambiguidades e problemas a elas relacionadas. No livro, o autor buscou explicar ao público, principalmente a juristas, o relacionamento entre códigos de computador e códigos legais enfatizando a necessidade de melhor compreender o funcionamento dos primeiros, pois *Code is Law*[98], ou, numa tradução livre, "*Código é Direito"*[99].

Entretanto, considera-se equivocado iniciar o estudo da matéria diretamente pelas reflexões feitas em *Code*. Deveras, antes de escrever esse livro, o autor gradativamente construiu e amadureceu suas ponderações quanto à temática da regulação de tecnologias. Assim, antes de descrever as principais ideias contidas em *Code*, o próximo subcapítulo buscará apresentar, de forma cronológica, os estudos feitos por Lessig. Desta maneira, tornar-se-á mais fácil compreender suas ideias, quer para aceitá-las, quer para criticá-las.

2.2.1 Lawrence Lessig, a "Nova Escola de Chicago" e a Regulação pela Arquitetura de Tecnologias de Informação e Comunicação

Durante a 2ª Guerra Mundial, a cidade de Londres sofreu inúmeros bombardeios por parte da *Luftwaffe* que causaram consideráveis danos em prédios históricos e importantes. Dentre os edifícios danificados, o Parlamento Britânico e, em especial, a Câmara dos Comuns foi particularmente afetada em razão de bombas incendiárias, sendo necessária a sua reconstrução.

---

[97] No âmbito do Projeto de Lei nº 8.503/2017, de autoria do Deputado Federal Edmilson Rodrigues, o autor é expressamente referido na justificação da proposta legislativa (BRASIL. Câmara dos Deputados. **Projeto de Lei nº 8.503, de 2017**. Altera a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), para tornar expresso o direito de obter informações relativas à aquisição e funcionamento de softwares, hardwares e códigos mediadores de funções públicas e tornar obrigatória a disponibilização dos códigos-fonte dos algoritmos utilizados para a distribuição de processos nos órgãos do Poder Judiciário. Brasília: Câmara dos Deputados, 2017. p. 2).

[98] LESSIG, Lawrence. **Code 2.0.** New York: Basic Books, 2006. p. 5.

[99] Importante deixar claro que a ideia de que códigos de computador possuem capacidade de regular condutas de forma semelhante ao direito não é criação original de Lessig. Como ele mesmo reconhece, Joel Reidenberg e William Mitchell (MITCHELL, William J. **City of Bits:** space, place, and the infobahn. Cambrigde: MIT Press, 1996. p. 111) foram os primeiros a escrever sobre a questão. Todavia, partindo destas primeiras reflexões, Lessig aprofundou muito mais o estudo da matéria.

Assim, naquela ocasião, surgiu entre os parlamentares a ideia de aproveitar a oportunidade para modificar a arquitetura do local, alterando a tradicional estrutura de dois conjuntos de bancos contrapostos para uma sistemática de anfiteatro, a exemplo de outras casas legislativas ocidentais. Entretanto, o então Primeiro Ministro Winston Churchill foi radicalmente contrário à proposta por considerar que o antigo desenho do lugar era responsável pelo sistema político que seria a essência da democracia parlamentar britânica. Assim, durante as deliberações sobre o assunto, ficou célebre a sua frase "*We shape our buildings and afterwards our buildings shape us"*[100].

De fato, a concepção de que a arquitetura ou *design* influencia ou regula a conduta humana é antiga, porém apenas mais recentemente passou a ser estudada com mais profundidade por juristas sob a perspectiva de tecnologias de informação e comunicação. Desse modo, a presente subseção buscará presentar a evolução dos estudos e pensamento de Lawrence Lessig, autor estadunidense que provavelmente possui o mais extenso e relevante conjunto de trabalhos sobre o tema.

Embora não tenha estado entre os primeiros estudiosos estadunidenses a examinar e escrever acerca da regulação de tecnologias de informação e comunicação e de sua arquitetura, a atenção de Lessig quanto ao tema iniciou cedo, já em 1995, concomitantemente à abertura comercial da internet pelo governo do Presidente Bill Clinton. Na ocasião, assim como outros estudiosos do primeiro estágio doutrinário, o autor formulou duas questões primordiais para a compreensão do recente paradigma tecnológico[101]: a) seria necessário utilizar a analogia para regular este novo espaço ou seria preciso abandoná-la e começar do zero? b) seria este espaço algo efetivamente novo?

Tomando como comparativo o processo de desenvolvimento regulatório da *common law*, este pesquisador, ao contrário de outros autores, não considerou a lentidão e casuísmo da regulação na área tecnológica algo intrinsecamente ruim, pois esta evolução gradual significava que pequenas mudanças iriam aos poucos consolidar um corpo experimental a partir do qual novos entendimentos poderiam ser produzidos. Desse modo, ao invés de achar que a lentidão regulatória estatal seria algo a militar contra a regulação das novas tecnologias, entendeu que este fator era necessário para uma regulação mais madura desse cenário[102]. Igualmente,

---

[100] CHURCHILL, Winston. House of Commons Rebuilding. **Commons Sitting,** 28 oct. 1943. Tradução livre: "Nós damos forma a nossos edifícios e depois nossos edifícios nos dão forma".
[101] LESSIG, Lawrence. The Path of Cyberlaw. **Yale Law Journal**, v. 104, p. 1743-1755, 1995. p. 1743.
[102] Idem, p. 1745.

considerou que o ponto relevante não era apenas o debate sobre o "equilíbrio" entre regulação mais ou menos permissiva, mas sim o *momento* em que este equilíbrio deva ser fixado[103].

Enquanto alguns autores do primeiro período[104] possuíam uma visão extremamente positiva (e talvez até ingênua) das benesses futuras a serem trazidas pelo avanço tecnológico, desde seus estudos iniciais sobre o tema Lessig já apontou para os possíveis problemas oriundos da "cegueira" e falta de diálogo entre dois grupos envolvidos neste processo: a comunidade técnica e os agentes reguladores estatais.

No que tange aos primeiros, lembrou que as mesmas tecnologias capazes de promover avanços para a humanidade também poderiam, se permitidas, destruir a própria essência daquilo que se define como individualidade[105]. Com efeito, embora asseverasse que a comunidade técnica não seria formada por delinquentes[106] [107], pontuou que nem sempre os valores e preocupações mantidos por este grupo seriam os mesmos do restante da sociedade. Em virtude disso, sistemas e programas de computador por eles projetados, embora possam ter grande potencial de impacto socioeconômico, frequentemente não têm a preocupação de proteger os indivíduos dos possíveis abusos oriundos da utilização destas mesmas tecnologias[108].

Quanto aos segundos, constatou que a atuação dos agentes reguladores estatais também representava um risco considerável diante do avanço de novas tecnologias de informação e comunicação. Deveras, os impactos trazidos pelo desenvolvimento de novas tecnologias trazem preocupações reais para o Estado, cuja atuação passa a ser demandada pela sociedade diante dos diversos interesses em conflito. Entretanto, no esforço de romper o vácuo normativo, a falta de compreensão adequada dos agentes públicos sobre o funcionamento desses novos mecanismos também pode trazer consequências negativas e afetar liberdades fundamentais[109].

---

[103] Idem, p. 1752.
[104] Exemplificativamente, pode-se citar, entre outros, os autores John Perry Barlow, David Post e David Johnson, cujas obras já foram apresentadas no capítulo 2.1 acima.
[105] Idem, p. 1748.
[106] Não obstante, existem inúmeras críticas a respeito da eticidade da conduta de grandes empresas de tecnologia e seus fundadores (SALMON, Felix. Musk, Zuckerberg, Bezos, and Ethically Iffy 'Philanthropy". **Wired**, 15 may. 2018. Não paginado).
[107] Por outro lado, a postura crítica para com as instituições sociais frequentemente motiva posturas de ativismo político (ou "hacktivismo") por parte desses grupos (GONÇALVES, Eduardo Vicente. **Hacktivism and its Struggle in Changing the World:** The Aaron Swartz Case, Access to Knowledge and Economic Model. 2017. Dissertation (MA in Sociology Research). Department of Sociology, University of Essex, Essex, 2017. p. 1)
[108] LESSIG, Lawrence. The Path of Cyberlaw. **Yale Law Journal**, v. 104, p. 1743-1755, 1995. p. 1749.
[109] Idem, p. 1751-1754. Verdadeiramente, críticas acerca do "analfabetismo tecnológico" de agentes estatais persiste até os dias de hoje. Vide: DREYFUSS, Emily. Tech Illiteracy is a Huge Threat to Our Government. **Wired**, 11 may. 2017. Não paginado.

Por certo, isso não significava uma defesa em prol da ausência de regulação: desde seu primeiro artigo sobre o assunto Lessig já chamou atenção para a falácia que era afirmar que as novas tecnologias de informação e comunicação não eram reguladas ou reguláveis[110]. Porém, naquele momento introdutório e de "descobrimento", entendeu que a regulação estatal deveria permitir, o tanto quanto possível, que a própria sociedade civil experimentasse e compreendesse os efeitos destas novas tecnologias sob o seu cotidiano[111].

Outro ponto estudado por este autor foi a concepção de que o "ciberespaço", isto é, o conjunto de redes de computadores responsável pela formação da internet, seria por si só um "lugar" autônomo. No primeiro estágio doutrinário, autores como David Post e David Johnson defendiam que o ciberespaço, as tecnologias e os sistemas nele envolvidos seriam um lugar autônomo e soberano e que, portanto, deveria não apenas ter regras especiais para si, mas também regras concebidas por sua própria comunidade de usuários[112]. Da mesma forma, entendiam que normas advindas de entes estatais seriam ilegítimas, pois estes não possuiriam soberania neste novo "território" e seriam "externos" à rede e seus usuários[113].

Todavia, Lessig desde o começo discordou desse posicionamento: não só os usuários desse novo espaço estão localizados *dentro* do território de Estados, como também os efeitos de suas ações são sentidos por pessoas que não utilizam estas novas tecnologias[114]. Estas razões, por si só, já justificariam a atuação regulatória. Ademais, para o autor tampouco era relevante se a regulação não seria tão eficaz em virtude das novas características desse novo espaço: uma norma jurídica não precisa ser absolutamente eficaz para que tenha a sua criação justificada, bastando que produza um resultado considerado adequado para os fins para os quais foi formulada, pois, do contrário, sequer existiria regulação estatal no "espaço real" [115]. Em síntese:

---

[110] LESSIG, Lawrence. The Path of Cyberlaw. **Yale Law Journal**, v. 104, p. 1743-1755, 1995. p. 1754.
[111] Idem, p. 1755.
[112] JOHNSON, David R.; POST, David. Law and Borders: The Rise of Law in Cyberspace. **Stanford Law Review**, v. 48, p. 1367-1402, 1996. p. 1387-1391. Igualmente, interessante consultar a perspectiva sociológica de Julian Dibbel acerca do processo de formação de normas sociais em comunidades digitais (DIBBEL, Julian. A Rape in Cyberspace: How na Evil Clown, a Haitian Trickster Spirit, Two Wizards and a Cast of Dozens Turned a Database Into a Society. **The Village Voice**, 23 dez. 1993. Não paginado).
[113] JOHNSON, David R.; POST, David. Law and Borders: The Rise of Law in Cyberspace. **Stanford Law Review**, v. 48, p. 1367-1402, 1996. p. 1380.
[114] LESSIG, Lawrence. The Zones of Cyberspace. **Stanford Law Review**, v. 48, p. 1403-1411, 1996. p. 1404-1405.
[115] Idem, p. 1405. Aliás, a concepção de que num regime sem custos de transação as negociações entre as partes acarretariam em acordos que maximizariam a riqueza independentemente do marco jurídico inicial é um dos conceitos-chave por trás do "Teorema de Coase" (COASE, Ronald H. **Prize Lecture**: The Institutional Structure of Production. Stockholm: Nobel Foundation, 1991. Não paginado).

postulou que a regulação seria possível, porém por meios distintos[116] (e frequentemente não estudados por juristas).

Nesta senda, ao criticar o posicionamento de Post e Johnson, Lessig começou a efetivamente descrever as primeiras linhas de como efetivamente considerava que as novas tecnologias de informação e comunicação seriam reguladas: não só pelo uso direto de normas jurídicas, mas também pela interação *indireta* com normas sociais e normas de mercado[117]. Além disso, também chamou a atenção para o fato de que não apenas as novas tecnologias passariam a ser sujeitas à regulação, como também *elas mesmas* passariam a servir como mecanismo regulatório[118] [119].

Para ele, o elemento crucial para compreender esta função regulatória das tecnologias de informação e comunicação seria o seu *design* e os valores ou objetivos escolhidos pelo seu desenvolvedor quando de sua concepção[120]. Outro elemento essencial para esta compreensão é a forma como esta modalidade de regulação interage com aqueles que estão sujeitos às suas normas: num sistema bem implementado, o usuário não possui efetivamente a "opção" de obediência, ficando sua margem de ação absolutamente adstrita às escolhas de seus desenvolvedores. Deste modo, se a escolha do *design* por estes agentes seria tão relevante, tornava-se necessário começar a avaliar as decisões por eles tomadas levando em conta suas consequências frente aos interesses da coletividade[121].

Paulatinamente, passou a dedicar maior atenção ao *design* de tecnologias de informação e comunicação e a sua capacidade de conformar o comportamento dos agentes a ele sujeitos[122]. Nesse sentido, traçando um paralelo com a capacidade que a natureza possui de limitar as ações dos indivíduos, descreveu que, assim como ambientes físicos, códigos de sistemas não

---

[116] LESSIG, Lawrence. The Zones of Cyberspace. **Stanford Law Review**, v. 48, p. 1403-1411, 1996. p. 1406.
[117] Idem, p. 1407-1410.
[118] Idem, p. 1408.
[119] Conforme será explicitado mais adiante, tecnologias de informação e comunicação estruturadas como plataformas não apenas passam a ser mecanismos regulatórios a serem utilizados pelo Estado como também pelos próprios agentes privados responsáveis por seu desenvolvimento e manutenção. Para um exame dos impactos deste fenômeno no âmbito dos direitos fundamentais, vide, por exemplo: LYNSKEY, Orla. Regulation by Platforms: the Impact on Fundamental Rights. In. BELLI, Luca; ZINGALES, Nicolo (ed.). **Platform Regulations:** How Platforms are Regulated and How they Regulate Us. Rio de Janeiro: Fundação Getúlio Vargas, 2017.
[120] Idem, p. 1408.
[121] Idem, p. 1410-1411.
[122] Embora o foco dos estudos de Lessig diga respeito aos efeitos regulatórios da arquitetura de tecnologias de informação e comunicação, o estudo sobre a "capacidade regulatória" da arquitetura em si pode ser encontrado anteriormente em autores como William Mitchel, Michel Foucault (FOUCAULT, Michel. **Discipline & Punish:** The Birth of the Prison. New York: Vintage Books, 1995. p. 195-209) e Jeremy Bentham (BENTHAM, Jeremy. **The Works of Jeremy Bentham:** Published Under the Superintendence of his Executor John Bowring. Edinburgh: William Tait, 1838. 11v. em 4. p. 39).

conferem liberdade de escolha além daquilo que já está estabelecido[123]: uma pessoa não consegue ver através de um muro de concreto, nem um usuário consegue utilizar um programa de computador sem informar sua senha caso este requisito esteja implementado. Além disso, ao contrário das normas jurídicas ou sociais, as quais apenas conseguem regular a conduta de forma *mediata* por meio da ameaça de sanção posterior, tanto a natureza quanto o código são capazes de afetar os indivíduos de modo imediato e anterior à própria realização da conduta[124].

Ao contrário da natureza, porém, o código por trás de tecnologias de informação e comunicação seria extremamente *plástico* e *modificável*, sendo sua arquitetura, superados certos limites técnicos[125], dependente apenas das escolhas de seus desenvolvedores. Isto, somado ao fato de que os mecanismos clássicos de regulação estatais se tornariam cada vez mais ineficientes num mundo globalizado e digital, fez o pesquisador levantar a hipótese de que o Estado passaria a utilizar cada vez mais códigos de computador como substitutos às normas jurídicas, as quais passariam a ter como objeto não a regulação imediata da conduta de indivíduos, mas a própria arquitetura de como sistemas eletrônicos são construídos[126].

Entretanto, ao contrário das normas jurídicas, as quais podem geralmente ser diretamente conhecidas e acessadas pelos indivíduos a elas sujeitos, normas escritas em código de sistemas de computador são uma modalidade de regulação indireta com a qual a sociedade e suas instituições de forma geral não estão acostumadas a interagir[127]. Desta forma, por considerar que o Estado passaria a utilizar cada vez mais modalidades indiretas de regulação em substituição à regulação direta clássica, apresentou uma proposta de teoria para o estudo deste fenômeno, a qual denominou de "Nova Escola de Chicago"[128].

De acordo com o autor, esta teoria compartilhava algumas das premissas com a "velha" Escola de Chicago: ambas utilizariam uma abordagem a respeito do fenômeno regulatório que foca em mecanismos de regulação distintos do Direito. Igualmente, as duas identificariam

---

[123] LESSIG, Lawrence. The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulations. **Common Law Conspectus**, v. 5, p. 181-191, 1997. p. 181.
[124] Idem, p. 184.
[125] BOOCH, Grady. The Limits of Technology. **IBM Developer Works**, 13 jan. 2003. p. 1
[126] LESSIG, op. cit., 1997, p. 184-185.
[127] Idem, p. 191.
[128] LESSIG, Lawrence. The New Chicago School. **The Journal of Legal Studies**, v. 27, n. 2, p. 661-691, 1998. p. 661. Esta teoria também é frequentemente chamada de "The Pathetic Dot Theory", numa tradução livre do Inglês, "Teoria do Ponto Patético" (BODÓ, Balázs; GIANNOPOLOU, Alexandra. The Logics of Technology Decentralization: the case of distributed ledger technologies. **Amsterdam Law School Legal Studies Research Papers**, n. 5, 2019. p. 5. DEXE, Jacob. **Constraining the Digital World**: Structuring net neutrality regulation through the lens of Lessig's New Chicago School model. Lund: Lund University, Department of Political Science, 2015. p. 5).

situações em que estes outros mecanismos de regulação podem ser mais eficientes em regular que o Direito. No entanto, possuiriam uma distinção fundamental: ao passo que a "Velha Escola", verificando esta ineficiência, concluiria que o Direito deveria ceder espaço para estas outras modalidades de regulação, a "Nova Escola" identificaria nelas um novo conjunto de ferramentas para atingir os fins regulatórios[129].

Em primeiro lugar, embora não desconhecesse a existência de outras modalidades de regulação, Lessig listou quatro tipos de restrição ao comportamento[130]: a) o *direito*, o qual estabelece ameaças de sanções *ex post* a serem executadas pelo Estado em caso de descumprimento; b) o *costume* ou *normas sociais*, os quais também estabelecem ameaças de sanções *ex post*, porém vigiadas por uma determinada comunidade ou grupo no qual o indivíduo está inserido; c) o *mercado*, o qual conforma a conduta de indivíduos por intermédio do preço; d) a *arquitetura*, cujos limites ou características do espaço ou local no qual o indivíduo está inserido determinam sua amplitude de ações. Para melhor descrever a interação das modalidades regulatórias frente ao objeto regulado, o autor se vale da figura abaixo[131]:

Figura 1- Interação das modalidades regulatórias sobre o objeto regulado

Fonte: Lessig, op. cit., 2006, p. 123.

Em segundo lugar, o autor asseverou que essas quatro forças não atuariam sozinhas, mas sempre de forma simultânea, ainda que com intensidades distintas. Assim, será sempre o resultado da soma destes fatores que efetivamente descreveria a regulação a qual estaria

[129] Idem, p. 661.
[130] Idem, p. 662-663.
[131] Numa tradução livre da Língua Inglesa: "Market" traduz-se por "Mercado"; "Law" traduz-se por "Direito"; "Architecture" traduz-se por "Arquitetura"; e "Normas" por "Costume" ou "Normas Sociais".

submetida determinada conduta de um indivíduo[132]. Além disso, também salientou que essas quatro forças não são autônomas entre si, mas estão constantemente interagindo, seja reforçando[133], seja enfraquecendo os efeitos das outras[134].

Tendo em vista esta interação entre cada modalidade de regulação, Lessig apontou para a importante necessidade dos operadores do direito compreenderem o funcionamento de cada uma. Deste modo, reconheceu que estas modalidades poderiam ser utilizadas pelo direito para ampliar sua capacidade regulatória, de modo a regular comportamentos não apenas de maneira *direta*, mas também de maneira *indireta* ao influenciar estes mecanismos com a adoção de determinada norma jurídica[135].

Por outro lado, este foco em modalidades indiretas de regulação também acarretaria a necessidade de se examinar aspectos relativos à *subjetividade* ou *objetividade* das medidas impostas às condutas dos indivíduos quando da adoção destes mecanismos. O autor compreendeu que isto seria relevante em razão da internalização de determinadas medidas ser um fator crucial para o seu funcionamento: políticas *objetivas* não requerem a adesão dos indivíduos para produzir resultados, ao passo que aquelas *subjetivas* não podem prescindir de algum nível adesão para que sejam efetivas[136]. Todavia, de forma geral não existiriam medidas de regulação indireta que sejam sempre objetivas ou subjetivas já que este aspecto seria extremamente dependente do contexto onde são aplicadas. Assim sendo, a internalização de políticas regulatórias não seria algo que poderia ser presumido, mas, sim, algo que requereria para a sua compreensão a análise de três fatores[137]: a) a extensão na qual uma medida objetiva *é* subjetivamente efetiva; b) a extensão na qual uma medida objetiva *pode ser* subjetivamente efetiva; c) a extensão na qual uma medida que não é objetiva *é* ou *pode ser* subjetivamente efetiva.

Contudo, esta "meta-função" do Direito de influenciar outros mecanismos regulatórios não deveria apenas ser vista sob a ótica de uma capacidade ou poder ampliado. Com efeito, se o direito efetivamente possui a capacidade de atingir outras modalidades de regulação, isto significaria que cada modificação no conjunto de normas jurídicas possuiria o condão de gerar

---

[132] Idem, p. 663.
[133] Em razão deste aspecto (e talvez de forma excessivamente otimista), Kenneth Dam postulou já em 1999 a redução a barreiras legais que impedissem o desenvolvimento e uso de tecnologias e sistemas eletrônicos voltados à execução automática de direitos (DAM, Kenneth W. Self-Help in the Digital Jungle. **Journal of Legal Studies**, v. 28, n. 2, p. 393-412, jun. 1999. p. 412).
[134] LESSIG, op. cit., 1998. p. 666.
[135] Idem, p. 666.
[136] Idem, p. 677-678.
[137] Idem, p. 679.

ao mesmo tempo efeitos positivos e negativos[138]. Portanto, ao estabelecer uma determinada política pública, o agente regulador deve sempre considerar seus efeitos sistêmicos, de modo a identificar se a medida implementada aumenta ou reduz os custos sociais da conduta que buscou influenciar e de outras situações que com ela se relacionam[139].

Além destas questões, existiria outro aspecto particularmente relevante ressaltado pela "Nova Escola de Chicago" no que tange aos problemas da regulação indireta enquanto meio de intervenção estatal. De fato, sendo a regulação direta mais conhecida, sua estrutura e processo de desenvolvimento já foram adequadamente estudados pelos juristas, os quais construíram durante os anos diversos mecanismos de controle diante de atuações do Estado que sejam eventualmente consideradas injustas, ilegais ou ilegítimas.

No que se refere aos mecanismos de regulação indireta, estes ainda seriam pouco compreendidos ou mesmo pouco percebidos pela sociedade de forma em geral. Nesse sentido, por ser uma modalidade de atuação regulatória menos sujeita a riscos políticos em razão de sua menor exposição e conhecimento pelo público[140], a regulação indireta poderia ser utilizada de forma arbitrária sem os obstáculos dos institutos de controle construídos durante séculos pelas sociedades. Assim, entendeu ser necessário compreender melhor estes mecanismos de maneira a permitir a construção de estruturas de resistência contra abusos dessas modalidades de exercício de poder[141].

Gradativamente, a preocupação para com a capacidade regulatória da arquitetura de tecnologias de informação e comunicação e o relacionamento destas com os entes públicos e privados se tornou o foco primordial do autor. Nesse sentido, em 1999 Lessig publicou a obra *Code*[142], a qual pode ser descrita como sendo um dos principais e mais influentes estudos[143] a respeito da regulação de tecnologias. Neste título, buscou, além de aprofundar alguns assuntos já examinados em artigos anteriores, abordar questões que ainda não havia estudado. Assim, dividiu o texto em cinco grandes etapas, a saber: a) análise da regulabilidade de sistemas eletrônicos; b) exame da regulação feita por intermédio desses sistemas; c) observação dos impactos desses sistemas eletrônicos em determinadas espécies de direitos; d) avaliação dos

---

[138] Idem, p. 669-670.
[139] Nesse sentido, vide Ronald Coase (COASE, Ronald H. The Problem of Social Cost. **Journal of Law and Economics**, v. 3, p. 1-44, 1960. p. 44).
[140] LESSIG, Lawrence. The New Chicago School. **The Journal of Legal Studies**, v. 27, n. 2, p. 661-691, 1998. p. 690.
[141] Idem, p. 691.
[142] LESSIG, Lawrence. **Code 2.0.** New York: Basic Books, 2006.
[143] MCCULLAGH, Declan. What Larry Didn't Get. **Cato Unbound**, 4 may. 2009. Não paginado.

efeitos dos sistemas eletrônicos perante a soberania estatal; e) propositura de possíveis respostas frente aos fenômenos acarretados pela ampliação e disseminação da regulação feita por sistemas eletrônicos[144].

No que tange ao tópico da regulabilidade, Lessig tentou convencer o leitor a tratar com ceticismo qualquer tipo de retórica que, baseada em substantivos como "natureza" ou "essência", postule uma suposta impossibilidade das normas jurídicas de influenciar mudanças em tecnologias eletrônicas[145]. Para ele, o fato deste tipo de argumento ser frequentemente utilizado se deve ao desconhecimento geral sobre como funciona seu processo de desenvolvimento. Como não somos treinados para pensar nas diferentes maneiras com as quais sistemas eletrônicos podem atingir o mesmo fim mediante meios distintos, acabamos deixando de compreender o quão "plástico" é este processo[146]. Evidentemente, esta plasticidade não é sem limites, nem sempre sendo possível incluir numa determinada tecnologia algum objetivo ou requisito que desejamos[147]. Porém, nestes casos, o autor defendeu que a seus próprios desenvolvedores incumba o ônus de demonstrar esta impossibilidade técnica[148].

Desta maneira, procurou enfatizar a importância do *design* como momento determinante para a definição da capacidade ou possibilidade de se regular uma aplicação tecnológica. Realmente, sendo nesta fase em que serão definidos os requisitos do sistema, será nela onde os valores, objetivos ou finalidades poderão ser "inseridos" no processo de concepção. Assim, será nesta ocasião na qual será possível estipular qual será o grau de restrição ao qual os usuários deste sistema estarão submetidos, bem como qual será intensidade com a qual o poder do ente estatal poderá se manifestar.

Portanto, assim como havia sido reconhecido por Joel Reidenberg, Lessig entendeu que os desenvolvedores destes sistemas de informação passariam a ter um novo rol de responsabilidades para além daqueles relacionados à "mera" produção de tecnologias,

---

[144] Embora não seja estadunidense, interessante mencionar Roger Brownsword, o qual, estudando o tema posteriormente, denominou a regulação feita por meio de mecanismos tecnológicos de "administração/gestão tecnológica" (Original em Inglês "technological management") (BROWNSWORD, Roger. In the Year 2061: from law to technological management. **Law, Innovation and Technology,** v. 7, n. 1, p. 1-51, jul. 2015. p. 2).
[145] LESSIG, op. cit., 2006. p. 31.
[146] Idem, p. 31.
[147] De fato, no que diz respeito à produção de tecnologias baseadas em computadores, Grady Booch, um dos responsáveis por elaborar o importante conceito de programação orientada a objetos, lista as seguintes limitações às quais a ciência da computação estaria limitada, em ordem decrescente de dificuldade: a) as leis da física; b) as leis de software; c) o desafio dos algoritmos; d) a dificuldade de distribuição; e) os problemas de design; f) os problemas de funcionalidade; g) a importância da organização; h) o impacto econômico; i) a influência da política (BOOCH, op. cit., p. 1).
[148] LESSIG, op. cit., 2006. p. 31. p. 34.

porquanto precisariam levar em consideração as consequências das escolhas feitas na fase do *design* do sistema. Além disso, esta nova responsabilidade dos engenheiros de sistemas acarretaria também um interesse maior a respeito de suas atividades por parte de entes reguladores estatais. Por certo, como a coletividade de desenvolvedores se constitui em um alvo menor, menos difuso e mais identificável do que a coletividade de usuários, regular este ponto focal de intermediários acabaria por ser significativamente mais simples[149].

No que se refere à *regulação* feita por intermédio de tecnologias de informação e comunicação, o autor chamou atenção para o importante papel representado pela: a) *identificação* do usuário; e b) *autenticação* necessária para tornar sua identidade certa[150].

Em primeiro lugar, determinar a identidade de um indivíduo e seus atributos é um elemento essencial para que seja possível atribuir a ele responsabilidade pelas ações que realiza dentro de um sistema. Embora não seja necessária para que um sistema funcione, a existência de elementos técnicos que permitam confiar em um agente para a realização de transações é um atributo relevante para o desenvolvimento de confiança e continuidade de sistemas eletrônicos comerciais ou governamentais[151]. Entretanto, a possibilidade de identificar um indivíduo também pode acarretar consequências no que diz respeito à proteção de sua privacidade e de seus dados pessoais, já que as informações relacionadas ao usuário acabarão sendo coletadas e armazenadas pelos serviços que precisem desta identidade. Desta forma, quaisquer decisões relacionadas à eventual implementação de requisitos que exijam a inclusão desta espécie de informação deverão considerar os riscos e consequências de cada alternativa.

Em segundo lugar, tendo em vista que a inserção de dados em um sistema não passa de uma simples declaração unilateral por parte do usuário, a autenticação é exigida no âmbito destes sistemas para que seja possível confiar nestes dados. Porém, considerando que este processo nada mais é do que o cruzamento da informação original com outras informações, muitas delas pessoais, isso novamente gera novas preocupações com relação à proteção da

---

[149] Idem, p. 67-68. Ainda, conforme assevera Jonathan Zittrain, essa tendência se fortaleceria cada vez mais conforme o modelo de mercado baseado *software* enquanto serviço passasse a substituir o modelo de *software* enquanto produto (ZITTRAIN, Jonathan. A History of Online Gatekeeping. **Harvard Technology Law Review,** v. 19, n. 2, p. 253-298, 2006. p. 296).

[150] LESSIG, op. cit., 2006, p. 39.

[151] No caso da internet, a identificação dos usuários não é algo intrínseco ao funcionamento da rede mundial de computadores, pois, para tornar a infraestrutura o mais simples possível, adotou-se o princípio da arquitetura "end-to-end". Esta filosofia postula que a rede deve ser composta apenas dos protocolos mais relevantes e estratégicos para o seu funcionamento, sendo outras eventuais necessidades atendidas por protocolos colocados nas "pontas" da rede, a qual ficaria mais leve e simples para funcionar (SALTZER, J.H.; REED
, D.P.; CLARK, D.D. End-to-end Arguments in System Design. **ACM Transactions on Computer Systems,** v. 2, n. 4, p. 277-288, 1984).

privacidade dos indivíduos envolvidos. Igualmente, sendo este processo de autenticação realizado por um ou mais agentes, questionamentos acerca da confiança neles depositada tornam-se inevitáveis, devendo ser levadas em conta quando de sua implementação.

Sobre os impactos desses sistemas eletrônicos no âmbito de direitos já existentes, Lessig buscou inicialmente fazer uma reflexão sobre os efeitos destas tecnologias frente a técnicas de interpretação como o originalismo[152] e o que denominou de "tradução"[153]. Nesse sentido, utilizando como exemplo o caso *Olmstead v. United States*[154], no qual a Suprema Corte estadunidense se deparou com a necessidade de avaliar se a proteção constitucional se estendia a casos de alegada violação trazida por avanços tecnológicos, ele buscou avaliar de que maneira a interpretação constitucional deveria reagir frente ao advento de novas tecnologias.

Em primeiro lugar, entendeu que o originalismo, por buscar a solução para casos concretos no pensamento dos constituintes originários, acabaria resultando num processo gradativo de redução das proteções constitucionais frente a novas tecnologias não concebidas pelos legisladores quando da edição das normas constitucionais[155]. Esse foi o efeito da utilização desta metodologia quando da decisão final em *Olmstead*, tendo em vista que o tribunal considerou não aplicáveis as normas da quarta emenda à constituição estadunidense[156] a situações envolvendo escutas telefônicas.

---

[152] Em síntese, o "originalismo" é uma corrente hermenêutica que busca interpretar o texto constitucional de acordo com o significado original concebido pelos constituintes que escreveram e ratificaram o diploma normativo (POSNER, Eric. Why Originalism is So Popular. **The New Republic**, 14 jan. 2011. Não paginado). Esta metodologia foi fortemente defendida na Suprema Corte estadunidense pelo falecido *Justice* Antonin Scalia (SCALIA, Antonin. Originalism: The Lesser Evil. **University of Cincinnati Law Review**, n. 57, p. 849-856, 1989). Atualmente, segue sendo defendida pelos *Justices* Neil Gorsuch (GORSUCH, Neil. Of Lions and Bears, Judges and Legislators, and the Legacy of Justice Scalia. **Case Western Reserve Law Review**, v. 66, n. 4, p. 905-920, 2016) e Clarence Thomas (LIPSHUTZ, Brian. Justice Thomas and the Originalist Turn in Administrative Law. **Yale Law Journal Forum**, v. 127, p. 94-103, 2015).

[153] De fato, junto com Lessig, Laurence Tribe (TRIBE, Laurence H. **The Constitution in Cyberspace:** Law and Liberty Beyond the Electronic Frontier. Cambrigde: Harvard University Press, 1991. Não paginado) e Cass Sunstein (SUNSTEIN, Cass. The First Amendment in Cyberspace. **Yale Law Journal**, v. 104, p. 1757-1804, 1995) podem ser considerados os primeiros estudiosos estadunidenses a refletir sobre a interpretação constitucional frente aos desafios trazidos pelas novas tecnologias.

[154] UNITED STATES OF AMERICA. SUPREME COURT. **Olmstead v. United States.** 227 U.S. 438 (1928). Neste caso, a Suprema Corte aceitou analisar se o uso de conversas telefônicas privadas obtidas por meio de interceptação como meio de prova violaria a 4ª e 5ª emendas à Constituição estadunidense. Na ocasião, o tribunal entendeu por 5 votos a 4 que a proibição constitucional contra buscas e apreensões não razoáveis não seria aplicável no caso de interceptações telefônicas. Após o julgamento, ficou famoso o voto do *Justice* Brandeis, no qual o magistrado trouxe importantes reflexões sobre a necessidade de reinterpretar as proteções constitucionais frente aos possíveis riscos trazidos por novas tecnologias. Não obstante, este precedente prevaleceu durante 39 anos, sendo apenas superado em 1967 no caso *Katz v. United States* (UNITED STATES OF AMERICA. SUPRME COURT. **Katz v. United States.** 389 U.S. 347 (1967)).

[155] LESSIG, op. cit., 2006, p. 162.

[156] Diz o texto da emenda em questão que "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the

Em segundo lugar, quanto ao método da tradução, este consistiria num processo interpretativo que busca "neutralizar" os impactos de novas tecnologias ao texto constitucional[157]. Assim, partindo dos objetivos e valores inscritos na Constituição, a tradução acaba por ampliar a proteção constitucional diante dos novos desafios, acomodando o documento normativo às necessidades trazidas pelo avanço das tecnologias de informação e comunicação. De acordo com Lessig, esta foi a técnica utilizada pela Suprema Corte estadunidense quando da superação do entendimento fixado em *Olmstead* no julgamento do caso *Katz v. United States* em 1967, no qual o tribunal estendeu a proteção constitucional a casos relacionados a escutas telefônicas por considerar que os indivíduos possuiriam, de forma geral, uma expectativa razoável de privacidade.

Todavia, o autor apontou para o fato de quem nem sempre estas técnicas seriam capazes de oferecer soluções para determinados casos envolvendo novas tecnologias. Para ilustrar, citou como exemplo a proteção constitucional contra buscas e apreensões infundadas, a qual, de acordo com a doutrina estadunidense[158], teria surgido em virtude do abuso na utilização mandados de busca genéricos por oficiais da coroa britânica. Utilizados durante a época colonial, esses mandados eram frequentemente usados de modo abusivo pelos oficiais públicos, os quais possuíam alta margem de discricionariedade em sua aplicação. Entretanto, Lessig indicou que é atualmente possível, em virtude dos avanços da ciência da computação, desenvolver programas capazes de buscar, em computadores, tão-somente informações específicas, sem que nenhum outro dado seja "vasculhado" pelo *software*. Assim, por exemplo, seria hipoteticamente viável a um programa nesses moldes buscar documentos eletrônicos obtidos ilegalmente sem que nenhuma intrusão a aspectos privados fosse realizada[159]. Deste modo, questionou se ainda haveria necessidade de proteção constitucional em razão de não existir, nesta situação, margem técnica para intrusão arbitrária na esfera privada[160].

---

persons or things to be seized" (UNITED STATES OF AMERICA. **Amendments to the Constitution of the United States of America**. Washington: Government Publishing Office, 1992. p. 25).

[157] LESSIG, op. cit., 2006, p. 163.

[158] CLANCY, Thomas K. The Importance of James Otis. **Mississippi Law Journal**, v. 82, n. 2, p. 487-523, 2013. p. 488.

[159] LESSIG, op. cit., 2006, p. 25.

[160] Para uma análise de outros casos nos quais entendimentos jurídicos estadunidenses já consolidados enfrentam dificuldades para se amoldar a aspectos técnicos do funcionamento da internet, vide: BELLOVIN, Steven M. *et allia.* It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law. **Harvard Journal of Law & Technology**, v. 30, n. 1, p. 1-101, fall. 2016. Igualmente, para exame de um caso prático envolvendo a legislação britânica sobre análise preventiva de vulnerabilidades digitais por órgãos de prevenção de incidentes, vide: CORMACK, Andrew. Can CSIRTs Lawfully Scan for Vulnerabilities? **Scripted**, v. 11, n. 3, p. 308-319, dec. 2014.

Para o autor, esta inevitável necessidade de reflexão sobre questões não consideradas quando da edição das constituições do Século 20[161] acabaria por gerar uma grande pressão sobre os entes públicos. Estes, contudo, teriam ainda um desafio maior ocasionado pelo processo de paulatina corrosão da soberania estatal trazido pela existência de redes distribuídas em múltiplas jurisdições simultaneamente. De fato, assim como autores do primeiro estágio doutrinário, Lessig também reconheceu que o avanço das novas tecnologias de informação e comunicação, em especial a internet, afetaria substancialmente a capacidade dos Estados em aplicar suas normas a casos nos quais a rede mundial de computadores estivesse envolvida. Contudo, ao contrário destes estudiosos, compreendeu que o poder de aplicar sanções estatais estava diretamente relacionado à infraestrutura e a arquitetura existentes[162]. Assim, considerou que os crescentes incentivos econômicos e políticos existentes em prol de um maior controle do fluxo de informações gradativamente modificaria este cenário de "inexistência" de normas para um ambiente no qual seja possível atribuir responsabilidade às ações realizadas na internet[163]. Nesta senda, a maior possibilidade de responsabilizar as ações feitas por agentes em redes de computadores permitiria o desenvolvimento de um processo cada vez mais profundo e pervasivo de regulação e controle das condutas de indivíduos, alterando o cenário de maior liberdade até então vivenciado[164].

Durante a maior parte de *Code*, Lessig buscou descrever os efeitos trazidos pelas novas tecnologias de informação e comunicação sob uma ótica distinta – e mais madura – daquela do primeiro estágio doutrinário. Nesse sentido, aduziu que a ausência de respostas prontas frente a estas novas indagações inevitavelmente levaria à necessidade de profunda reflexão e deliberação política acerca de quais serão os valores constitucionais que irão ser efetivamente abraçados pela sociedade. Todavia, o estudioso também se mostrou reticente quanto à capacidade da sociedade e das instituições estatais de serem capazes de lidar com a complexidade destes novos desafios, receando que grupos de interesse pudessem capturar os órgãos regulatórios e movimentar o debate político de acordo com as suas agendas. Desta maneira, durante o restante de sua obra o autor procurou apresentar os problemas que seriam enfrentados pela sociedade civil diante de um ambiente cada vez mais regulado por intermédio de códigos, bem como possíveis propostas sobre como lidar com eles.

---

[161] No caso dos EUA, no Século 18.
[162] LESSIG, op. cit., 2006, p. 282.
[163] Idem, p. 309-310.
[164] Idem, p. 310.

Primeiramente, com relação ao Poder Judiciário, o autor demonstrou preocupação com o fato de que no cenário de desenvolvimento de tecnologias de informação e comunicação, muitas vezes são os atores privados – e não os estatais – os verdadeiros responsáveis pela definição de uma série decisões políticas importantes para sociedade[165]. Com efeito, ainda que esse processo de deferência à iniciativa particular dos indivíduos não seja algo intrinsecamente ruim, Lessig chamou atenção para a circunstância de que essas decisões tomadas por agentes privados não necessariamente se encontram sob os mesmos limites constitucionais impostos aos atos estatais ou mesmo sujeitas à revisão judicial[166]. Deste modo, propôs como solução para os tribunais a adoção de posicionamentos que, diante dos casos concretos, estimulem decisões voltadas a garantir a deliberação democrática pela sociedade[167], evitando assim que magistrados substituam os cidadãos no processo de deliberação política.

No que se refere ao Poder Legislativo, Lessig considerou que um dos desafios mais significativos estaria relacionado o sentimento de ceticismo que a população em geral possui frente decisões tomadas por parlamentos e assembleias[168]. De fato, confrontado com uma percepção cada vez maior de captura regulatória desses órgãos por grupos de interesse, o autor entendeu como compreensível a preocupação em delegar decisões sobre assuntos importantes e complexos aos legisladores, mesmo que ainda se dê valor a deliberações coletivas. Não obstante, também reputou como pouco producentes eventuais propostas de criação de órgãos independentes ou autônomos, pois isso, de forma geral, apenas transferiria os problemas já sofridos pelos legisladores a estas agências. Assim sendo, defendeu que seria necessário conceber mecanismos para aprimorar e tornar mais transparente a democracia representativa, sendo contrário a uma fuga total deste modelo de governança.

Com relação aos problemas envolvendo a regulação pela arquitetura, o autor referiu que os aspectos mais sensíveis estavam ligados à circunstância de a sociedade ainda não ter debatido publicamente acerca desta espécie de regulação[169]. Por certo, em virtude da pouca maturidade

---

[165] Idem, p. 317-318.
[166] Idem, p. 319. Não obstante, importante asseverar que Lessig escreveu sua obra tendo como contexto o sistema jurídico estadunidense, no qual a ordem constitucional e os atores políticos, de forma geral, preocupam-se muito mais em limitar o poder estatal do que regular ou restringir a atividade dos agentes privados, os quais possuem ampla margem de atuação. Por outro lado, no sistema jurídico brasileiro, em especial após a Constituição Federal de 1988, tanto a doutrina quanto a jurisprudência do Supremo Tribunal Federal reconhecem a denominada eficácia "horizontal" dos direitos fundamentais, isto é, entre sua aplicabilidade perante as relações entre privados (SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. rev. atual. ampl. Porto Alegre: Livraria do Advogado, 2015. p. 400-401).
[167] LESSIG, op. cit., 2006, p. 326.
[168] Idem, p. 320.
[169] Idem, p. 323.

institucional quanto à temática, uma série de questionamentos cruciais para a vida pública estariam sem respostas, o que geraria um vácuo político que seria preenchido por atores não necessariamente preocupados com valores reputados relevantes pela comunidade. Isto, somado ao cenário de ceticismo da população para com mecanismos de governança coletiva, acabaria por agravar os desafios enfrentados pela sociedade, a qual se estaria entrando num novo século sem ferramentas para lidar com eles[170].

Entretanto, ao invés de propugnar uma conduta inerte, o autor se posicionou de forma favorável ao preenchimento desses espaços deliberativos pelos indivíduos e instituições públicas que os representam, sejam elas o Poder Judiciário, o Legislativo ou o Executivo. De fato, por se considerar um constitucionalista, ele buscou sublinhar a importância da participação no processo de decisão das políticas públicas voltadas às novas tecnologias de informação e comunicação, já que apenas isso seria capaz de tornar democráticas e transparentes as medidas eventualmente escolhidas[171].

Por fim, Lessig também buscou chamar a atenção para as importantes consequências relacionadas ao desenvolvimento aberto e desenvolvimento fechado de códigos de computador[172]. Realmente, a possibilidade de ter acesso à integralidade dos comandos escritos pelos programadores significa também permitir ao público conhecer os valores e princípios escolhidos pelos desenvolvedores para compor o programa desenvolvido e os caminhos utilizados para atingi-los. Notadamente no caso das tecnologias de informação e comunicação adotadas pelo Estado, essa capacidade de conhecer os valores imbuídos no código permitiria que os cidadãos pudessem ter condições de controlar as atividades dos entes estatais que utilizem este meio para implementar sua regulação[173].

Além dessa característica, o pesquisador considerou que, no que diz respeito à sua filosofia de desenvolvimento, a transparência inerente aos códigos abertos tem como implicação não apenas o maior controle, mas também a maior *participação* pelo público[174]. Com efeito, apesar de ter reconhecido que as participações de diferentes pessoas

---

[170] LESSIG, Lawrence. **Governance.** [s.l.]: CPSR Conference on Internet Governance, 1998. p. 1.
[171] Idem, p. 15.
[172] O tópico relativo a produção de softwares em código aberto ou fechado será tratado com mais atenção na seção **4.2.1**. Não obstante, para os fins desta etapa, importa dizer que a diferença entre as duas modalidades de produção de software está no fato de a primeira disponibilizar o código-fonte para qualquer interessado, independentemente de autorização, ao passo que na segunda o código-fonte apenas estará acessível àqueles autorizados pelo seu criador.
[173] LESSIG, op. cit., 2006, p. 327-328.
[174] LESSIG, Lawrence. Open Code and Open Societies: Values of Internet Governance. **Chicago-Kent Law Review**, v. 74, p. 101-116. 1999. p. 112.

inevitavelmente não serão iguais, Lessig refletiu ser importante para uma democracia, especialmente diante desta nova realidade, a manutenção da participação enquanto um valor constitucionalmente consagrado[175]. Em síntese, longe de defender a substituição da propriedade privada pelo *commons*, compreendeu ser crucial para o regime democrático o encontro de um ponto de equilíbrio[176], no qual seja possível à população ter liberdade para escolher os valores que irão informar seus mecanismos de governança num momento em que cada vez mais plataformas eletrônicas se tornam relevante para o funcionamento da sociedade[177].

2.3 DO TERCEIRO ESTÁGIO DO DEBATE DOUTRINÁRIO: A RELEITURA CRÍTICA SOBRE O PAPEL E LIMITES DA ARQUITETURA DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO COMO MECANISMO REGULATÓRIO

Os estudos e reflexões realizados pelo segundo estágio do debate doutrinário trouxeram profundos impactos na forma como as tecnologias de informação e comunicação são vistas sob a ótica de sua capacidade de conformar condutas. De fato, em virtude das contribuições de autores como Joel Reidenberg e, principalmente, Lawrence Lessig, outros pesquisadores passaram a estudar as características da regulação baseada em códigos de computador, bem as consequências que determinadas escolhas sobre o *design* destas tecnologias poderiam acarretar para a vida dos indivíduos a elas sujeitas. Como a segunda etapa da discussão doutrinária foi marcada pela crítica à primeira geração de autores que estudaram o fenômeno das novas tecnologias sob a perspectiva jurídica, o terceiro momento doutrinário também possui como característica a apresentação de respostas por parte destes pensadores às críticas recebidas.

Talvez por ter sido diretamente criticado em *Code*[178], Declan McCullagh pode ser considerado um dos primeiros a se manifestar contra a ideia de que não se poderia deixar as escolhas políticas relacionadas à regulação baseada em tecnologias de informação e comunicação exclusivamente para o setor privado[179]. A despeito de concordar com a

---

[175] Idem, p. 116.
[176] Ou, conforme Henry Perrit Jr, "uma forma de conexão" (PERRIT JUNIOR, Henry H. Book Review: Lawrence Lessig, Code and Other Laws of Cyberspace. **Connecticut Law Review**, v. 32, p. 1061-1064, mar. 2000. p. 1064).
[177] Idem, p. 116. FREITAS, Marcio Luiz Coelho de. Entre tecnodeterminismo e interesse público: limites e possibilidades de regulação da internet. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 10, n. 1, p. 125-146, maio. 2018. p. 141-142.
[178] De fato, o último capítulo do livro se chama "What Declan Didn't Get", o que, numa tradução livre, significa "O que Declan não Entendeu".
[179] MCCULLAGH, Declan. Lessig Suffers from Bad Code. **Wired,** 06 out. 1999. Não paginado.

constatação de que somos cada vez mais regulados por intermédio de códigos de computador, McCullagh considerou que o manifesto feito pelos tecnorealistas[180] não poderia ser levado a sério pois, ainda que as decisões tomadas pelo mercado não sejam sempre as melhores, elas seriam superiores àquelas adotadas pelo governo. De fato, para ele as falhas governamentais relacionadas ao risco moral, captura regulatória e *rent-seeking* de medidas estatais ligadas a políticas públicas sobre novas tecnologias demonstravam que mecanismos privados de seriam mais eficientes na tomada de decisões do que o Estado[181].

Além de Declan McCullagh, outros também compartilhavam a criticavam a afirmação de que plataformas privadas assumiriam papel cada vez mais relevantes no controle de condutas. Nesse sentido, Adam Thierer, por exemplo, considerava que o ideário de autores como Lessig, Wu e Zittrain acabava efetivamente por impedir o desenvolvimento de ecossistemas mais livres para a criação de novas tecnologias ao incentivar a intervenção por agentes estatais com foco coletivista[182].

David Post, por sua vez, embora afirmasse não desconhecer os riscos que qualquer concentração de poder poderia trazer às liberdades dos indivíduos, rejeitou a conclusão de Lessig de que o Estado, enquanto representante da vontade coletiva, deveria intervir para salvaguardar a liberdade da sociedade[183]. Para ele, ainda que vontade coletiva manifestada por meio de mecanismos estatais fosse importante em muitos momentos, isso não significaria que devesse ser sempre a resposta adequada para a resolução de problemas. Nesse sentido, reforçou mais uma vez seu entendimento segundo o qual, no mais das vezes, a resposta para os problemas advindos da internet seria oriunda do agregado de decisões individuais não coagidas por algum fator externo[184]. Por outro lado, Paul Schwartz e Marc Rotenberg, ao examinar algumas das ideias contidas em *Code*, criticaram fortemente a importância que Lessig teria conferido à ação isolada de indivíduos para a proteção de direitos por intermédio da arquitetura de tecnologias. Para eles, problemas envolvendo a racionalidade limitada dos agentes e a dificuldade de

---

[180] No contexto estadunidense, o "tecnorealismo" foi um movimento político idealizado por jornalistas e escritores entre 1998 e 1999 em defesa de uma postura não extremista frente aos avanços tecnológicos experimentados na proximidade dos anos 2000. Para eles, era necessário adotar uma compreensão crítica, nem utópica ou distópica, sobre os impactos que as novas tecnologias de informação e comunicação estavam exercendo na sociedade (SHENK, David; SHAPIRO, Andrew J.; JOHNSON, Steven. **Technorealism**. [s.l., s.n.]: 1998. Não paginado).
[181] MCCULLAGH, Declan. What Larry Didn't Get. **Cato Unbound**, 4 may. 2009. Não paginado.
[182] THIERER, Adam. Code, Pessimism, and the Illusion of "Perfect Control". **Cato Unboud**, 8 may. 2009. Não paginado.
[183] POST, David G. What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace. **Stanford Law Review**, v. 52, p. 1439-1459, may. 2000. p. 1443.
[184] Idem, p. 1458.

coordenação coletiva acabariam por colocar em xeque o desenvolvimento de sistemas para a salvaguarda da privacidade[185].

Entretanto, apesar de as críticas baseadas nos fundamentos filosóficos e econômicos serem relevantes para a compreensão da temática da regulação de tecnologias de informação e comunicação, a terceira etapa do debate doutrinário não se limitou a este aspecto. Nesse sentido, ao revisitar as considerações do segundo estágio doutrinário, Murray e Scott propuseram uma visão diferente sobre o modo de observar a regulação com base na teoria do controle[186]. Para eles, tomando por base os elementos necessários para a criação de um sistema de controle (definição de padrões, coleta de informações e modificação de comportamentos), a estrutura concebida por Reideberg e aprofundada por Lessig poderia ser aprimorada para melhor compreensão da regulação de plataformas tecnológicas[187].

De início, Murray e Scott propõem que a noção de "direito" ou normas exclusivamente jurídicas seja substituída pelo conceito de "controle hierárquico". Deste modo, ao invés de focar na fonte do mecanismo de controle, a análise poderia estudar com mais atenção a *forma* do mecanismo de controle e, com isso, abranger elementos não-estatais que também impõem deveres de atuação[188]. Com relação ao conceito de "normas sociais", propõem a utilização do conceito de "controle comunitário", capaz de abranger não somente estruturas sociais informais, como também modelos mais formalmente estruturados, tais como mecanismos de auto-regulação reconhecidos pelo Estado[189]. Quanto à regulação advinda do "mercado", a qual Lessig compreende como baseada em mecanismos de preço, sugerem a utilização do conceito de "competição", o qual é aplicável com mais facilidade em contextos nos quais não é possível delimitar com precisão o mercado, os agentes nele envolvidos e o preço dos produtos, a exemplo de situações de concorrência entre reguladores[190]. Finalmente, ao invés de focar exclusivamente em "códigos" enquanto mecanismos de regulação, os autores recomendam a utilização do conceito de "design" o qual, sendo mais abrangente, consegue de abarcar também

[185] SCHWARTZ, Paul M. Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices. **Wisconsin Law Review**, v. 2000, n. 1, p. 743-788. 2000. p. 766. ROTENBERG, Marc. Fair Information Practices and the Architecture of Privacy: What Larry Doesn't Get. **Stanford Technology Law Review**, v. 1, 2001. p. 33.
[186] MURRAY; SCOTT, op. cit., p. 502.
[187] BROWNSWORD, Roger. Code, Control, and Choice: why East is East and West is West. **Legal Studies**, v. 25, n. 1, p. 1-21, apr. 2006, p. 7.
[188] MURRAY; SCOTT, op. cit., 502.
[189] Idem, p. 503.
[190] Idem, p. 503.

arcabouços institucionais que, por sua própria modelagem, são capazes de conformar a conduta de indivíduos[191].

De fato, a partir da contribuição feita por Murray e Scott se torna mais simples compreender o argumento desenvolvido por Timothy Wu segundo o qual códigos de computador não apenas servem para conformar a conduta de indivíduos, mas também podem ser utilizados como mecanismos anti-regulatórios[192]. Para este autor, além da capacidade de substituir ou reforçar outras modalidades de regulação, a arquitetura de *softwares* e *hardwares* pode ser empregada como ferramenta por indivíduos ou grupos geralmente desorganizados para avançar agendas políticas que de outro modo não conseguiriam impactar significativamente na sociedade[193].

Com efeito, Wu desenvolveu sua tese tomando como base elementos de duas áreas que estudam o comportamento de grupos e indivíduos quando confrontados com institutos de regulação jurídica[194]: o *compliance,* o qual argumenta que agentes irão procurar *evitar* normas jurídicas que julguem particularmente onerosas e a *political choice,* que observa que agentes irão buscar *modificar* estas normas quando preenchidas condições semelhantes.

De forma sintética, os modelos econômicos básicos por trás *compliance theory* referem que grupos obedecem à lei quando os custos estimados da punição excederem os benefícios estimados da conduta proibida[195]. Porém, para além desses elementos, é igualmente necessário que sejam considerados na equação os *investimentos* feitos pelos agentes para evitar a punição[196]. Nesse sentido, a doutrina prossegue por descrever dois mecanismos distintos utilizados para evitar a sanção legal[197]: a) a "evasão", que consistiria simplesmente no investimento geral em maneiras se evitar ser punido; e b) a "elisão", a qual se configura quando são utilizados procedimentos jurídicos para desviar um determinado procedimento legal de seu propósito ou aproveitar ambiguidades normativas, sem, contudo, agir ilegalmente. Por sua vez, o modelo econômico básico que lastreia a *political choice theory* aborda a modificação de uma

---

[191] Idem, p. 503.
[192] WU, Timothy. When Code Isn't Law. **Virginia Law Review**, v. 89, n. 4, p. 103-170, 2003.
[193] Idem, p. 106.
[194] Idem, p. 109.
[195] BECKER, Gary. Crime and Punishment: An Economic Approach. **Journal of Political Economy,** v. 76, n. 2, p. 169-217. mar./apr. 1968. p. 204.
[196] BECKER, Gary S.; STIGLER, George J. Law Enforcement, Malfeasance, and Compensation of Enforcers. **The Journal of Legal Studies**, v. 3, n. 1, p. 1-18, jan. 1974. p. 2-6.
[197] WU, op. cit., p. 115. No artigo em questão, o autor utiliza respectivamente os termos "evasion" e "avoision" para descrever estas duas estratégias utilizadas para evitar sanções (Idem, p. 114-116).

determinada decisão legislativa (mediante lobby) – ou mesmo judicial (através de litígios)[198] – como sendo uma *commodity* disponível para aquisição por grupos de interesse[199]. Todavia, ao contrário de um bem econômico qualquer, a "aquisição" ou "consumo" de uma determinada política pública – isto é, o sucesso de um grupo em modificar determinada decisão estatal – irá automaticamente transferir riqueza de um grupo para outro[200]. Em outras palavras, para cada grupo beneficiado regulação existirá um grupo prejudicado por ela[201].

Por certo, embora a finalidade dessas reações de *modificar* ou *evitar* a regulação seja mesma, o "custo" de cada uma é significativamente distinto. De acordo com a lógica por trás da *collective action* descrita por Mancur Olson[202], quanto maior um grupo de indivíduos, maiores serão os custos e desafios por eles enfrentados para fazer avançar sua agenda política[203]. Assim, aqueles grupos que não possuírem os recursos necessários acabarão por ser derrotados no processo político pela modificação da regulação objeto de disputa coletiva[204].

Contudo, discordando da conclusão de Olson de que os grupos derrotados "sofreriam em silêncio"[205], Timothy Wu argumentou que as novas tecnologias de informação e comunicação, em virtude de seu custo comparativamente reduzido e sua utilização disseminada, podem ser utilizadas como ferramenta para evitar sanções legais[206]. Notadamente no caso de grupos menores ou mesmo de indivíduos isolados, sistemas de computador podem ser configurados muito mais facilmente para atingir os objetivos de evasão ou elisão pretendidos pelos seus desenvolvedores. Com efeito, iniciativas com características *peer-to-peer*[207] e *open source*[208] são ainda mais eficientes nesse propósito, porquanto a difusão dos agentes envolvidos torna

---

[198] LANDES, William M.; POSNER, Richard A. The Independent Judiciary in an Interest-Group Theory. **The Journal of Law and Economics**, v. 18, n. 3, p. 875-901. dec. 1975. p. 894.
[199] STIGLER, op. cit., 1971. p. 12-13. PELTZMAN, Sam. Toward a More General Theory of Regulation. **The Journal of Law and Economics**, v. 19, n.2, p. 211-240, 1976. p. 212. STIGLER, George J. The Size of Legislatures. **The Journal of Legal Studies**, v. 5, n. 1, p. 17-34, jan. 1976. p. 19.
[200] PELTZMAN, op. cit., p. 213-214.
[201] WU, op. cit., p. 126. STIGLER, op. cit., 1976. p. 19.
[202] OLSON JUNIOR, Mancur. **The Logic of Collective Action**: Public Goods and the Theory of Groups**.** Cambridge: Harvard University Press, 1971.
[203] Idem, p. 53.
[204] Idem, p. 165.
[205] Idem, p. 165.
[206] WU, op. cit., p. 128.
[207] De acordo com a RFC 5694, um sistema *peer-to-peer*, também chamado de P2P, é um sistema no qual os elementos que o compõem compartilham seus recursos para fornecer o serviço para o qual a rede foi concebida. Nesse sentido, os elementos desse sistema são ao mesmo tempo fornecedores e utilizadores de serviços (CAMARILLO, G. (ed.). **Request For Comments 5694:** Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability. Finland: Network Working Group, 2009. p. 3-4).
[208] O conceito de "open source" será tratado com mais atenção na seção **4.2.1**, não obstante, para o presente momento consideramos "open source" aqueles sistemas cujo código-fonte está disponível de forma livre para qualquer modificação e redistribuição (OPEN SOURCE INIATIATIVE. **The Open Source Definition.** S.l.: OSI, 2007. Não paginado).

ainda mais difícil a individualização usualmente exigida para a aplicação de sanções estatais. Somado a isso, naquelas situações onde a regulação questionada for particularmente controvertida ou não tiver suporte significativo da população, mecanismos de coerção social podem não ser eficientes para coibir (ou podem até mesmo incentivar) que programadores concebam *softwares* aptos a burlar ou evitar a aplicação de sanções[209].

A compreensão de que a arquitetura de sistemas – o código – pode ser utilizada não apenas para reforçar, mas também para atenuar a efetividade de outros mecanismos de regulação certamente representa um adendo relevante para a estrutura desenvolvida pelos autores do segundo estágio doutrinário. Afinal, uma das principais preocupações dos autores deste estágio era de que códigos de computador cada vez mais serviriam para como instrumentos de controle a erodir a liberdade de ação e enfraquecer os demais direitos dos indivíduos.

Todavia, até este ponto a literatura jurídica aqui examinada, apesar de examinar a regulação feita por intermédio da arquitetura de sistemas, não focou no estudo de códigos computador em si mesmos. Por certo, ainda que a um jurista não seja necessário conhecer diretamente como programar e utilizar linguagens de computador, compreender minimamente o funcionamento dessas ferramentas torna-se relevante para que não atingir conclusões equivocadas, desprovidas de bases fáticas ou sem conexão com a realidade. Essa foi a preocupação de James Grimmelmann ao estudar a regulação feita por *softwares*[210] e suas característica sob a perspectiva técnica.

Embora anuísse à tese de que códigos de computador sejam uma modalidade regulatória, o autor considerou que a análise feita por Lessig seria incompleta em razão de existirem diferenças qualitativas significativas entre a regulação feita por estruturas físicas e aquela resultante de arquiteturas de tecnologias de informação e comunicação em razão de três principais características destas últimas: automação, imediaticidade e plasticidade[211]. Para Grimmelmann, a interação entre essas características geraria consequências que separariam

---

[209] WU, op. cit, p. 170. Para ilustrar seu argumento, o autor apresentou diversos exemplos, tais como: a) desenvolvimento de pornografia gerada por computador naqueles casos em que a legislação proíbe a filmagem de pessoas fazendo sexo; b) utilização de domínios e servidores localizados em outros países quando a jurisdição local proíbe determinada atividade online; c) criação de redes de compartilhamento gratuito de pedaços de arquivos para quanto a lei proíbe a alienação total ou a alienação onerosa de determinado objeto eletrônico (Idem, p. 129-130).

[210] GRIMMELMANN, James. Regulation by Software. **Yale Law Journal**, v. 114, p. 1719-1758, 2005.

[211] Idem, p. 1722-1723.

paradigmaticamente a regulação por *softwares* dos demais mecanismos regulatórios, transformando-a em uma modalidade distinta cuja análise mereceria maiores cuidados[212].

Em primeiro lugar, no que se refere à *automação*, ela significa que o único agente necessário para fazer um sistema eletrônico funcionar é o seu próprio programador. Nesse sentido, uma vez concluída a construção da arquitetura do código, o custo marginal para executá-lo pode ser extremamente reduzido. Assim, um sistema pode produzir seus efeitos desejados e prescindir da ação de agentes humanos.

Em segundo lugar, no que tange à *imediaticidade*, ela significa que as normas estabelecidas pelo desenvolvedor do *software* estão já delineadas aprioristicamente antes da realização da conduta sujeita à regulação. Isso ocorre porque a estrutura de um programa é baseada nas informações existentes no momento de sua concepção. Deste modo, para que um determinado conjunto de dados seja levado em consideração no momento da execução do código, é necessário que seu programador tenha incluído essa circunstância em seus requisitos, sob pena destes fatores serem completamente ignorados pelo sistema. Em decorrência disso, programas de computador não podem, ao contrário de normas jurídicas, se adaptar a circunstâncias desconhecidas antes do momento da análise do caso concreto.

Em terceiro lugar, quanto à *plasticidade*, dela decorre que o processo de desenvolvimento de tecnologias de informação e comunicação estão sujeitos praticamente apenas à capacidade do programador. De fato, um processo capaz de ser descrito de forma lógica, precisa e em um número finito de etapas é apto a ser expresso em linguagem de programação[213]. Somada à capacidade computacional crescente oriunda de semicondutores cada vez mais eficientes, isso significa que mesmo processos contendo milhões de etapas diferentes podem ser tornados eletrônicos.

Essas três características ajudam a compreender o motivo pelo qual tecnologias de informação e comunicação substituem processos não eletrônicos porquanto o aumento exponencial da capacidade produtiva acaba por ser argumento praticamente impossível de ser resistido. Todavia, esses mesmos fatores também acarretam consequências relevantes que, a despeito de previsíveis, não são frequentemente apontadas pela literatura jurídica que explora essa temática regulatória.

---

[212] Idem, p. 1728-1732.
[213] KNUTH, Donald Erving. **The Art of Computer Programming:** fundamental algorithms. 3 ed. Reading: Addison-Weiley, 1997. p. 4-6.

Com efeito, a primeira consequência se refere à estrutura normativa de sistemas baseados em códigos de computador. Tendo em vista as características de automação e imediaticidade, *softwares* são estruturados exclusivamente a base de regras, não utilizando, ao contrário de mecanismos jurídicos, uma mistura normativa de princípios e regras[214]. Disso decorrem pontos importantes, conforme se listam abaixo.

Estruturas não definidas aprioristicamente, baseadas em conceitos indeterminados, tais como "justiça", "boa fé" ou "equidade", simplesmente não podem ser descritas. Assim, naqueles casos em que não o responsável por definir o mecanismo regulatório não detiver informações suficientes para formular regras adequadas, a utilização de sistemas eletrônicos não será a melhor opção. Além disso, diferentemente de regras jurídicas, regras escritas em código de computador possuem uma definição muito maior, não dependendo de preconcepções de seu usuário ou preocupações políticas para serem executadas após terem sido definidas por seu programador.

Somados a estes pontos, regras escritas em código respondem de forma notadamente diferente das regras jurídicas frente à complexidade do sistema em que estão inseridas. Tratando-se de regras jurídicas, quanto mais extenso for a articulação de seu enunciado e quanto maior for o número de normas que tiver de interagir, mais difícil será a sua aplicação. Regras em código, ao seu turno, não sofrem deste problema, sendo perfeitamente comum que um sistema seja composto de centenas ou milhares de regras articuladas logicamente em linguagem de programação sem que isso resulte em alguma indefinição ou impossibilidade de execução.

Por sua vez, a segunda consequência está diretamente relacionada à "transparência" de mecanismos regulatórios baseados em tecnologias de informação e comunicação[215]. Em sistemas jurídicos, a previsibilidade da aplicação das normas e a possibilidade de se opor a aplicações consideradas injustas são considerados fatores fundamentais para a existência de um Estado de Direito[216]. Contudo, tratando-se de normas escritas em códigos, a assimetria informacional existente entre o desenvolvedor do sistema (agente regulador) e seu usuário (agente regulado) implica que este último, muito embora possa eventualmente perceber sua incapacidade de agir de determinada maneira, não compreenda o motivo disto[217]. Ademais,

---

[214] Idem, p. 1732.
[215] Idem, p. 1734.
[216] Roger Brownsword também postula que a possibilidade de um indivíduo em escolher por respeitar ou não uma norma está intimamente relacionada à sua dignidade enquanto ser humano (BROWNSWORD, op. cit., 2006, p. 17-19).
[217] GRIMMELMANN, op. cit., p. 1736.

devido à complexidade que um sistema eletrônico pode facilmente atingir, nem sempre os próprios agentes responsáveis pela sua programação são capazes de explicar o comportamento de suas criações[218]. Portanto, se a própria explicação sobre os motivos de determinado funcionamento é complicada, com muito mais razão será difícil se opor a determinados resultados indesejados por não ser possível identificar a sua origem.

A terceira consequência relativa à utilização de códigos de computador para regulação está vinculada à impossibilidade prática dos agentes regulados de ignorar regras impostas por estes mecanismos[219]. De fato, ainda que existam normas jurídicas para a regular praticamente qualquer conduta em nossa sociedade, os indivíduos geralmente não precisam invocar elas na maior parte de suas interações cotidianas. Nesse sentido, quando o resultado-padrão estabelecido pela norma jurídica não se encontra de acordo com seus interesses, as pessoas negociam soluções alternativas de acordo com os seus interesses e de acordo com a estrutura admitida por normas sociais. Assim, as normas jurídicas apenas se tornam efetivamente relevantes como *ultima ratio*, quando agentes não conseguem atingir satisfatoriamente uma solução por seus próprios meios. Porém, isto tudo apenas é possível devido ao fato de que normas jurídicas e sociais não possuem – ao contrário de sistemas eletrônicos – a característica da automação. Realmente, no caso de regras escritas em linguagem de programação, esta faceta pode acabar por aumentar os custos de transação se a solução final determinada pelo desenvolvedor do sistema for ineficiente. Ademais, ao contrário de outras modalidades regulatórias, a automação e a assimetria informacional do usuário, inerentes à regulação via tecnologias de informação e comunicação, dificultam que os responsáveis por seu desenvolvimento tomem medidas para prevenir problemas advindos de sua execução, pois estes muitas vezes após são percebidos após se concretizarem.

Finalmente, o quarto fator a ser levado em conta quando da utilização de estruturas regulatórias baseadas em sistemas eletrônicos diz respeito ao fato de que estes estão sujeitos a vulnerabilidades ocasionadas por falta de robustez, erros de programação[220] ou ataques de *hackers*[221]. Muito embora programas de computador sejam ferramentas indissociáveis da vida

---

[218] Idem, p. 1737.
[219] Idem, p. 1738.
[220] CHARETTE, Robert N. Why Software Fails: We waste billions of dollars each year on entirely preventable mistakes. **IEEE Spectrum**, 2 set. 2005. Não paginado.
[221] Trata-se de termo da Língua Inglesa sem tradução específica para a Língua Portuguesa. Em síntese, "hackers" são indivíduos proficientes em ciência da computação, capazes de explorar, invadir e modificar sistemas eletrônicos. De acordo com a RFC1983, "hacker" seria "a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular" (MALKIN, Gary Scott (Ed.). **Request for Comments 1983:** Internet Users' Glossary. Burlington: 1996. p. 22). Original em Inglês. Tradução

moderna e sejam cada vez mais onipresentes no cotidiano, isto não significa que estão isentos de problemas em seu funcionamento.

De fato, para além do campo de operações aritméticas básicas, construir algoritmos lógicos em linguagem de programação não é uma tarefa fácil, pois cada elemento introduzido no código-fonte de um sistema adiciona progressivas camadas de complexidade. Nesse sentido, a depender da arquitetura utilizada, elementos inseridos no código-fonte em momentos diferentes podem ter interações inesperadas e imprevisíveis, as quais podem acarretar desde um "simples" funcionamento ineficiente até uma falha completa do sistema capaz de torna-lo inoperante.

Estes problemas oriundos da interação entre elementos diferentes do código podem ocorrer ainda que o desenvolvedor não erre ou troque por equívoco sequer um símbolo alfanumérico durante o processo de desenvolvimento. Entretanto, em condições normais, é extremamente corriqueiro a existência de erros acidentais em códigos de sistemas. Exemplificativamente, expressões como "X = Y", "X = = X" e "X =! Y", embora aparentemente semelhantes, possuem resultados completamente diferentes quando implementadas. Assim, considerando que programas de computador podem chegar a ter milhões de linhas de código, é comum a existência de centenas – ou mesmo milhares – de erros, os quais podem ter consequências imprevisíveis e inesperadas, gerando fragilidades e reduzindo a confiabilidade destas ferramentas.

Além destas fragilidades naturais, tecnologias de informação e comunicação estão corriqueiramente sujeitas a ataques por parte de indivíduos ou grupos que buscam comprometer a integridade do sistema ou roubar ou modificar dados nelas armazenadas. De fato, quanto mais complexo um sistema, maior será a sua "hackeabilidade"[222], porquanto um agente dedicado poderá estudar o seu funcionamento e explorar os inevitáveis pontos fracos existentes em seu favor, alterando a finalidade de um programa e prejudicando seus usuários. Infelizmente, a despeito do avanço da utilização de novas tecnologias computacionais pela sociedade ter impactos significativos na melhoria da produtividade de empresas e na qualidade de vida das

---

livre "uma pessoa que tem prazer em ter um conhecimento íntimo do funcionamento interno de um sistema, computadores ou redes de computadores em particular". Este termo não deve ser confundido com "cracker", o qual é definido pela RFC 1983como sendo "an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers [...]" (Idem, p. 13). Original em Inglês. Tradução livre: "um indivíduo que tenta acessar sistemas de computador sem autorização. Estes indivíduos geralmente agem de má-fé, ao contrário de hackers [...]".

[222] Trata-se de tradução livre do termo da Língua Inglesa "hackability". Em síntese, o termo descreve a característica do nível de sujeição ou propensão de um determinado sistema eletrônico a ataques ou invasões feitas por "hackers".

pessoas em geral, este processo de digitalização do cotidiano também tem levado a uma progressiva ampliação dos riscos relacionados à cibersegurança.

Em síntese, muito embora a ubiquidade de sistemas eletrônicos tenha propiciado o surgimento de novos mercados e oportunidades tanto para o setor privado quanto para o setor público, relatórios atualmente apontam que é impossível eliminar completamente riscos relativos à segurança digital[223]. Por causa disso, no momento de definição de uma estratégia regulatória faz-se necessário examinar não apenas os possíveis impactos de uma regulação baseada em tecnologias de informação e comunicação, mas também avaliar tal modalidade é definitivamente a mais indicada para a consecução da finalidade desejada. Em sua análise sobre o tema, James Grimmelmann concluiu que ainda que em alguns casos sistemas eletrônicos possam ser atrativos, sua utilização, em razão das características e fatores descritos acima, também pode ser demasiadamente perigosa[224]. Portanto, a formulação de políticas que envolvam este tipo de abordagem deve levar permanentemente em conta estes riscos, justificando decidir assumi-los ou não e explicando as medidas que serão tomadas para reduzi-los e para atenuar seus impactos caso venham a se concretizar. Além disso, políticas públicas voltadas a regular a arquitetura de tecnologias de informação e comunicação devem também considerar essas características da utilização de linguagens e códigos de programação, sob pena de serem ineficientes ou mesmo incompletas e incapazes de atender todos os tópicos pretendidos.

2.4 SÍNTESE DESTA SEÇÃO

O avanço progressivo das tecnologias de informação e comunicação desde a segunda metade do Século 20 gerou – e continua gerando – profundos impactos na sociedade atual, modificando significativamente a forma se produz e dissemina informações. Neste cenário, juristas cada vez mais têm se deparado com a necessidade de estudar o relacionamento do Direito frente a estes novos mecanismos e ferramentas, os quais podem ser utilizados tanto para reforçar como para atenuar os regulamentos estatais.

---

[223] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Managing Digital Security and Privacy Risk.** Paris: OECD, 2016. p. 4.
[224] GRIMMELMANN, op. cit., p. 1758.

Deste modo, considerando que o cenário jurídico estadunidense possui, em razão de motivos históricos, mais experiência com o estudo da temática do que o Brasil, buscou-se examinar a evolução do debate doutrinário a respeito de regulação e tecnologias de informação e comunicação especialmente no que tange aos principais às principais teses. Assim, em primeiro lugar, buscou-se separar os estágios da discussão, identificando os principais autores e suas teses centrais.

Nesta senda, foi possível delinear a existência de três grandes etapas do debate acadêmico, cujas características, na nossa opinião, estão ligadas ao grau de maturidade e compreensão adequada sobre o funcionamento de sistemas eletrônicos e seu relacionamento com o Estado e a regulação dele advinda. Assim, na primeira fase do debate, Clark, Postel, Cerf, Barlow, Post, Johnson, Easterbrook, entre outros, defenderam fortemente o afastamento do Estado e suas normas do setor de tecnologia de informação e comunicação. Estes autores, céticos quanto à capacidade dos agentes estatais de compreenderem o funcionamento destas novas ferramentas, questionavam tentativas governamentais de regulação. De forma geral, para eles os órgãos de regulação central não conseguiriam impor suas regras em ambientes digitais descentralizados. Ademais, mesmo que conseguissem, a atuação estatal não seria legítima, pois reduziriam ou eliminariam as liberdades individuais existentes em um espaço que não pertenceria a nenhum Estado em específico.

Por sua vez, estudiosos da fase seguinte, como Netanel, Radin, Wagner, Zittrain, Perrit Junior, Reidenberg e Lessig possuíam um entendimento diverso, mais realista, sobre o relacionamento entre a regulação estatal e tecnologias de informação e comunicação. Para eles essas tecnologias seriam capazes de gerar efeitos nas sociedades que não poderiam ser ignorados pelos Estados, os quais não apenas deveriam, como seriam plenamente capazes de interagir, desde que com cautela, frente a estes efeitos. Para tanto, reguladores públicos deveriam passar a compreender e interagir mais com os desenvolvedores e engenheiros de sistemas eletrônicos, porquanto estes também passaram a ser capazes de regular a conduta de indivíduos em razão da arquitetura escolhida para seus programas. De fato, os autores deste momento doutrinário postulavam que o processo de desenvolvimento de programas havia se transformado em um verdadeiro processo de formulação de políticas públicas, sendo, portanto, imperioso considerar se os valores informativos de determinada arquitetura tecnológica estão em conformidade com valores públicos constitucionalmente relevantes e protegidos. Ademais, consideravam que a arquitetura destes sistemas seria apenas mais uma dentre diversas

modalidades de regulação, as quais apenas poderiam ser adequadamente utilizadas se analisadas em conjunto.

Finalmente, ao analisar estes argumentos, a terceira fase da doutrina adotou posicionamentos mais difusos. Assim, McCullagh, Thierer, Post, Schwartz e Rotenberg, muito embora aceitassem a constatação de que códigos de computador também seriam capazes de regular e entendessem a relevância das regras por eles estabelecidas, continuavam a criticar a defesa em prol de um maior avanço do Estado para regular o desenvolvimento de tecnologias de informação e comunicação. De acordo com esses autores, a regulação estatal padeceria de permanente captura por parte de determinados setores, sendo incapaz de produzir normas aplicáveis ao setor tecnológico que não prejudicassem os cidadãos. Ademais, a lentidão das instituições estatais prejudicaria o processo de inovação tecnológica já que criaria mais incertezas e ônus ao desenvolvimento de novas ferramentas. Deste modo, argumentavam que a autorregulação pelos agentes de mercado seguia sendo o único mecanismo capaz de produzir os melhores resultados e, ao mesmo tempo, salvaguardar as liberdades individuais. Ao seu turno, Wu e Grimmelmann preferiram focar em tópicos distintos, identificando que sistemas eletrônicos não seriam ferramentas regulatórias perfeitas e aplicáveis em qualquer caso, além de servirem como subterfúgio a outras modalidades regulatórias ao reduzir seus efeitos.

Diante do que foi exposto, torna-se claro que conhecer as reflexões feitas pela doutrina estadunidense se mostra importante para estudar e compreender propostas regulatórias que pretendam influenciar a atividade de responsáveis pelo desenvolvimento de sistemas eletrônicos a implementar políticas públicas. De fato, a contribuição destes autores para o estudo da área, ao permitir identificar o funcionamento da regulação pela arquitetura de tecnologias de informação e comunicação e o papel de cada ator envolvido neste processo gradativamente modificou a estratégia adotada por entes reguladores. Influenciados por este novo entendimento, legisladores passaram a defender a adoção de medidas normativas cuja abordagem não estava em simplesmente estabelecer proibições, mas em desenvolver mecanismos que incentivasse a internalização de valores socialmente relevantes. Dentre estas novas metodologias de proteção de direitos fundamentais, aquela cuja finalidade está voltada a salvaguardar a privacidade de indivíduos, denominada *privacy by design*, passou recentemente a receber cada vez mais atenção em diplomas jurídicos de diversas jurisdições, dentre elas a União Europeia e o Brasil. Em virtude disso, a seção **3** a seguir buscará estudar melhor este instituto, de forma a identificar sua origem e desenvolvimento, sua evolução normativa e, ao final, sua operacionalização.

3 REGULAÇÃO DA ARQUITETURA DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO PARA A PROTEÇÃO DA PRIVACIDADE: O INSTITUTO DO *PRIVACY BY DESIGN*

Desde a publicação do artigo de Samuel Warren e Louis Brandeis[225] em 1890, a literatura jurídica se preocupa com os impactos causados ao direito fundamental à privacidade pelo advento de novas tecnologias de informação e comunicação[226]. Porém, não apenas juristas externavam preocupação quanto ao assunto. De fato, motivadas pela falta de confiança no tratamento de dados pelos órgãos estatais [227] e receosos da utilização abusiva de suas informações pessoais, as populações dos países ocidentais[228], em particular as do hemisfério norte, foram gradativamente compelindo e pressionando os agentes políticos a desenvolver um arcabouço normativo voltado ao tema[229].

Entretanto, até o início da década de 90, agentes reguladores de forma em geral percebiam a utilização crescente de tecnologias de informação e comunicação apenas como sendo a fonte do problema[230]. Em virtude disso, propostas regulatórias até então existentes de forma geral transitavam principalmente entre regimes de responsabilização civil[231] ou o reconhecimento de direitos de propriedade vinculados à esfera individual de privacidade[232].

De fato, antes da invenção da *World Wide Web* em 1989 por Tim Berners-Lee e do lançamento do navegador *Mosaic* em 1993 pela equipe de Marc Andreessen e Eric Bina[233], a

---

[225] WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy.** Harvard Law Review, v. 4, n. 5, p. 193-220, dec. 1890.
[226] Idem, p. 195.
[227] Exemplificativamente, um evento marcante na história estadunidense foram os debates e polêmicas em torno da proposta fracassada, feita em 1965, de um *National Data Center*, destinado a concentrar dados estatísticos da população de forma centralizada (DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006. p. 294). No cenário europeu, por sua vez, diversas leis voltadas ao tema foram gradativamente sendo promulgadas a partir da década de 70, começando com os *Länder* de Hesse e da Bavária (1970) e seguida pelo Reino da Suécia (1973), a República Federal da Alemanha (1977) e a República da França (1978) (DONEDA, op. cit., p. 228).
[228] Em virtude da dificuldade imposta pela distância cultural e barreiras linguísticas, o presente trabalho não possui quaisquer condições de traçar considerações a respeito da regulação da arquitetura de tecnologias de informação e comunicação e proteção da privacidade em países do continente asiático ou africano.
[229] Para uma análise comparativa dos modelos europeu e estadunidense de proteção de dados pessoais, vide: DONEDA, op. cit., p. 221- 306.
[230] EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 5/2018:** Preliminary Opinion on Privacy by Design. Brussels: EDPS, 2018. p. 4.
[231] Esta inclusive foi a posição de Warren e Brandeis em sua exposição inaugural sobre a matéria (Idem, p. 219).
[232] BARLET, Robert. Developments in the Law: The Law of Cyberspace. **Harvard Law Review**, v. 112, p. 1574-1704, 1999. p. 1634. RICHARDS, Neil M.; SOLOVE, Daniel J. Prosser's Privacy Law: A Mixed Legacy. **California Law Review,** v. 98, p. 1887-1924, 2010. p. 1922
[233] Embora não tenha sido o primeiro navegador para internet a ser desenvolvido, a versão 1.0 do Mosaic foi a primeira a disponibilizar a funcionalidade de apresentar texto e imagem numa só tela. Além disso, o navegador

internet era utilizada praticamente apenas por uma pequena comunidade de pesquisadores ligados a universidades e servidores públicos de órgãos governamentais ligados a setores de defesa nacional, exploração aeroespacial e inteligência. Assim, seus usuários possuíam predominantemente formação em áreas técnicas, tais como ciência da computação, física, matemática e engenharia elétrica. Estes diversos fatores (utilização científica ou governamental, número reduzido de usuários e usuários com formação acadêmica elevada) tornavam significativamente menores e mais administráveis os riscos de exposição ou vazamento indevido de dados.

Contudo, o avanço sensível da utilização de tecnologias de informação e comunicação em razão da expansão mundial da internet a partir do início da década de 90 passou a exigir uma releitura do assunto. Por certo, o aumento exponencial do uso por um número elevado de indivíduos sem qualificação técnica e para fins diversos, em especial o uso comercial e recreativo, ampliou de forma relevante a probabilidade de incidentes de segurança e vazamentos de dados capazes de gerar danos até então desconhecidos. Igualmente, não só indivíduos passaram a usar cotidianamente a rede mundial de computadores, como também as empresas identificaram sua utilidade tanto como ferramenta e objeto de negócios[234].

Nesse cenário de expansão do uso comercial e recreativo da internet, diversos estudos passaram a indicar que, tanto sob a ótica da proteção da segurança de dados[235], quanto sobre a ótica de proteção da privacidade de dados[236], incidentes de vazamento ou comprometimento de informações pessoais possuem significativos impactos econômicos. Definitivamente, a incerteza e insegurança quanto à adequada coleta e tratamento de dados pessoais prejudica a confiança dos indivíduos nas novas tecnologias de informação e comunicação, reduzindo sua adoção e disseminação[237]. Por consequência, este abalo na confiança também afeta os esforços

---

possuía versões disponíveis para Windows e Mac, cujo download podia ser feito gratuitamente. Esses fatores possibilitaram sua rápida expansão pelos domicílios de usuários com acesso à rede mundial de computadores (CALORE, Michael. April 22, 1993: Mosaic Browser Lights Up Web With Color and Creativity. **Wired**, 22 apri. 2010. Não paginado).

[234] Ilustrativamente, as primeiras duas companhias a atingir, em 2018, a histórica marca de U$1trilhão em valor de mercado (DAVIES, Rob; RUSHE, Dominic. Amazon becomes world's second company to be valued at $1tn. **The Guardian**, 4 set. 2018. Não paginado).

[235] CAMPBELL, Katherine et alli. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. **Journal of Computer Security.** v. 11, n. 3, p. 431-448, mar. 2003. p. 444-446. CAVUSOGLU, Huseyin; MISHRA, Birendra; RAGHUNATHAN, Srinivasan. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. **International Journal of Electronic Commerce**, v. 9, n. 1, p. 69-104, 2004. p. 97.

[236] ACQUISTI, Alessandro; FRIEDMAN, Allan; TELANG, Rahul. Is There a Cost to Privacy Breaches? An Event Study. **Proceedings of the 27th International Conference on Information Systems**. December 2006. p.18.

[237] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Digital Economy Outlook 2017.** Paris: OECD, 2017. p. 250.

de digitalização de serviços públicos e privados, impactando iniciativas voltadas a tornar mais eficientes diversos setores da economia e, assim, reduzindo o efeito esperado de melhoria na qualidade de vida dos indivíduos.

Nesse contexto, passou-se cada vez mais a considerar que a utilização exclusiva de institutos jurídicos clássicos seria insuficiente para a adequada garantia das informações pessoais de indivíduos [238]. De fato, com a consolidação cada vez maior das camadas estruturais[239] do setor de tecnologia de informação e comunicação por grandes corporações e suas plataformas, existiriam menos incentivos por parte desses agentes para desenvolver sistemas e arquiteturas de códigos que respeitem os direitos de seus usuários[240]. Além disso, os próprios programadores e engenheiros destas tecnologias, por não possuírem formação ou treinamento na área, estariam mais propensos a ignorar estes requisitos quando da concepção de um sistema[241].

Deste modo, a partir da contribuição de estudos de outras ciências, pesquisadores e agentes reguladores passaram a defender e propor a utilização de técnicas diferentes de regulação, as quais, ao serem combinadas [242] com os institutos jurídicos clássicos, como proibição e sanção, permitiriam o desenvolvimento de um cenário mais propício à proteção da privacidade frente a ameaças tecnológicas. Estas medidas, destinadas a incidir durante todo o ciclo de vida de um sistema eletrônico, indo o processo de desenvolvimento ou concepção até a seu efetivo funcionamento, serão estudadas nesta seção. Deste modo, esta etapa deste trabalho será dividida em três subsubseções, cuja estrutura pretende apresentar o leitor não familiarizado ao instituto do *privacy by design*. Assim, a subseção **3.1** examinará a origem e desenvolvimento inicial da matéria, de modo a possibilitar uma melhor contextualização do assunto. Por sua vez, a subseção **3.2** apresentará uma análise da evolução normativa do instituto, buscando identificar

---

[238] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Digital Security Risk Management for Economic and Social Prosperity.** Paris: OECD, 2015. p. 25. ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** Paris: OECD, 2013. p. 117. UNITED NATIONS. Human Rights Council. **Report of the United Nations High Commissioner for Human Rights:** The Right to Privacy in the Digital Age. New York: United Nations, 2018. p. 4-7.

[239] O conceito de "camadas" é utilizado para descrever cada parte da estrutura necessária para o funcionamento de tecnologias de informação e comunicação e seus diferentes papeis e características. Embora a quantidade varie de acordo com ótica analisada, geralmente se diz que a internet é composta de seis camadas: a) conteúdo; b) aplicação; c) transporte; d) internet; e) ligação; f) física (SOLUM, Lawrence; CHUNG, Minn. The Layers Principle: Internet Architecture and the Law. **University of San Diego School of Law Research Paper**, n. 55, p. 1-114, jun. 2003. p. 3. YOO, Christopher S. Protocol Layering and Internet Policy. **University of Pennsylvania Law Review,** v. 161, n. 6, p. 1707-1771, 2013. p. 1742-1747).

[240] HUNT, Reed. The Future of the Net – Comments on Lawrence Lessig's Code and Other Laws of Cyberspace and The Future of Ideas. **Brooklyn Law Review**, v. 68, n. 1, p. 289-308. 2002. p. 299.

[241] WALDMAN, Ari Erza. Designing Without Privacy. **Houston Law Review,** v. 55, p. 659-727, 2018. p. 726.

[242] SCHWARTZ, op. cit., 2000. p. 781.

as primeiras normas a preverem a implementação de medidas tecnológicas e organizacionais voltadas à proteção da privacidade, com particular atenção para o diálogo entre as experiências estadunidense e europeias. Por fim, a subseção **3.3** estudará a operacionalização do *privacy by design*, em particular a seu funcionamento sob uma perspectiva técnica e organizacional e os mecanismos institucionais com os quais interage para assegurar a sua eficácia.

3.1 DA ORIGEM E DESENVOLVIMENTO INICIAL DO *PRIVACY BY DESIGN* NA DOUTRINA

Muito embora seja verdadeiro afirmar que o *privacy by design* tenha passado a receber um nível de atenção consideravelmente maior após a formulação e entrada em vigor, em 25 de maio de 2018, do *General Data Protection Regulation* pela União Europeia, o instituto não é recente, nem tampouco uma criação original deste bloco de países. Já na década de 80, anos antes de a proposta ser apresentada com esta nomenclatura, cientistas da computação, preocupados com o fato de que a disseminação de computadores poderia acarretar profundos impactos aos direitos fundamentais e à democracia, já defendiam a construção de modelos tecnológicos para a proteção da privacidade[243]. De fato, estes pesquisadores entendiam que não se poderia esperar de governos e organizações para a defesa da privacidade, considerando necessário que a própria comunidade técnica tomasse medidas a respeito, escrevendo códigos que implementassem, por exemplo, criptografia forte, comunicações anônimas e assinaturas digitais[244]. Nesta época, o crescente ceticismo que se disseminava pela comunidade técnica pode ser bem ilustrado o *"Cypherpunk's Manifesto*", escrito em 1993 pelo matemático, criptógrafo e programador Eric Hughes. Nele, o autor amalgamou alguns dos pensamentos correntes nas listas de e-mails anônimos da época[245], asseverando que "*Privacy is necessary for*

[243] Realmente, a preocupação com o tema inclusive motivou a *Internet Activities Board* a dedicar a RFC 1087 exclusivamente para o tema "Ética e a Internet". Nela, a IAB afirmou seu posicionamento de defesa ao uso responsável dos recursos da internet, refutando qualquer uso que, dentre outros aspectos, prejudicasse a privacidade dos usuários (INTERNET ACTIVITIES BOARD. **Request for Comments 1087:** Ethics and the Internet. [s.l.]: Internet Activities Board, 1989. p. 2).

[244] HUGHES, Eric. **A Cypherpunk's Manifesto.** [s.l.: s.n.], 1993. Não paginado.

[245] Listas de e-mails anônimos eram um meio popular de comunicação utilizado na década de 90 por meio dos quais os correspondentes trocavam mensagens coletivamente removendo ou encriptando elementos tecnológicos que permitiam identificar a sua autoria.

an open society in the electronic age. […] We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it"[246].

Assim, gradativamente o estudo sobre a temática acarretou o surgimento de metodologias de desenvolvimento de tecnologias de informação e comunicação que buscavam introduzir a proteção à privacidade enquanto requisito destes sistemas[247]. Neste contexto, em 1995 um relatório conjunto produzido pelo *Registratiekamer*, autoridade holandesa de proteção de dados, e pelo *Information and Privacy Commissioner*, autoridade de proteção de dados da província canadense de Ontário, identificou que apesar de requisitos de proteção da *segurança* da informação serem conhecido entre agentes públicos e privados, requisitos de proteção da *privacidade* da informação não eram[248]. Assim, estas autoridades delinearam e defenderam o conceito de *Privacy-Enhancing Technology*[249], que se referiria a uma "variedade de tecnologias que salvaguardam a privacidade ao minimizar ou eliminar a coleta de dados identificáveis"[250]. Para estes órgãos públicos, o mais importante requisito para o desenvolvimento de tecnologias em prol da privacidade seria questionar, desde do início, se informações identificáveis seriam realmente necessárias para o funcionamento do sistema[251].

Aos poucos, este termo foi recebendo maior atenção, sendo a sua definição aprimorada para conter também elementos de relacionados à necessidade e consentimento no tratamento dos dados pessoais. Nesse sentido, Van Blarkorm, Borking e Verhaar definem *Privacy-Enhancing Technology* como[252]:

---

[246] HUGUES, op. cit., 1993. Não paginado. Original em inglês. Tradução livre: "Privacidade é necessária para uma sociedade livre na era eletrônica. [...] Nós sabemos que alguém precisa escrever softwares para defender a privacidade e, já que não podemos ter privacidade semque todos tenham, nós iremos escrevê-los.".

[247] CHAUM, David. Security Without Identification: Transactions Systems to Make Big Brother Obsolete. **Communications of the ACM**, v. 28, n. 10, p. 1030-1044, oct. 1985. p. 1030. CHAUM, David. Achieving Electronic Privacy. **Scientific American,** p. 96-101, ago. 1996. p. 96.

[248] INFORMATION AND PRIVACY COMMISSIONER; REGISTRATIEKAMER. **Privacy-Enhancing Technologies:** the path to anonymity. Toronto, The Hague: Information and Privacy Commissioner; Registratiekamer, 1995. p. 13.

[249] Numa tradução livre, o termo pode ser traduzido como "tecnologias para fortalecimento/aprimoramento da privacidade".

[250] Tradução livre. No original: "variety of technologies that safeguard personal privacy by minimizing or eliminating the collection of identifiable data" (Idem, p. 4).

[251] Idem, p. 8.

[252] Tradução livre. No original: "Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system." (VAN BLARKORM, G.W.; BORKING, J.J.; VERHAAR, P. Privacy Enhancing Technologies. In.: HUIZENGA, J. (coord.). **Handbook of Privacy and Privacy-Enhancing Technologies:** the case of Intelligent Software Agents. The Hague: PISA Consortium, 2003. p. 33).

> […] um sistema de medidas de tecnologia de informação e comunicação que protegem a privacidade informacional ao eliminar ou minimizar dados pessoais, prevenindo o processamento desnecessário ou indesejado de dados pessoais, sem perder a funcionalidade do sistema de informação.

Todavia, muito embora o desenvolvimento de medidas tecnológicas para a proteção da de dados pessoais fosse uma etapa importante e necessária para evitar danos ao direito à privacidade dos indivíduos, as *Privacy-Enhancing Technologies* se apresentavam insuficientes ou incapazes de atender plenamente o problema. De fato, ainda que diversas iniciativas, algumas inclusive propondo o estabelecimento de padrões universais[253], tenham surgido com este foco, elas também eram objeto de inúmeras críticas por parte de estudiosos.

Nesta senda, autores apontavam para o fato de que estas iniciativas ainda eram muito dependentes de uma postura proativa por parte das empresas de tecnologia. Todavia, ocorre que mercados informacionais, especialmente aqueles baseados na internet, são altamente propensos a sofrer "efeitos econômicos de rede"[254]. De forma sintética, este fenômeno ocorre quando determinados produtos ou serviços, embora possuam nenhum ou pouco valor isoladamente, adquirem e geram valor quando agregados ou combinados com outros[255]. Em determinados casos, o ponto de equilíbrio destes mercados não necessariamente será socialmente eficiente, pois, dentre outros motivos[256]: a) a economia de escala e a diferenciação de produto tendem a concentrar estes mercados; b) a tendência à concentração tende a ser reforçada pelos custos de produção em razão de investimentos em pesquisa e desenvolvimento; c) as externalidades acarretadas por produtos e serviços destes mercados nem sempre são internalizáveis.

---

[253] Um exemplo de iniciativa neste sentido foi o *Protocol for Privacy Preferences Project* (P3P), desenvolvido pela *World Wide Web Consortium*, cuja proposta era estabelecer um padrão universal para que sítios eletrônicos e *softwares* de navegação na internet fossem capazes de reconhecer automaticamente as preferências de privacidade de seus usuários, os quais, a partir desta informação, evitariam coletar as informações cujos usuários não desejassem (WORLD WIDE WEB CONSORTIUM. **Protocol for Privacy Preferences:** an introduction. [s.l.]: W3C, 2000. Não paginado).

[254] FROOMKIM, Michael A. "PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology. **Ohio State Law Journal**, v. 74, n. 6, p. 965-994, 2013. p. 971.

[255] Michael Katz e Carl Shapiro descrevem este fenômeno como ocorrendo quando "[...] the utility that a given user derives from the good depends upon the number of other users who are in the same 'network' as is he or she" (KATZ, Michael L.; SHAPIRO, Carl. Network Externalities, Competition, and Compatibility. **The American Economic Review**, v. 75, n. 3, p. 424-440. jun. 1985. p. 424).

[256] KATZ, Michael L.; SHAPIRO. Systems Competition and Network Effects. **The Journal of Economic Perspectives.** v. 8, n. 2, p. 93-115, 1994. p. 112.

Em reforço a estes aspectos, a existência de grandes agentes econômicos cujas plataformas atuam como intermediárias[257] entre consumidores e fornecedores em ambientes eletrônicos também restringe a disseminação de tecnologias que protejam a privacidade de indivíduos. Como os agentes que disponibilizam estas plataformas utilizam os dados pessoais de seus usuários simultaneamente como insumo e mercadoria[258], eles acabam por possuir significativos incentivos econômicos para restringir ou impedir o sucesso de produtos e serviços cujos modelos de negócios prejudiquem diretamente os seus próprios modelos[259]. Desta maneira, pode não ser uma alternativa viável esperar que a livre concorrência seja capaz de resolver desta falha de mercado, porquanto a probabilidade de surgimento de competição por novos agentes que protejam a privacidade de dos usuários de seus produtos e serviços é restrita[260].

Além destes aspectos, estudiosos também sinalizavam para a circunstância de que agentes envolvidos com tecnologia de informação e comunicação frequentemente se ressentem do considerável desconhecimento por parte de agentes públicos reguladores acerca de particularidades do funcionamento do seu setor. Por certo, ao contrário de outros insumos existentes em setores da economia mais antigos, a informação é altamente fluída e pouco dependente de barreiras geográficas. Assim, tanto a sua produção quanto o seu consumo podem ocorrer em várias jurisdições simultaneamente, dificultando que iniciativas de regulação por parte de agentes estatais utilizem soluções jurídicas clássicas, a exemplo da proibição e sanção negativa, para incentivar o desenvolvimento de *Privacy Enhancing Technologies*. Além disso, era relativamente comum que legislações mais antigas de outros setores – e mais conhecidas e aplicadas pelos agentes reguladores – entrassem em conflito iniciativas destinadas a restringir

---

[257] Frequentemente, essas plataformas operam como mercados bilaterais ou multilaterais. De acordo com Jean-Charles Rochet e Jean Tirole, esses mercados são caracterizados quando plataformas possuem como modelo de negócios construir uma estrutura que possibilite interações entre agentes de segmentos distintos. Quanto maiores forem a participação e interação entre os agentes essas plataformas conseguirem promover, maiores serão os benefícios por elas obtidos (ROCHET, Jean Charles; TIROLE, Jean. Two-Sided Markets: a progress report. **The RAND Journal of Economics**, v. 37, n. 3, p. 645-667, 2006. p. 645-646). Essa espécie de mercado pode representar um desafio regulatório em razão da difícil aplicação de conceitos clássicos de direito concorrencial frente aos efeitos econômicos de rede gerados pelas plataformas (LEMLEY, Mark A.; MCGOWAN, David. Legal Implications of Network Economic Effects. **California Law Review**, v. 86, n. 3, p. 481-611, 1998. p. 497).

[258] SHELANSKI, Howard A. Information, Innovation, and Competition Policy for the Internet. **University of Pennsylvania Law Review**, v. 161, n. 6, p. 1663-1705, 2013. p.1678-1679. Para uma análise a respeito da propriedade de dados em mercados de plataforma, vide: WEBER, Rolf H. Data Ownership in Plataform Markets. In.: BELLI, Luca; ZINGALES, Nicolo (ed.). **Platform Regulations:** How Platforms are Regulated and How they Regulate Us. Rio de Janeiro: Fundação Getúlio Vargas, 2017.

[259] Ilustrativamente, estudo encomendado em 2017 pela Comissão Europeia, apontava que em 2015 as fatias de mercado da Play Store, da Google, e a Apple Store, da Apple, corresponderiam, respectivamente a 68,1% e 21% do mercado (DUCH-BROWN, Néstor. **The Competitive Landscape of Online Platforms.** Brussels: European Commission, 2017. p. 14).

[260] FROOMKIM, op. cit., 2013. p. 971.

o consumo de dados pessoais[261], tornando difícil um cenário de desenvolvimento de tecnologias voltadas à proteção da privacidade.

Em síntese, pelos motivos indicados acima, a "tradução" de conceitos legais relativos à proteção da privacidade em requisitos de sistemas eletrônicos não logrou produzir resultados significativos[262]. Realmente, a necessidade de uma abordagem multidisciplinar quanto ao tema passou paulatinamente a ser considerada um elemento crucial para o sucesso de iniciativas tecnológicas de proteção de dados pessoais na medida em que passou a ser identificada a existência de conceitos oriundos tanto da ciência da computação quanto da ciência jurídica importantes para este assunto[263].

Nesse contexto, buscando promover a temática, Ann Cavoukian, então Comissária do *Information and Privacy Commissioner* da província canadense de Ontário entre 1997 a 2014, postulou que mais do que simplesmente estabelecer requisitos técnicos para o desenvolvimento de tecnologias de informação e comunicação, a proteção da privacidade está intimamente ligada ao *processo* de desenvolvimento e posterior gestão e não apenas ao *produto* desenvolvido em si[264]. Para ela, essa abordagem era necessária em razão de ser improvável o estabelecimento uma solução técnica universal para a proteção da privacidade porquanto isto seria extremamente dependente do tipo de produto, da espécie de informação e das características do setor econômico onde a empresa opera as suas atividades[265]. Assim, a autora propôs uma metodologia que chamou de *Privacy by Design*, a qual consistiria num processo dotado de uma ótica holística para a proteção das informações pessoais dos indivíduos, desde o planejamento, desenvolvimento e produção do produto ou serviço até às práticas de negócios[266].

Entretanto, ao invés de apresentar um conceito delineado, Cavoukian referiu que o *Privacy by Design* seria composto por sete "princípios fundantes", os quais deveriam ser observados por qualquer iniciativa voltada à proteção da privacidade de indivíduos. De acordo

---

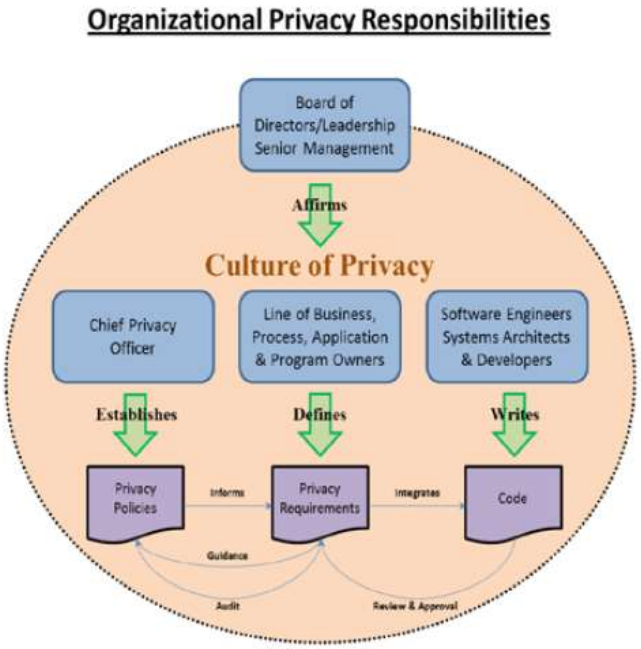
[261] FROOMKIM, op. cit., 2013, p. 971-972. Exemplificativamente, o autor refere normas que exigiriam a utilização de medidas tecnologias para coletas de dados sobre operações financeiras de indivíduos com a finalidade de utilização posterior em questões relativas ao combate à corrupção, lavagem de dinheiro, entre outros (Idem).
[262] EUROPEAN DATA PROTECTION SUPERVISOR, op. cit., 2018. p. 3.
[263] TSORMPATZOUDI, Pagona; BERENDT, Bettina; COUDERT, Fanny. Privacy by Design: Research and Policy to Practice – the Challenge of Multi-disciplinarity. In.: BERENDT, Bettina *et alli* (Eds.). **Privacy Technologies and Policy.** Luxembourg: Springer, 2015. p. 200.
[264] CAVOUKIAN, Ann. **Operationalizing Privacy by Design:** a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. p. 2.
[265] Idem, p. 2.
[266] Idem, p. 8.

com ela, os princípios a serem seguidos seriam[267]: a) proatividade e prevenção; b) privacidade enquanto configuração padrão; c) privacidade imbuída no *design*; d) funcionalidade completa; e) segurança de ponta-a-ponta; f) visibilidade e transparência; g) respeito pela privacidade do usuário.

De fato, conforme se verifica a partir de uma leitura da proposta, para além de aspectos tecnológicos, Cavoukian buscou, por intermédio da defesa do *Privacy by Design*, incentivar e fomentar o desenvolvimento de uma cultura institucional de responsabilidade dos atores envolvidos[268]. Em sua opinião, isso seria necessário porque um dos principais aspectos para o sucesso na proteção da privacidade não seria apenas o desenvolvimento de códigos, mas sim o estabelecimento de uma política interna clara e definida, capaz de esclarecer o papel de cada agente na promoção e proteção dos dados pessoais de indivíduos coletados e/ou tratados pela entidade. Desta maneira, por meio de sua posição como *Information and Privacy Commissioner*, a autora estimulou o desenvolvimento de um ecossistema empresarial que reconhecesse a importância da proteção da privacidade como um valor e objetivo de negócio. Em resumo, propôs a afirmação de uma cultura favorável à privacidade onde todos os agentes desenvolvessem uma ação coordenada, conforme ilustrado no diagrama abaixo.

Figura 2 - Estrutura institucional do *privacy by design*

[267] CAVOUKIAN, op. cit., 2012. p. 8. Neste momento a análise se limitará a apresentar a lista. Os princípios serão abordados com maior atenção no subcapítulo **3.3**, a seguir.
[268] Idem, p. 10.



Fonte: CAVOUKIAN, op. cit., 2012.

Com efeito, além do estabelecimento de responsabilidades claras, a proposta de Cavoukian para a proteção da privacidade de indivíduos também procurou abordar os problemas vinculados aos vieses dos agentes envolvidos no desenvolvimento de tecnologias de informação e comunicação. Desde a década de 90 pesquisadores como Batya Fridman e Helen Nissenbaum já identificavam que as preconcepções das pessoas e da sociedade representavam uma variável importante no resultado do processo de produção de softwares[269]. Notadamente sob a perspectiva dos usuários, estes autores verificavam que a predominância de certos vieses na indústria tecnológica poderia ampliar ou reduzir drasticamente a liberdade dos indivíduos na utilização de funcionalidades dos sistemas[270]. Deste modo, defendiam como imperiosa a necessidade de identificar esses possíveis vieses aos quais a produção de tecnologias poderia estar exposta para que se tornasse viável atenuar ou eliminar aqueles que resultassem em efeitos socialmente negativos ou indesejados[271].

[269] FRIEDMAN, Batya; NISSENBAUM, Helen. Discerning Bias in Computer Systems. **93 Conference Companion on Human Factors in Computing Systems.** p. 141-142, apr. 1993. p. 142. FRIEDMAN, Batya; NISSENBAUM, Helen. Bias in Computer Systems. **ACM Transactions on Information Systems**. v. 14, n. 3, p. 330-347, jul. 1996. p. 345.
[270] NISSENBAUM, Helen. Values in the Design of Computer Systems. **Computers and Society**. p. 38-39, mar. 1998. p. 38.
[271] FRIEDMAN; NISSENBAUM, op. cit., 1996. p. 342-345.

Muito embora a proteção da privacidade seja reconhecida como um valor prezado pela sociedade em geral, sua definição concreta é extremamente suscetível ao contexto no qual a informação e o indivíduo a que ela se refere estão inseridos[272]. De fato, a complexidade e a dificuldade de modelar tecnologicamente conceitos cujos significados dependem do contexto são frequentemente apontadas como fatores tendentes a inviabilizar soluções voltadas a atender às necessidades da privacidade da população em geral[273]. Não obstante, ao propugnar que medidas voltadas a implementar uma política de *Privacy by Design* sejam sempre pensadas de acordo com o caso concreto, Cavoukian tentou fugir de soluções padronizadas, as quais estariam fadadas ao fracasso por não levar em conta a realidade e conjuntura informacional envolvidas.

De toda maneira, longe de ter aparecido como uma proposta regulatória pronta e acabada, o *privacy by design* é fruto de um longo processo de evolução normativa, fruto do diálogo constante entre agentes reguladores de jurisdições ocidentais, particularmente os EUA, a União Europeia e fóruns internacionais compostos por estadunidenses e europeus. Nesse sentido, por reputarmos que o conhecimento quanto a este processo de desenvolvimento normativo é fundamento para a adequada compreensão do instituto, a seção **3.2** a seguir buscará precisamente abordar esta temática.

3.2 DA EVOLUÇÃO NORMATIVA DA PROTEÇÃO À PRIVACIDADE E A CONSTRUÇÃO DO *PRIVACY BY DESIGN* NA LEGISLAÇÃO

Em 26 de janeiro de 1999, diante de um auditório lotado, Scott McNeally afirmou que a noção de privacidade estaria "superada", sendo necessário que as pessoas se acostumassem a este novo paradigma[274]. Na ocasião, a fala do então *Chief Executive Officer* (CEO) da *Sun Microsystems*, uma das maiores empresas de *hardware* e *software* do mundo, atraiu a atenção da mídia especializada e acarretou diversas críticas de variados setores da sociedade. Anos mais tarde, em 10 de janeiro de 2010, Mark Zuckerberg, criador e CEO do *Facebook*, repetiu

[272] NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus**, v. 140, n. 4, p. 32-48, 2011. p. 45. NISSEMBAUM, Helen. Respecting Context to Protect Privacy: Why Meaning Matters. **Science and Engineering Ethics**, v. 24, n. 3, p. 831-852, 2015. p. 20.

[273] PAGALLO, Ugo. On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In.: GURVITS, S. et alli (eds.). **European Data Protection:** in good health?. Amsterdam: Springer, 2012. p. 343.

[274] Em inglês, sua fala foi "You have zero privacy anyway.[…] Get over it." (MCNEALLY, Scott. apud SPRENGER, Polly. Sun on Privacy: 'Get Over it". **Wired**, 26 jan. 1999. Não paginado).

assertiva semelhante, defendendo que a privacidade "não seria mais uma norma social"[275] e que isto justificaria modelos de negócio baseados em explorar dados e informações pessoais. Novamente, diversos agentes criticaram a fala do executivo, a qual ocorria próxima a um contexto de reação pública contra as políticas da empresa em relação ao tratamento de dados pessoais de seus usuários[276].

Entretanto, a despeito das falas de representantes de grandes empresas de tecnologia indicar um baixo zelo à proteção da privacidade de indivíduos por parte destes atores, essa não é a realidade na seara regulatória. De fato, desde meados da década de 60 o cenário regulatório envolvendo o fluxo e tratamento de dados tem recebido constante atenção por parte de entes públicos e privados com a finalidade de estabelecer um ecossistema normativo estável e uniforme[277]. Nesse contexto, a proteção aos dados pessoais mediante a utilização de mecanismos voltados a influenciar a arquitetura de sistemas de informação e comunicação paulatinamente foi avançando e recebendo contornos mais definidos conforme se verificava o amadurecimento nas discussões e o aumento do tamanho do mercado[278].

Apesar deste trabalho, em sua seção **2**, ter analisado primariamente a doutrina estadunidense quanto ao tema da regulação de tecnologias de informação e comunicação, a seção **3** adotará recorte mais abrangente, porquanto será necessário incluir também a análise da evolução normativa da União Europeia quanto à proteção de dados pessoais. Com efeito, dentre as razões que podem ser elencadas para isso está o fato de que, embora possuam tradições jurídicas diferentes, existe um diálogo constante entre os países europeus e os Estados Unidos da América quanto à matéria em razão do intenso intercâmbio de dados entre si. Nessa senda, apesar de os estadunidenses, até o presente momento[279], terem adotado uma postura regulatória

---

[275] JOHNSON, Bobbie. Privacy is no Longer a Social Norm, Says Facebook Founder. **The Guardian**, 11 jan. 2010. Não paginado.

[276] BANKSTON, Kevin. Facebook's New Privacy Changes: The Good, The Bad and The Ugly. **Electronic Frontier Foundation**, 9 dec. 2009. Não paginado.

[277] Em 1969, em meio ao debate sobre a criação do *National Data Center*, Arthur Miller já se preocupava com os possíveis efeitos que a proliferação de computadores acarretaria à privacidade cotidiana, em especial no que se referia à perda do controle, pelos indivíduos, de suas informações pessoais (MILLER, Arthur R. Personal Privacy in the Computer Age: The Challenge of a New Technology. **Michigan Law Review,** v. 67, n. 6, p. 1089-1246, apr. 1969. p. 1107).

[278] Conforme se explicará mais adiante, um dos motivos para a edição do *General Data Protection Regulation* pela União Europeia foi justamente a necessidade de integrar a comunidade de países tendo em vista a criação de um "mercado digital comum" (EUROPEAN COMMISSION. Commission outlines next steps towards a European data economy. **European Commission**, 10 jan. 2017. Não paginado).

[279] Embora de forma geral a regulação federal estadunidense seja setorial, diversos eventos em 2018 fortaleceram movimentos, inclusive por parte de empresas de tecnologia, pela edição de uma legislação nacional sobre o tema (ZAKRZEWSKI, Cat; HAWKINS, Derek. Tech Executives Voice Support for National Privacy Law. **The Washington Post**, 26 set. 2018. Não paginado. KANG, Cecilia. Tech Industry Pursues a Federal Privacy Law, on Its Own Terms. **The New York Times,** 26 ago. 2018. Não paginado).

em prol de normas setoriais[280], estudiosos dos dois lados do Atlântico se dedicam a estudar constantemente os avanços normativos presenciados em cada continente[281]. Em especial, é possível notar com certa frequência entre estudiosos estadunidenses opiniões que, embora critiquem a complexidade dos diplomas europeus, vejam de modo favorável o tratamento consideravelmente mais uniforme da matéria no velho continente[282].

Com efeito, o primeiro evento relevante no que tange à evolução normativa do instituto do *privacy by design* pode ser considerado como sendo a edição, em 1973, do *Code of Fair Information Practices* [283] pelo *Health, Education and Welfare Advisory Committee on Automated Data Systems*[284]. Na ocasião, este comitê vinculado ao Poder Executivo federal dos EUA, formado por diversos especialistas do setor público e privado e presidido por Willis Ware[285], produziu um extenso relatório sobre os possíveis impactos da disseminação do tratamento automatizado de informações sobre indivíduos. Ao final, o documento apresentou uma série de recomendações fundamentadas em cinco princípios considerados essenciais para o tratamento de dados pessoais, a saber[286]:

> ***a)*** *There must be no personal data-recording systems whose very existence is secret;* ***b)*** *There must be a way for an individual to find out what information about him is in a record and* ***how it is used****;* ***c)*** *There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent;* ***d)*** *There must be a way for a person to correct or amend a record of identifiable information about the*

[280] DONEDA, op. cit., 2006, p. 305-306. BELING, Graig T. Transborder Data Flows: International Privacy Protection and the Free Flow of Information. **Boston College International and Comparative Law Review**, v. 6, n. 2, p. 591-624, 1983.

[281] GELLMAN, Robert M. Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions. **Software Law Journal,** v. 6, n. 2, p. 199-238, 1993. p. 201. REIDENBERG, Joel. Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? **Federal Communications Law Journal**, v. 44, n. 2, p. 196-243, 1992. p. 238-242. RUSTAD, Michael L; KOENIG, Thomas H. Towards a Global Data Privacy Standard. **Suffolk University Legal Studies Research Paper Series,** n. 18, p. 1-89, set. 2018. p. 87-88. GREENLEAF, Graham. The Influence of European data privacy standards outside Europe: implications for globalization of Convention 108. **International Data Privacy Law**, v. 2, n. 2, p. 68-92, 2012. p. 91-92.

[282] REIDENBERG, op. cit., 1992, p. 241-242. Em sentido contrário: BELING, op. cit., 1983, p. 623-624.

[283] Original em inglês. Tradução livre: "Código de Boas Práticas em Informação".

[284] Original em inglês. Tradução livre: "Comitê Consultivo [do Departamento] de Saúde, Educação e Bem-Estar sobre o Sistemas de Dados Automatizados".

[285] Willis Ware foi um engenheiro elétrico da *RAND Corporation* responsável por diversos avanços pioneiros no campo de segurança computacional e privacidade de informações pessoais. Suas propostas para a proteção de dados pessoais quanto ao tratamento automatizado de informações influenciaram profundamente o *Privacy Act*, de 1974 e, posteriormente, as iniciativas da OECD e do Conselho da Europa (MARKOFF, John. Willis Ware, 93, Engineer at Dawn of Computer Age, Dies. **The New York Times**, 01 dez. 2013. Não paginado. GELLMAN, Robert. Willis Ware's Lasting Contribution to Privacy: Fair Information Principles. **IEEE Security & Privacy,** v. 12, n. 4, p. 51-54, 2014. p. 53-54).

[286] UNITED STATES OF AMERICA. Department of Health, Education and Welfare. **Records, Computers, and the Rights of Citizens.** Washington: DHEW, 1973. p. xx-xxi.

> *person;* ***e) Any organization*** *creating, maintaining, using, or disseminating records of identifiable personal data* ***must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data***[287]. (grifou-se)

Como se pode verificar, a preocupação do comitê estava diretamente vinculada à necessidade de se estabelecer uma relação de confiança entre os indivíduos e as entidades que utilizam seus dados pessoais. Deste modo, a partir dos princípios listados procurou-se fixar alguns requisitos gerais para o tratamento de dados pessoais, sendo possível identificar que a arquitetura dos sistemas e o agente por ela responsável já eram considerados importantes, pois, dentre outros pontos, já se exigia a qualquer entidade que administrasse um sistema de tratamento automatizado de banco de dados[288]:

> *[...]Take affirmative action to inform* ***each of its employees having any responsibility or function*** *in the* ***design, development, operation, or maintenance*** *of the system, or the use of any data contained therein, about all the* ***safeguard requirements*** *and all the rules and procedures of the organization* ***designed to assure compliance*** *with them;* (grifou-se)

Muito embora fosse constituído principalmente de recomendações e não de regras cogentes em sentido estrito, o *Code of Fair Information Practices* representou um marco significativo no que se refere à proteção de dados pessoais e ao posterior desenvolvimento posterior do conceito de *Privacy by Design*, sendo sua adoção e incorporação defendida pela doutrina[289]. De fato, a preocupação que Willis Ware e seus colegas trouxeram com relação aos aspectos institucionais e tecnológicos do tratamento de informações de indivíduos influenciou outras iniciativas regulatórias voltadas a atender a este problema.

Ao mesmo tempo que a discussão sobre o tópico da proteção da privacidade avançava nos EUA, no cenário europeu também era possível identificar movimentações nesse mesmo

---

[287] Original em inglês. Tradução livre: "a) Não devem existir sistemas de coleta de dados pessoais cuja própria existência seja secreta; b) Deve existir uma maneira para que um indivíduo saiba qual informação a seu respeito está num registro e como está sendo utilizada; c) Deve existir uma maneira para um indivíduo prevenir que suas informações sejam utilizadas para propósitos distintos ou tornada disponível para outros propósitos sem o seu consentimento; d) Deve existir uma maneira para que um indivíduo possa corrigir ou aditar um registro de informação identificável sobre a sua pessoa; e) Qualquer organização que crie, mantenha, use ou dissemine registros de informações pessoais identificáveis deve assegurar a confiança destes dados para a sua utilização e prevenir a utilização indevida destes dados".

[288] Original em inglês. Tradução livre: "Tome medidas necessárias para informar cada um de seus empregados que tenham responsabilidade ou funções no desenho, desenvolvimento, operação ou manutenção do sistema ou, no uso de quaisquer dados nele armazenado, sobre todas as exigências de segurança e todas as regras e procedimentos da organização estipuladas para assegurar seu cumprimento." (UNITED STATES OF AMERICA, op. cit., 1973, p. xxiv).

[289] SCHWARTZ, op. cit., 2000, p. 787-788.

sentido. Preocupado com os impactos que o avanço tecnológico estava gerando na sociedade, o Comitê de Ministros do Conselho da Europa[290], organização internacional formada por 47 países europeus, determinou ao seu comitê de cooperação jurídica que estudasse a temática[291]. Como resultado desses estudos, o órgão consultivo apresentou duas propostas de resoluções acerca do tratamento de dados pessoais, sendo uma destinada ao setor público[292] e outra ao setor privado[293]. Em ambos os documentos, ainda que não houvesse menção expressa ao *privacy by design*, alguns de seus elementos estavam presentes, em especial a necessidade de estabelecimento de medidas organizacionais que incentivassem uma atuação responsável dos indivíduos envolvidos no tratamento de dados pessoais[294]. Assim, apesar de aspectos vinculados a medidas tecnológicas de proteção de dados não terem recebido atenção naquela ocasião, os princípios gerais ali definidos podem ser considerados como os primeiros passos de um processo contínuo de harmonização de normativa na Europa.

Por certo, a crescente discussão regulatória sobre a proteção de dados de indivíduos por iniciativa de vários de seus membros influenciou o processo de edição, pela própria Organização para Cooperação e Desenvolvimento Econômico, de importantes recomendações internacionais quanto ao tema do fluxo transfronteiriço de dados no período entre 1970 e 1980. Criada em 1948 por países europeus, Estados Unidos da América e Canadá, com a finalidade de auxiliar na execução do Plano Marshall, a OCDE promove diversas iniciativas voltadas a harmonizar o cenário regulatório de seus membros, de modo a permitir que o incremento no intercâmbio comercial promova seus objetivos institucionais. Assim, este organismo internacional representa um importante fórum de diálogo entre os atores estadunidenses e europeus no que tange à regulação voltada à proteção da privacidade. De fato, observando o aumento no fluxo de dados entre seus países membros, a entidade produziu e publicou uma série de diretrizes voltadas a estimular a redução de conflitos normativos entre jurisdições nacionais de seus países membros[295]. Deste modo, buscando influenciar um consenso entre seus

---

[290] Instituído em 1949 por meio do Tratado de Londres, o Conselho da Europa não faz parte da União Europeia, apesar de 27 de seus membros serem simultaneamente membros desta última.
[291] COUNCIL OF EUROPE. EUROPEAN COMMITTEE ON LEGAL CO-OPERATION. **Addendum I to the Report on the 19th meeting of the CCJ.** Strasboug: Council of Europe, 1973. p. 7.
[292] COUNCIL OF EUROPE. COMMITTEE OF MINISTERS. **Resolution (74) 29.** On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector. Strasbourg: Council of Europe, 1974.
[293] COUNCIL OF EUROPE. COMMITTEE OF MINISTERS. **Resolution (73) 22**. On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector. Strasbourg: Council of Europe, 1973.
[294] COUNCIL OF EUROPE. EUROPEAN COMMITTEE ON LEGAL CO-OPERATION, op. cit., p. 13.
[295] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Recommendation Of The Council Concerning Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data.** Paris: OECD, 1980. Não paginado.

membros, a OCDE tentou facilitar a exportação de dados entre os países da organização ao reduzir o potencial conflito de leis de jurisdições distintas[296].

Da mesma maneira que o *Code of Fair Information Practices* e que as resoluções editadas pelo Conselho da Europa, as diretrizes foram redigidas com a estrutura de princípios, facilitando a sua adesão e implementação pelos membros da OCDE. Em síntese, os oito princípios propostos pela entidade foram[297]: a) princípio da limitação da coleta; b) princípio da qualidade dos dados; c) princípio da especificação de propósito; d) princípio do uso limitado; e) princípio da segurança; f) princípio da transparência; g) princípio da participação individual; h) princípio da responsabilização do responsável. Igualmente relevante, as diretrizes também estabeleceram o fundamental conceito de "controlador de dados", o qual foi definido como sendo o agente com poder de decisão sobre a coleta, tratamento e uso dados, independentemente destas ações serem executadas por ele próprio ou por terceiros.

Um ano após a edição das diretrizes pela OCDE, o Conselho da Europa concluiu negociações e promulgou em 28 de janeiro de 1981 o texto da Convenção 108, referente à proteção de indivíduos quanto ao processamento automatizado de dados[298]. Fruto de um processo de amadurecimento e envolvendo intensa cooperação entre a própria OCDE e o Conselho da Europa, este diploma internacional significou, pela primeira vez, a criação de um texto efetivamente vinculante[299] e aberto à adoção não apenas por países europeus, mas por qualquer outro Estado interessado em proteger os dados pessoais dos indivíduos sob sua jurisdição[300]. Assim, além de disseminar um conjunto de determinações legais semelhantes àquelas das recomendações europeias promulgadas em 1973 e 1974 e as da OCDE, este instrumento internacional também estabeleceu mecanismos para assegurar melhor sua eficácia normativa, tais como a criação de um órgão específico para acompanhar sua implementação e mecanismos de cooperação entre os estados-parte.

---

[296] Idem. Não paginado.
[297] Idem. Não paginado.
[298] COUNCIL OF EUROPE. **Convention 108**: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg: Council of Europe, 1981.
[299] De acordo com o artigo 27 da Convenção de Viena sobre Direito dos Tratados: "A party may not invoke the provisions of its internal law as justification for its failure to perform a treaty […]. Original em Inglês. Tradução livre: "Uma parte não poderá invocar previsões de seu direito interno como justificativa para sua falha em executar um tratado" (UNITED NATIONS. **Viena Convention on the Law of Treaties.** Viena: United Nations, 1965. p. 11).
[300] COUNCIL OF EUROPE. **Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Data.** Strasbourg: Council of Europe, 1981. p. 16.

Com efeito, após a edição da Convenção 108, a discussão entre agentes reguladores sobre a necessidade de proteção de dados pessoais começou a se intensificar no âmbito da comunidade europeia. Deste modo, o observando que muitos de seus países membros já começavam a legislar internamente sobre o assunto, a União Europeia se preocupou com o fato de que o estabelecimento de requerimentos legais distintos poderia acabar por enfraquecer os direitos dos cidadãos do bloco tendo em vista que a proteção deficiente em um país poderia facilmente afetar os demais em virtude da característica facilidade do trânsito de dados[301]. Nesta senda, ao propor em 1990 o estabelecimento de uma diretiva, efetivamente adotada em 1995[302], a União Europeia induziu seus membros a legislar medidas concretas para salvaguardar a privacidade de seus cidadãos[303]. Procurou-se também com isso aprofundar o processo de integração econômica do bloco em direção ao fortalecimento de um mercado comum.

De fato, a Diretiva 46 representou um passo importante no estabelecimento de um marco normativo mais estruturado no que tange à proteção da privacidade: enquanto a Convenção 108 do Conselho da Europa continha 27 artigos, sendo apenas 20 deles referentes especificamente ao objeto do tratado, esta Diretiva da União Europeia continha 34 artigos, sendo 30 referentes ao seu objeto. Além disso, em razão da técnica legislativa utilizada pela União Europeia na edição de instrumentos jurídicos, o diploma continha também um preâmbulo contendo 72 parágrafos, os quais, muito embora não possuam efeito normativo imediato, têm como finalidade explicar a função das normas descritas no instrumento e servir de parâmetro interpretativo. Nesse sentido, apesar de a noção de *privacy by desing* não ser mencionada explicitamente no trecho normativo da Diretiva 46, o parágrafo 46 do preâmbulo deste diploma ilustra que já estava presente a preocupação acerca da necessidade de proteger os dados pessoais de indivíduos no momento do desenvolvimento do sistema eletrônico. O texto referido dizia que[304]:

---

[301] COMMISSION OF THE EUROPEAN COMMUNITIES. **Commission Declaration:** on the protection of individuals in relation to the processing of personal data in the Community and Information security. Brussels: European Community, 1990. p. 4.

[302] EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Directive 95/46/EC:** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Luxembourg, 1995. Não paginado.

[303] REIDENBERG, Joel R. The Privacy Obstacle Course: Hurding Barriers to Transnational Financial Services. **Fordham Law Review**, v. 60, n. 6, p. 137-177, 1992. p. 176.

[304] Original em inglês. Tradução livre: "a proteção dos direitos e liberdades dos titulares de dados com relação ao processamento de dados pessoais exigem que as medidas técnicas e organizacionais apropriadas sejam tomadas, tanto no momento do *design* do sistema eletrônico quanto no momento do próprio processamento, particularmente para manter a segurança e assim prevenir qualquer utilização não autorizada; cabe aos Estados Membros assegurar que controladores observem estas medidas; estas medidas devem assegurar um nível apropriado de segurança, levando em consideração o estado da arte e os custos de sua implementação com relação aos riscos inerentes no

> *[...] the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken,* ***both at the time of the design of the processing system and at the time of the processing itself****, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected; (grifou-se)*

Entretanto, apesar desta menção a "medidas técnicas e organizacionais" a serem tomadas "no momento do *design* do sistema eletrônico", a Diretiva 46 possuía um foco voltado mais propriamente a ações destinadas à *segurança* dos dados do que propriamente à *privacidade* dos dados[305]. Cite-se, exemplificativamente, o artigo 17 da Diretiva, o qual se refere expressamente à "segurança do processamento". Essa mesma perspectiva foi adotada quando da edição, pela União Europeia, da Diretiva 5, de 1999[306], e da Diretiva 58, de 2002[307], as quais abordavam, respectivamente, a proteção da privacidade na telecomunicação feita por equipamentos de rádio e a proteção da privacidade no setor de comunicações eletrônicas.

Ao que tudo indica, o primeiro reconhecimento internacional expresso sobre o *privacy by design* se deu no âmbito da 32ª Conferência de Comissários de Proteção de Dados e Privacidade[308], realizada em 2010, em Jerusalém. Na ocasião, Ann Cavoukian, então *Privacy and Informational Commissioner* da Província de Ontário, Canadá, apresentou uma proposta de resolução explicitamente sobre esta temática[309].

No texto, aprovado pela unanimidade dos presentes, os representantes das autoridades de proteção de dados reconheciam que as medidas até então realizadas não estavam sendo

---

processamento e a natureza dos dados a serem protegidos." (EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. op. cit., 1995. Não paginado).

[305] BYGRAVE, Lee A. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. **Oslo Law Review**, v. 4, n. 2, p. 105-120, 2017. p. 108.

[306] EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Directive 99/5/EC:** on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity. Brussels: European Union, 1999.

[307] EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Directive 2002/58/EC:** concerning the processing of personal data and the protection of privacy in the electronic communications sector. Brussels: European Union, 2002.

[308] Criada em 1979, esta conferência internacional é realizada anualmente com a finalidade de promover o intercâmbio de conhecimentos entre as autoridades de proteção de dados pelo mundo (INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS. **History of the Conference.** [s.n.s.l.]: 2018. Não paginado).

[309] INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS. **Resolution on Privacy by Design**. Jerusalem: ICDPP, 2010. p. 1.

suficientes para a proteção adequada da privacidade dos indivíduos. Além disso, compreendiam que, sendo importante a utilização de uma abordagem abrangente, a adoção de medidas abarcadas no conceito de *privacy by design* se apresentava como fundamental para a proteção da privacidade e que, portanto, deveriam ser promovidas pelos agentes estatais com competência sobre a matéria. Por fim, num claro sinal da importância do papel desempenhado por Cavoukian na disseminação deste instituto, as autoridades ali presentes listaram os sete "princípios fundantes", criados pela pesquisadora, como sendo parâmetros norteadores dos esforços a serem desempenhados quanto à matéria[310].

Com a adoção da resolução citada, o *privacy by design* disseminou-se na pauta de discussão regulatória. Assim, um dos primeiros casos a serem relacionados é o da OCDE, a qual, durante o processo de revisão de suas diretrizes de proteção à privacidade em 2013, passou a reputar como essencial a implementação de mecanismos para salvaguardar os dados pessoais desde o processo de concepção das tecnologias de informação e comunicação[311].

Examinando os avanços institucionais e a experiência obtida desde 1980, a OCDE identificou como consideravelmente preocupante o fato de que o custo para correção de tecnologias desenvolvidas sem preocupação com a privacidade era um constante impeditivo para uma melhor proteção das informações pessoais dos indivíduos[312]. Deste modo, propugnou que, desde o início, qualquer tecnologia de informação e comunicação voltada a processar dados pessoais começasse o processo de desenvolvimento realizado uma análise de impacto de privacidade, de modo a identificar os possíveis riscos existentes[313]. Ademais, também reputou estratégico que as entidades públicas e privacidades desenvolvessem uma cultura "pró-privacidade", incentivando a adoção de posturas institucionais responsáveis e transparentes no tratamento de dados[314]. Em resumo, a proteção deveria abranger todo o ciclo de vida dos dados pessoais dentro das organizações, incluindo mecanismos adequados desde a coleta e tratamento até a sua efetiva eliminação. A partir disso, a OCDE acreditava que o risco de danos aos indivíduos e prejuízos às instituições que utilizassem seus dados seria reduzido, tornando-se mais fácil o fluxo transfronteiriço de informações e interoperabilidade de sistemas[315].

---

[310] Idem, p. 2.
[311] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines.** Paris: OECD, 2013. p. 5.
[312] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** Paris: OECD, 2013. p. 104
[313] Idem, p. 104.
[314] Idem, p. 105.
[315] Idem, p. 104-105.

Todavia, não foi apenas a OCDE que percebeu a importância da coordenação no esforço internacional de proteção de dados. De fato, no âmbito da União Europeia diversos observadores já identificavam que a existência de mais de uma dezena de diplomas nacionais sobre a proteção de dados pessoais estava na realidade a dificultar a salvaguarda da privacidade dos cidadãos europeus. Nesse contexto, a fragmentação e a insegurança jurídica, somada à inexistência de um mecanismo para garantir a interpretação harmônica desse conjunto de normas estava também prejudicando os esforços de integração da comunidade europeia na criação de um mercado digital comum.

De acordo com um estudo realizado em 2012 pela Comissão Europeia para compreender o assunto[316], esta situação estava intimamente relacionada à Diretiva 46/1995, suas premissas, estrutura e efeitos. Em primeiro lugar, o panorama da economia digital já não era mais o mesmo do que quando o diploma havia sido editado: diversas tecnologias que sequer eram concebíveis na época passaram a ser praticamente lugar comum, tais como redes sociais, *smartphones*, entre outros[317]. Em segundo lugar, a modalidade normativa escolhida pela União Europeia para regulamentar a temática – uma diretiva [318] – trouxe como consequência uma grande fragmentação no ambiente regulatório, porquanto cada país editou normas com parâmetros distintos[319]. Portanto, era preciso que um novo marco regulatório, mais atualizado e mais apto a harmonizar as normas aplicáveis ao mercado digital comum, fosse editado. Por último, o bloco de países membros também desejava reforçar sua já significativa influência no cenário regulatório vinculado à proteção da privacidade, induzindo mais países a adotar seus padrões normativos de proteção[320].

Desta maneira, após um longo processo de negociações e deliberações iniciados em 2012, a União Europeia aprovou em 2016 o texto final do Regulamento 679 também conhecido

---

[316] EUROPEAN COMMISSION. **Commission Working Paper:** Impact Assessment on Regulation Proposal. Brussels: European Union, 2012.
[317] Idem, p. 9.
[318] Conforme o art. 288 do Tratado para o Funcionamento da União Europeia, uma diretiva é um documento vinculante que impõe aos Estado Membros a busca por um determinado objetivo, mas que deixa às autoridades nacionais escolher as formas e métodos para alcançar o referido objetivo. Diz o texto original em inglês que "A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods" (EUROPEAN UNION. **Treaty on the Functioning of the European Union.** Rome: European Union, 2012. Não paginado).
[319] EUROPEAN COMMISSION. **Commission Staff Working Paper:** Impact Assessment on Regulation Proposal. Brussels: European Union, 2012. p. 50.
[320] BACH, David; NEWMAN, Abraham L. The European regulatory state and global public policy: micro-institutions, macro influence. **Journal of European Public Policy**, v. 14, n. 6, p. 827-846, 2007. p. 833-834. BRADFORD, Anu. The Brussels Effect. Northwestern University Law Review, v. 107, n. 1, p. 1-68, 2012. p. 22-24.

em Inglês como *General Data Protection Regulation* ou *GDPR*[321]. Além de revogar e substituir expressamente a Diretiva 46 e, por ser um regulamento[322], ter a sua aplicação obrigatória frente a todos os Estado Membros, o GDPR significou um avanço notável nesta seara. Sendo composto de um preâmbulo explicativo com 173 parágrafos e possuindo 99 artigos em sua parte normativa, o texto do GDPR é consideravelmente mais robusto do que o da diretiva, possuindo disposições muito mais detalhadas quanto à proteção de dados pessoais.

De forma detalhada, o GDPR assegura aos indivíduos direitos subjetivos à informação sobre a coleta e tratamento de dados pessoais; à correção ou eliminação dos dados coletados ou tratados; à restrição de tratamento de dados; à objeção a decisões tomadas com base tratamento automatizado e à portabilidade de dados pessoais. Igualmente, o diploma também elenca uma série de mecanismos para assegurar a sua efetividade, os quais vão desde o estabelecimento de processos de certificação, a obrigação de designação de responsáveis por dados pessoais, análises de impactos à privacidade, a criação de autoridades independentes de proteção de dados até o estabelecimento de organismos internacionais para harmonização regulatória.

Ainda, no que é pertinente ao presente trabalho, o GDPR também contou com previsões específicas e expressas sobre *privacy by design*. Primeiramente, no parágrafo 78 do preâmbulo do diploma, o legislador europeu asseverou que[323]:

> *The protection […] of natural persons with regard to the processing of personal data* ***require that appropriate technical and organisational measures be taken*** *to ensure that the requirements of this Regulation are met. […] the controller should* ***adopt***

[321] EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679:** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Brussels: European Union, 2016. Não paginado.

[322] De acordo com o art. 288 do Tratado para o Funcionamento da União Europeia, um regulamento é uma espécie de texto normativo de aplicação geral, vinculante em sua totalidade e diretamente aplicável em todos os Estados Membros (EUROPEAN UNION. **Treaty on the Functioning of the European Union.** Rome: European Union, 2012. Não paginado).

[323] Original em inglês. Tradução livre: "A proteção dos direitos e liberdades de pessoas naturais com relação ao processamento de dados pessoais requer que as medidas técnicas e organizacionais apropriadas sejam tomadas para assegura que as exigências deste Regulamento sejam atingidas. Para ser capaz de demostrar o cumprimento deste Regulamento, o controlador deve adotar políticas internas e implementar medidas que sejam compatíveis com os princípios de proteção de dados *by design* e por padrão. Tais medidas poderiam consistir, entre outros, na minimização do processamento de danos pessoais, a pseudonimização de dados pessoais tão logo possível, transparência com relação às funções e processamento de dados pessoais, permitindo ao titular dos dados monitorar o processamento e habilitando o controlador a criar e aprimorar recursos de segurança. Ao realizar o desenvolvimento, design, seleção e utilização de aplicações, serviços e produtos que são baseados no processamento de dados pessoais ou que processam dados pessoais para suas atividades, os produtores devem ser encorajados a levar em consideração o direito à proteção de dados e, considerando o estado da arte, assegurar que controladores e processadores de dados sejam capazes de cumprir suas obrigações de proteção de dados. Os princípios de proteção de dados *by design* e por padrão também devem ser levados em consideração no contexto de contratações públicas."

> ***internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.*** *Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible,* ***transparency with regard to the functions and processing of personal data****, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features****. When developing, designing, selecting and using applications, services and products*** *[…] producers […] should be encouraged to take into account the right to data protection* ***when developing and designing*** *such products, services and applications and,* ***with due regard to the state of the art****, […]. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.* (grifou-se)

Além do preâmbulo, na parte normativa do diploma o artigo 25, denominado *data protection by design and by defaut*, dedica os incisos 1 e 2 ao tema. Nestes termos[324]:

> *1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*
> *2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

Num primeiro momento, deve-se atentar para o fato de que o texto se refere a "data protection by design" e não precisamente a "privacy by design". De fato, no curso do processo

[324] Original em inglês. Tradução livre:"1. Levando em conta o estado da arte, o custo da implementação e a natureza, abrangência, contexto e propósitos do processamento, bem como os riscos variáveis e a gravidade representados pelo processamento de dados para os direitos e liberdades de pessoas naturais, o controlador deverá, tanto ao tempo da determinação dos meios de processamento e ao tempo do próprio processamento, implementar medidas técnicas e organizacionais apropriadas, tal como a pseudonimização, que sejam projetadas para implementar princípios de proteção de dados, como minimização de dados, de maneira efetiva e para integrar as garantias necessárias no processamento de modo a atingir as exigências desta regulação proteger os direitos dos titulares de dados. 2. O controlador deverá implementar medidas técnicas e organizacionais apropriadas para assegurar que, por padrão, apenas dados pessoas que sejam necessários para cada propósito específico do processamento sejam processados. Esta obrigação se aplica ao montante de dados pessoais coletados, à extensão de seu processamento, ao período de sua manutenção e à sua acessibilidade. Em particular, tais medidas devem assegurar que por padrão dados pessoais não sejam acessíveis sem a intervenção do indivíduo a um número indefinido de pessoas naturais. "

de deliberação do GDPR, os termos foram inclusive usados como sinônimos[325]. Da mesma forma, os termos constavam como sinônimos na primeira versão do anteprojeto do GDPR[326].

De acordo com alguns observadores[327], a distinção entre "data protection" e "privacy" seria extremamente dependente do contexto cultural e tradição jurídica. Em especial, o termo "privacy" possuiria significado mais amplo e vago, sendo utilizado – particularmente no sistema jurídico estadunidense – de forma multidimensional [328] para descrever questões relacionadas à intimidade ou à autonomia privada de um determinado indivíduo [329]. Exemplificativamente, Warren e Brandeis utilizam a frase de Thomas Cooley "*right to be let alone*" como uma das possíveis formas de descrever o *right to privacy*[330]. Ann Cavoukian, ao seu turno, considera que *privacy* "*revolve[s] around control – personal control over collection, use and disclosure of one's identifiable info"*[331].

Por outro lado, a expressão "data protection" seria mais delimitada e precisa, referindo-se diretamente ao controle e segurança sobre o trânsito de dados, sendo este o motivo para adoção do conceito no GDPR[332]. Este também é o entendimento do *European Data Protection Supervisor*, o qual, em opinião técnica sobre o tema, considerou que o conceito de "data protection by design" estaria mais estritamente vinculado às obrigações legais definidas no artigo 25 do GDPR[333].

Por certo, a relativa novidade do tema na legislação estrangeira e nacional e a ausência de precedentes jurisprudenciais em cortes estrangeiras e nacionais impedem que seja possível

---

[325] EUROPEAN COMMISSION. **Commission Staff Working Paper:** Impact Assessment on Regulation Proposal. Brussels: European Union, 2012. p. 70.
[326] EUROPEAN COMMISSION. **Proposal for a Regulation of the European Parliament and of the Council:** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Brussels: European Union, 2012. p. 60.
[327] GUAMÁN, Danny. Privacy vs. Data Protection vs. Information Security. **Software and Services Engineering**, 01 nov. 2016. Não Paginado. GILBERT, Francoise. Privacy v. Data Protection: What is the Difference. **Privacy, Security, and Cloud Computing.** 1 oct. 2014. Não paginado.
[328] SOLOVE, Daniel J. A Taxonomy of Privacy. **University of Pennsylvania Law Review**, v. 154, n. 3, p. 477-560, jan. 2006. p. 558.
[329] De fato, o conceito de "privacy" foi inclusive utilizado como fundamento da decisão no caso Roe v. Wade, no qual a Suprema Corte estadunidense considerou legal a realização de procedimentos de aborto até o terceiro mês de gestação (UNITED STATES OF AMERICA.SUPREME COURT. **Roe v. Wade.** 410 U.S. 113 (1973)).
[330] WARREN; BRANDEIS. op. cit., p. 195. Em Língua Portuguesa, pode ser traduzido livremente como "direito de ser deixado só".
[331] Original em Inglês. Tradução livre: "privacidade gira em torno de controle – controle pessoal sobre coleta, uso e divulgação de informações pessoais sobre si" (CAVOUKIAN, Ann. **Privacy by Design in Law, Policy and Practice:** a White Paper for Regulators, Decision-Makers and Policy-makes. Ontario: Information and Privacy Commissioner: 2011. p. 6).
[332] EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 5/2018:** Preliminary Opinion on Privacy by Design. Brussels: EDPS, 2018. p. 1
[333] Idem, p. 1.

chegar a uma conclusão definitiva sobre qual o melhor termo a ser utilizado. Deste modo, feita a breve ressalva acima, para os fins do presente trabalho as expressões *data protection by design* e *privacy by design* serão tratadas como sinônimas, dando-se preferência à utilização desta última em razão de ser mais difundida e pelo fato de que, da análise das manifestações mais recentes de entes reguladores da comunidade europeia, não foi possível identificar uma preocupação efetiva destes entes em diferenciar estas expressões.

Verdadeiramente, a influência do GDPR para a propagação do *privacy by design* foi significativa, inclusive ao ponto de impactar no debate legislativo em curso no Congresso Nacional brasileiro acerca da proteção de dados pessoais. Com efeito, após um processo de deliberação legislativa que durou quase seis anos, foi promulgada a Lei Federal 13.709, de 14 de agosto de 2018, cujo texto possui diversos elementos consideravelmente semelhantes ao diploma europeu, a saber[334]:

> Art. 35 [...] § 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com **as medidas técnicas e organizacionais adotadas pelo operador**, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.
> [...]
> Art. 46. **Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais** de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, **considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia,** especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo **deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução**. (grifou-se)

Conforme se verifica, ao se referir a uma obrigação de realizar "medidas técnicas e organizacionais", "desde a fase da concepção do produto ou do serviço até a sua execução", para a proteção de dados pessoais, levando em conta a "natureza das informações", as "características específicas do tratamento" e o "estado atual da tecnologia", o legislador brasileiro ilustra a influência do GDPR em nosso país. Entretanto, a Lei Geral de Proteção de Dados brasileira, talvez em virtude da novidade das discussões sobre o tema, é também pouco

[334] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Não paginado.

clara sobre o que seria efetivamente o *privacy by design* e quais seriam as medidas necessárias para a sua implementação.

Deste modo, tendo em vista que a compreensão sobre o assunto é essencial para a efetiva proteção da privacidade dos indivíduos, a seção **3.3** a seguir buscará traçar considerações acerca do tema de forma a permitir como entender como se operacionaliza uma política voltada à implementação deste instituto, assim como os mecanismos organizacionais e tecnológicos existentes para assegurar seu cumprimento. Tendo em vista que as o *privacy by design* passou a receber mais atenção em virtude da edição recente do GDPR europeu, este diploma será adotado como referencial normativo para guiar a próxima parte deste texto. Não obstante, levando em conta a forte inspiração exercida pelo texto europeu no legislador brasileiro, na medida do possível procurar-se-á relacionar o texto da a Lei nº 13.079, de 14 de agosto de 2018 com o assunto abordado, da maneira a refletir a seu respeito, a despeito da relativa escassez de trabalhos sobre *privacy by design* no Brasil.

3.3 DA OPERACIONALIZAÇÃO DO *PRIVACY BY DESIGN*: SEU FUNCIONAMENTO E OS MECANISMOS INSTITUCIONAIS PARA SUA EFICÁCIA

Desde que seus primeiros contornos foram delineados pelo relatório produzido conjuntamente pelo *Privacy Information Commissioner* de Ontário e a autoridade holandesa de proteção de dados, o *privacy by design* passou um profundo processo de desenvolvimento. Naquele momento inicial, os especialistas responsáveis pelo estudo propunham a utilização de medidas eminentemente tecnológicas, tais como a minimização e a anonimização dos dados coletados[335], as quais inclusive estão previstas no texto do artigo 25 do GDPR já mencionado na seção anterior deste trabalho. Entretanto, apesar do principal e mais abrangente diploma sobre proteção de dados mencionar a minimização e anonimização como técnicas a serem utilizadas, especialistas no assunto entendem que o *privacy by design* não se limita apenas a medidas tecnológicas.

De fato, Ann Cavoukian, a quem é creditada a própria criação da expressão "*privacy by design*", afirma categoricamente que o instituto se refere a uma "filosofia e abordagem de

[335] INFORMATION AND PRIVACY COMMISSIONER; REGISTRATIEKAMER. **Privacy-Enhancing Technologies:** the path to anonymity. Toronto, The Hague: Information and Privacy Commissioner; Registratiekamer, 1995.

introduzir a privacidade [...] no *design*, operação e administração de sistemas e tecnologias de processamento de informação"[336]. Igualmente, ela entende que o instituto seria aplicável não só na área tecnológica, mas também nas práticas empresariais e no próprio *design* físico envolvido no tratamento de dados[337].

Diante dessa situação, bem como, atualmente, da inexistência de um conceito legal expresso e delimitado sobre o que seria o *privacy by design* no GDPR, o instituto foi desde cedo criticado pelo fato de não ser claro o suficiente, o que poderia gerar insegurança jurídica aos setores regulados[338]. Em verdade, a indefinição quanto ao significado do instituto foi abordada pela Comissão Europeia em 2012 já na primeira análise realizada quanto à necessidade de revisar a Diretiva 46/95. Na ocasião, alguns atores estatais demonstraram preocupação quanto à importância de não estabelecer uma definição precisa, de modo a garantir sua aplicação para várias hipóteses[339]. Por outro lado, representantes de setores empresariais manifestaram sua apreensão quanto ao fato do conceito de *privacy by design* ser muito vago e difícil de aferir se fosse para permanecer tecnologicamente neutro[340].

Justamente para manter a neutralidade tecnológica e preservar o objetivo de proteção ampla da privacidade, a Comissão Europeia categorizou o instituto de forma genérica, descrevendo-o como sendo constituído de "medida[s] destinada[s] a reduzir os riscos de violação da legislação de proteção de dados"[341]. Entretanto, esta indefinição quanto ao conceito a ser aplicado pelos órgãos reguladores não tem apenas a finalidade de ser tecnologicamente neutra. De fato, esta amplitude semântica permite à regulação alcançar não só a tecnologia em si, mas também questões organizacionais e institucionais de órgãos e entidades que realizam coleta e tratamento de dados pessoais, as quais também são importantes para a proteção da privacidade[342].

---

[336] Tradução livre. Original em Inglês: "the philosophy and approach of embedding privacy [...] into the design, operation and management of information processing technologies and systems" (CAVOUKIAN, Ann. **Privacy by Design**. Ontario: Information and Privacy Commissioner, 2009. p. 1).
[337] Idem, p. 1.
[338] KROENER, Inga; WRIGHT, David. A Strategy for Operationalizing Privacy by Design. **The Information Society**, v. 30, p. 355-365, 2014. p. 357.GURSES, Seda; TRONCOSO, Carmela; DIAZ, Claudia. Engineering Privacy by Design. **Conference on Computers, Privacy & Data Protection**, p. 1-25, 2011. p. 3.
[339] EUROPEAN COMMISSION. **Commission Staff Working Paper:** Impact Assessment on Regulation Proposal. Brussels: European Union, 2012. p. 82.
[340] Idem, p. 82.
[341] Tradução livre. Original em inglês: "measure aimed at reducing the risks of infringements of the data protection legislation (Idem, p. 110).
[342] O uso de técnicas regulatórias que evitem depender de textos muito específicos no âmbito da regulação de tecnologias é abordado com maior atenção por Chris Reed, o qual defende que textos muito específicos acabam por falhar em produzir os resultados normativos pretendidos (REED, Chris. How to Make Bad Law: Lessons from Cyberspace. **Modern Law Review**, v. 73, n. 6, p. 903-932, 2010. p. 911-913).

Nesse sentido, o *European Data Protection Supervisor*, entidade independente responsável pela supervisão e fiscalização da proteção à privacidade e dados pessoais em nível europeu, optou até o presente momento por abordar a temática examinando-a sob a ótica de quatro "dimensões"[343], evitando a necessidade de se comprometer com um só sentido. Assim sendo, tendo em vista que o entendimento do *European Data Protection Supervisor* orienta a matéria em todo o bloco europeu e influencia a discussão em outros países, este trabalho irá adotar e explorar esta estratégia para descrever a operacionalização do *privacy by design.*

Para o *European Data Protection Supervisor* a *primeira* dimensão estaria relacionada à constatação de que o tratamento de dados pessoais por uma tecnologia de informação e comunicação sempre será o resultado do *design* proposto para um projeto. Portanto, nesta fase inicial é necessário que se perceba que a proteção destas informações ocorre durante todo o ciclo de vida do produto. Desta maneira, deve-se identificar claramente os dados a serem coletados e tratados e os mecanismos protetivos necessários, incluindo-os na esfera dos requisitos do projeto a ser executado.

Neste contexto, a realização de uma *análise de impacto de privacidade*, também chamada de análise de impacto de proteção de dados, é considerada como sendo um passo preliminar e fundamental a ser realizado[344]. Oriundas de um longo processo de discussão iniciado nas décadas de 80 e 90 e influenciado pelas experiências de outras áreas, notadamente discussões sobre impactos ambientais, as análises de impacto de privacidade começaram a surgir expressamente a partir da década de 90 e no início dos anos 2000 por iniciativas desenvolvidas nos EUA, Europa e países da *Commonwealth*[345]. Por permitirem uma compreensão melhor sobre o tratamento e a coletada de dados realizados, são pré-requisitos de qualquer processo de implementação de uma política de *privacy by design.*

De acordo com Roger Clarke, uma análise de impacto de privacidade se difere de outros instrumentos relacionados ao tema em virtude das seguintes características[346]: a) é realizada com relação a projetos e à organização em si; b) é realizada antecipadamente e não retrospectivamente; c) não se preocupa apenas com os dados pessoais em si, mas também com

---

[343] EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 5/2018:** Preliminary Opinion on Privacy by Design. Brussels: EDPS, 2018. p. 6.
[344] WRIGHT, David. The State of the Art in Privacy Impact Assessment. **Computer Law & Security Review**, v. 28, n. 1, p. 54-61, fev. 2012. p. 55.
[345] BINNS, Reuben. Data Protection Impact Assessments: a meta-regulatory approach. **International Data Privacy** Law, v. 7, n. 1, p. 22-35, 2017. p. 23. CLARKE, Roger. Privacy Impact Assessment: Its Origins and Development. **Computer Law & Security Review**, v. 25, n. 2, p. 123-135, 2009. p. 127-129.
[346] CLARKE, op. cit., p. 124.

o contexto do tratamento e comportamento do indivíduo titular; d) não se foca apenas no interesse da organização que realiza a coleta ou tratamento ou seus parceiros institucionais, mas também nos interesses dos grupos cujos dados são coletados e tratados; e) realiza uma análise que não se restringe apenas ao *compliance* legal; f) é orientada a identificar tanto os problemas quanto suas possíveis soluções; g) exige a participação de executivos e administradores sêniores e não apenas dos funcionários ou advogados de nível hierárquico baixo ou intermediário na organização.

Tendo em vista que a concepção de "privacidade" é extremamente dependente do tipo de informação pessoal sob exame e do contexto em que está sendo analisada, existem diversas metodologias desenvolvidas tanto por autoridades públicas quanto por organismos privados para aplicação de uma análise de impacto, não sendo objetivo deste trabalho aprofundar-se nas particularidades de cada metodologia existente. Não obstante, buscando ilustrar minimamente a questão, é interessante trazer aqui algumas das considerações feitas por David Wright[347], o qual lista um total de dezesseis etapas para a implementação de uma análise de impacto de privacidade adequada, a saber[348]: 1º) determinar se a análise é necessária; 2º) identificar o time responsável por realiza-la e determinar as referências, recursos e prazo deste time; 3º) estabelecer um planejamento de execução; 4º) estabelecer um orçamento para execução; 5º) descrever o projeto a ser avaliado; 6º) identificar as partes interessadas; 7º) identificar os fluxos de informações existentes; 8º) consultar as partes interessadas; 9º) examinar se o projeto cumpre a legislação vigente; 10º) identificar riscos e soluções; 11º) formular recomendações; 12º) preparar e publicar o relatório; 13º) implementar as recomendações; 14º) realizar avaliação externa da análise de impacto realizada; 15º) atualizar a análise de impacto se o projeto sofrer modificações; 16º) fortalecer a percepção da importância de preservação da privacidade na organização. Estas são, em síntese, as etapas consideradas relevantes pelos estudiosos especialistas na matéria. Conforme se verificará abaixo, muitos dos elementos ali descritos estão presentes na legislação relacionada à temática, em particular, para os fins do presente estudo, a Lei nº 13.079, de 14 de agosto de 2018 e o *General Data Protection Regulation.*

Como foi dito acima, em razão de sua importância para o estabelecimento de uma política de *privacy by design,* diversas legislações recentes voltadas à proteção de dados

---

[347] Em razão de David Wright ser consultor da Comissão Europeia e responsável por diversos estudos que fundamentam a atuação do órgão europeu em matéria de proteção à privacidade, buscou-se privilegiar o entendimento deste autor quanto ao assunto.

[348] WRIGHT, David. Making Privacy Impact Assessment More Effective. **The Information Society International Journal**, v. 29, n. 5, p. 307-315, 2013. p. 310-313.

pessoais possuem previsão quanto à realização de análises de impacto. No Brasil, por exemplo, a Lei nº 13.079, de 14 de agosto de 2018 traçou algumas linhas sobre o tema. Assim, conforme o art. 5º, inciso XVII do diploma referido, o "relatório de proteção de dados pessoais" é definido como sendo[349]:

> [a] **documentação** do controlador que contém a **descrição dos processos de tratamento** de dados pessoais que **podem gerar riscos** às liberdades civis e aos direitos fundamentais, bem como **medidas, salvaguardas e mecanismos de mitigação de risco**. (grifou-se)

Mais adiante, o art. 38, parágrafo único do mesmo diploma esclarece um pouco mais quais seriam os elementos mínimos deste relatório. Deste modo, menciona que deverá conter, no mínimo: a) a descrição dos tipos de dados coletados; b) a metodologia utilizada para a coleta e para a garantia da segurança das informações; e c) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Todavia, a despeito destes dispositivos legais, a regulação brasileira, além de muito recente, dependerá de posterior desenvolvimento pela autoridade nacional de proteção de dados, que, apesar de ter sido recentemente prevista pela Medida Provisória nº 869[350], ainda não foi constituída pela Presidência da República[351].

É forçoso reconhecer que texto da legislação brasileira sobre o tema é sucinto, explorando pouco o mecanismo das análises de impacto à privacidade. Por outro lado, no cenário europeu, que serviu de principal inspiração para o legislador brasileiro, o GDPR possui um arcabouço normativo mais bem delineado quanto ao assunto. Por certo, o fato de as discussões sobre a proteção à privacidade estarem em curso a mais tempo no plano europeu ajuda a compreender os motivos pelos quais isso ocorre.

Ao contrário do Brasil, onde os instrumentos das análises de impacto à privacidade receberam um tratamento mais limitado, na União Europeia o art. 35 do GDPR dispõe mais extensamente sobre o tema, prevendo, em especial: a) a participação do agente de proteção de dados interno na avaliação; b) uma lista de atividades cuja realização de análises de impacto é

---

[349] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Não paginado.
[350] BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília: Presidência da República, 2018. Não paginado.
[351] Leva-se em consideração a data de 03/06/2019, na qual foi editada a última versão deste texto.

obrigatória; c) a possibilidade de a autoridade de proteção de dados prever novas hipóteses de atividades cuja análise de impacto é obrigatória, bem como estabelecer situações onde não o são; d) a obrigatoriedade de levar em conta, em situações determinadas, as opiniões dos titulares de dados ou seus representantes. Estes elementos, somados às legislações nacionais existentes nos estados-membros, demonstram a maior maturidade da legislação europeia.

Em seguida, a *segunda* dimensão do *privacy by design* estaria vinculada ao gerenciamento dos riscos aos quais estão sujeitos os dados pessoais durante sua coleta e tratamento pelo sistema eletrônico. De fato, a partir da elaboração de uma análise de impacto à privacidade adequada, uma organização terá conseguido realizar a identificação inicial dos dados a serem coletados e tratados, bem como os agentes responsáveis por cada etapa de funcionamento do sistema. Igualmente, será possível delinear o contexto e o propósito da coleta e do tratamento e localizar demais os elementos humanos, organizacionais e tecnológicos que possuam condições de propiciar riscos a estes dados. Diante dessas informações, faz-se necessário integrar os riscos à privacidade ao processo e às rotinas de gerenciamento dos demais riscos relacionados ao projeto[352].

Existem diversos modelos para se avaliar os possíveis riscos aos quais tecnologias de informação e comunicação estão sujeitas a depender do tipo de dados coletados, características de seus titulares, contexto do tratamento, jurisdições envolvidas[353], entre outros fatores. Nesse sentido, questionamentos como "existem agentes mal intencionados interessados nos dados?", "como os dados pessoais são compartilhados?", "qual o volume de compartilhamento?" e "qual a qualidade dos dados compartilhados?" são essenciais para identificar algumas das espécies de riscos existentes[354]. Diante das respostas obtidas, torna-se possível ao responsável pelo gerenciamento dos riscos avaliar efetivamente se os dados pessoais sob sua responsabilidade não estão sujeitos a riscos vinculados à legalidade, consentimento, finalidade, acurácia, transparência e segurança[355].

---

[352] WRIGHT, David et al. Integrating Privacy Impact Assessment in Risk Management. **International Data Privacy Law**, v. 4, n. 2, p. 155-170, 2014. p. 169.

[353] Exemplificativamente: CAVOUKIAN, Ann. **Privacy Risk Management:** Building Privacy Protection into a Risk Management Framework. Ontario: Information and Privacy Commissioner, 2010. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Methodology for Privacy Risk Management.** Paris: CNIL, 2018. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Risk Management Framework for Information Systems and Organizations.** Washington: NIST, 2018.

[354] HONG, Jason I. et al. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. **DIS '04 Proceedings of the 5th conference on Designing Interactive Systems.** Cambrigde: Association for Computing Machinery, 2004. p. 5.

[355] GHOLAMI, Ali et ali. Privacy Threat Modeling for Emerging Biobank Clouds. **Procedia Computer Science,** v. 37, p. 489-496. 2014. p. 494-496

Localizados os elementos relevantes, também devem ser identificadas as medidas a serem tomadas para eliminar os riscos existentes, bem como os agentes, no âmbito da organização, responsáveis e tecnicamente habilitados para desempenhar esta tarefa. Naqueles casos onde não seja possível a eliminação completa dos riscos identificados, mas apenas a sua mitigação, é necessário que sejam avaliadas a oportunidade, a conveniência e a necessidade da coleta e/ou do tratamento em questão, sendo apenas legítima a continuidade da operação naqueles casos em que forem imprescindíveis. Em casos como estes, alguns diplomas voltados à proteção de dados pessoais inclusive preveem a obrigatoriedade de anuência da autoridade de proteção de dados para que seja possível realizar a coleta e o tratamento[356].

Do mesmo modo, métricas e mecanismos devem ser traçados para que seja possível medir, controlar e avaliar permanentemente a evolução dos riscos aos dados pessoais durante a operação e funcionamento do sistema. Desta maneira, sempre que houver alguma modificação no panorama de riscos existentes, especialmente devido ao advento de novas tecnologias e técnicas de tratamento de dados ou a mudanças na legislação vigente, as medidas de proteção existentes devem ser reavaliadas para que se possa assegurar que ainda são capazes de proteger as informações cuja salvaguarda é exigida pelas normas de proteção de dados pessoais.

Por sua vez, a *terceira* dimensão do *Privacy by Design* seria relativa às ações realizadas para garantir que as medidas tomadas pela organização sejam apropriadas e efetivas para a proteção dos dados pessoais. Assim sendo, os responsáveis pelo desenvolvimento e operação do sistema eletrônico devem ser capazes de demonstrar o cumprimento das normas pertinentes à proteção das informações. Para tanto, além de ter todo o processo de coleta e tratamento de dados devidamente mapeado, é necessário que a documentação existente seja clara e acessível, demonstrando os riscos existentes, as medidas tomadas, os agentes responsáveis e as tecnologias utilizadas. Igualmente, é crucial que todas estas informações sejam transparentes e acessíveis aos titulares dos dados, possibilitando o efetivo desenvolvimento do consentimento para utilização das informações pessoais e, assim, proporcionar o surgimento de uma relação de confiança para com a tecnologia.

Tendo em vista a concepção de que mecanismos de regulação e fiscalização baseados exclusivamente em ações desempenhadas por entes estatais não produziriam, em tese,

---

[356] Exemplificativamente, o artigo 26 do *GDPR* prevê a obrigação do controlador de dados consultar previamente a autoridade de proteção de dados quando a análise de impacto à privacidade identificar riscos elevados no processamento de dados pessoais.

resultados satisfatórios no ambiente de tecnologias de informação e comunicação [357], abordagens que utilizam conjuntamente ações públicas e privadas têm recebido cada vez mais atenção[358]. Em razão disso, diplomas mais recentes voltados à proteção de dados pessoais têm buscado incluir no panorama regulatório mecanismos como selos e certificações, os quais, expedidos principalmente por organismos privados ou paraestatais de acordo com critérios estabelecidos ou reconhecidos por uma entidade pública, atestariam a adesão ou cumprimento de boas práticas organizacionais e/ou tecnológicas para proteção da privacidade[359].

Inspirada fortemente no GDPR europeu, a Lei nº 13.079, de 14 de agosto de 2018, não é exceção a esta tendência. Deste modo, o diploma brasileiro prevê em seu art. 35, §3º que "a autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento". Ainda, o §4º do mesmo artigo estabelece que "os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados". Todavia, em virtude de a reserva regulamentar prevista pelo legislador ordinário ainda não ter sido desempenhada[360], até o presente momento não é possível identificar os contornos que esta modalidade regulatória terá em nosso país.

No cenário europeu o GDPR, em seus artigos 42 e 43, regulamentou diversos aspectos relacionados ao funcionamento dos processos de certificação e dos organismos por eles responsáveis. Nesse sentido, no que se refere ao processo de certificação, o art. 42 do diploma referido prevê, em primeiro lugar, que este deverá ser encorajado pela União Europeia e países

---

[357] Não obstante, existem autores que defendem o estabelecimento de autoridades públicas com atribuições específicas para a fiscalização de algoritmos computacionais. Nesse sentido, por exemplo: BRACHA, Oren; PASQUALE, Frank. Federal Search Commission: Access, Fairness, and Accountability in the Law of Search. **Cornell Law Review**, v. 93, n. 6, p. 1149-1210, 2008. TUTT, Andrew. An FDA for Algorithms. **Administrative Law Review**, v. 69, p. 83-123, 2017.

[358] DONEDA, Danilo; ALMEIDA, Virgílio A. F. What is Algorithm Governance? **IEEE Internet Computing**. v. 20, n. 4, p. 60-63, jul./ago. 2016. p. 62. RODRIGUES, Rowena; WRIGHT, David; WADHWA, Kus. Developing a Privacy Seal Scheme (that works). **International Data Privacy Law**, v. 3, n. 2, p. 100-116, 2013. p. 116. LESK, Michael. Trust, but Verify. **IEEE Security & Privacy**, v. 12, n. 6, p. 94-96, nov./dec. 2014. p. 94-95.

[359] Por força do GDPR e com a finalidade de harmonizar as práticas do mercado digital comum, os países membros da União Europeia estão vinculados a regulamentar mecanismos de certificação voltados à proteção de dados pessoais (RODRIGUES, Rowena et al. The Future of Privacy Certification in Europe: an Exploration of Options under Article 42 of the GDPR. **International Review of Law, Computers & Technology**, v. 30, n. 3, p. 248-270, 2016. p. 266-267).

[360] Embora a Presidência da República tenha editado a Medida Provisória nº 869, de 27 de dezembro de 2018, buscando regulamentar a criação da Autoridade Nacional de Proteção de Dados, até o momento de conclusão da redação final deste trabalho o órgão em questão não havia sido criado (BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília: Presidência da República, 2018).

membros com o propósito de demonstrar a observância das normas de proteção de dados pessoais tanto por controladores quanto por processadores de dados, sempre levando em consideração as especificidades de micro, pequenas e médias empresas.

Embora o GDPR assevere que o processo de certificação seja voluntário mesmo aos entes obrigados a dar cumprimento às suas normas, o diploma também permite que entes que eventualmente não estejam sujeitos ao regulamento europeu também obtenham certificações. Com isso, os legisladores europeus buscaram ampliar a esfera de proteção de dados pessoais para outros setores econômicos[361], bem como fortalecer sua estratégia de criação de um mercado comum digital e induzir atores em outras jurisdições a adotar normas semelhantes às suas, reduzindo a assimetria regulatória e os custos de transação para empresas europeias[362].

Tendo em vista que uma das críticas recorrentes aos selos e certificações enquanto ferramenta regulatória reside justamente na baixa confiança nos organismos responsáveis por emitir as certificações[363], o artigo 43 do GDPR buscou tratar justamente esta questão. Assim, determinou aos estados-membros da União Europeia que apenas reconheçam organismos de certificação que, cumulativa ou alternadamente: a) sejam reconhecidos pelas autoridades nacionais de proteção de dados; ou b) sejam reconhecidos pelo órgão nacional de acreditação, nos termos do Regulamento nº 765/2008[364], cuja finalidade é justamente tratar sobre órgãos de acreditação e normalização técnica. Além disso, diversas outras exigências são feitas buscando assegurar a independência e a prevenção de conflitos de interesse nestes atores.

Finalmente, a *quarta* dimensão diria respeito à obrigação de integrar as salvaguardas identificadas a todo o ciclo de utilização dos dados pessoais, de forma a permitir a proteção completa destas informações. Deveras, as dimensões anteriormente descritas propiciam a estruturação de um arcabouço institucional onde os riscos aos dados pessoais estão identificados ou são identificáveis, os agentes responsáveis são conhecidos e possuem atribuições bem delineadas e os titulares dos dados são capazes de efetivamente exercer consentimento

---

[361] RODRIGUES, Rowena *et allia*, op. cit., 2016. p. 249.

[362] EUROPEAN COMMISSION. **Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy.** Brussels: European Union, 2017. Não paginado.

[363] RODRIGUES, Rowena et al, op. cit., p. 249. JAHN, Gabriele; SCHRAMM, Mathias; SPILLER, Achim. The Reliability of Certification: Quality Labels as a Consumer Policy Tool. **Journal of Consumer Policy**, v. 28, n. 1, p. 53-73, 2005. p. 54.

[364] EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Regulation (EC) 765/2008:** setting out the requirements for accreditation and market surveillance relating to the marketing of products. Brussels: European Union, 2008.

informado quanto à utilização de suas informações. Com todo este panorama, torna-se viável que o *privacy by design* seja definitivamente integrado a todo o processo de coleta e tratamento dos dados por meio das diversas técnicas de proteção de dados existentes.

Tendo em vista que o enfoque principal deste trabalho é, em última análise, jurídico, não se irá aqui realizar uma descrição exaustiva de todas as medidas técnicas existentes para proteção de dados pessoais passíveis de serem implementadas em um sistema eletrônico[365]. Todavia, tendo em vista que o próprio texto do GDPR menciona expressamente algumas das técnicas possíveis, é importante e necessário tecer comentários a seu respeito para poder aproximar o leitor não familiarizado com o tema.

Da leitura do artigo 25 do diploma europeu é possível identificar, de plano, duas técnicas utilizadas frequentemente para a proteção de dados, a saber: a) a pseudonimização; b) a minimização de dados.

Em primeiro lugar, a "minimização de dados" seria, de acordo com o GDPR, um dos princípios vinculantes do processamento de dados pessoais. Assim, para o artigo 5, (1), (c) do diploma europeu, a minimização de dados significaria que os dados pessoais devem ser "adequados, relevantes e limitados ao que for necessário aos propósitos para os quais são processado"[366]. Ao interpretar o assunto no âmbito de suas competências regulatórias, o órgão europeu responsável pela questão referiu que é necessário que os controladores da operação sejam capazes de claramente explicar e justificar a necessidade de processamento e coleta, especialmente tendo em vista a possibilidade de utilização de dados agregados[367]. No âmbito brasileiro, apesar de não constar expressamente com essa denominação, é possível reconhecer que o art. 6º, I da Lei nº 13.079, de 14 de agosto de 2018 também estabeleceu a minimização de dados como princípio a ser adotado ao conceituar o princípio da "necessidade" como sendo a[368]:

---

[365] Para fins ilustrativos, vide, exemplificativamente: HOEPMAN, Jaap-Henk. Privacy Design Strategies. **Privacy Law Scholars Conference.** Berkeley: Privacy Law Scholars Conference, 2013.

[366] EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679:** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Brussels: European Union, 2016. Não paginado.

[367] EUROPEAN UNION. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.** Brussels: Article 29 Data Protection Working Party, 2018. p. 11.

[368] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Não paginado.

> [...] limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Em resumo, trata-se de abordagem de desenvolvimento de tecnologias de informação e comunicação que procura refletir sobre a efetiva necessidade de coleta, utilização e armazenamento de dados[369]. Deste modo, durante a fase de concepção de um projeto, seus responsáveis ficam, a partir deste princípio, obrigados a considerar questões como "preciso coletar este dado?", "por que preciso deste dado?", "como vou armazenar este dado?", "por quanto tempo preciso armazenar este dado?", entre outras.

Na prática, a aplicação da minimização de dados resulta numa maior proteção à privacidade pelo simples fato de existem menos informações à disposição ou expostas ao risco. Entretanto, ainda que sua aplicação seja desejável, nem sempre será isenta de controvérsias. Com efeito, em alguns casos, para que seja possível a proteção da privacidade de determinados grupos de indivíduos, a coleta de dados pessoais sensíveis é considerada obrigatória pela legislação vigente. Exemplo disso é a situação em que, para a proteção do menor, a Lei nº 13.079, de 14 de agosto de 2018, exige em seu artigo 14, §2º a coleta de dados do responsável legal da criança para que seja viável determinar o seu consentimento. Essa mesma situação ocorre com o GDPR, cujo texto também estabelece requisitos especiais para o tratamento de dados de crianças, o que também acarreta a coleta de mais dados pessoais. Por certo, quanto maior a quantidade de dados cuja coleta é necessária para cumprir a legislação, maior será o risco. Em síntese, ainda que seja uma estratégia importante a ser levada em conta durante o desenvolvimento de sistemas, nem sempre será aceitável a sua utilização quando a legislação considerar existir outros interesses mais relevantes.

Em segundo lugar, a "pseudonimização" de dados, de forma simplificada, significa basicamente a substituição da atribuição ou relação original de um determinado dado por outra, que será utilizada em seu lugar, mantendo-se a atribuição ou relação original armazenada em local seguro para fins de recuperação caso necessário. Em razão de sua importância desta

---

[369] PFITZMANN, Andreas; HANSEN, Marit. **A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management.** Dresden: Faculty of Computer Science, 2010. p. 6.

técnica a proteção de dados, a legislação mais recente quanto ao tema passou a elencar a conceitos expressos a seu respeito. Nesse sentido, o artigo 4, (5) do GDPR refere que[370]:

> ***'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject*** *without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;* (grifou-se)

Em nosso país, a recém promulgada Lei nº 13.079, de 14 de agosto de 2018 também adota um conceito legal expresso para a pseudonimização quando da utilização de dados pessoais sensíveis para a realização de estudos em saúde pública[371]. Assim, conforme o art. 13, §4º do diploma, a pseudonimização seria "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".

É importante deixar claro que, embora se relacionem, "pseudonimização" e "anonimização" não são a mesma coisa. Nesta última, a atribuição ou relação original do dado é eliminada por meio de técnicas[372] que assegurem, em tese, a irreversibilidade do processo[373]. Essa ressalva quanto à reversibilidade do processo de anonimização é importante, pois tanto agentes reguladores quanto os responsáveis por sistemas eletrônicos que coletem e tratem dados

---

[370] Original em Inglês. Tradução livre: "Pseudonimização significa o processamento de dados pessoais de modo que o dado pessoal não possa mais ser atribuído a um titular de dados sem o uso de informações adicionais, desde que estas informações adicionais sejam armazenadas separadamente e sujeitas a medidas técnicas e organizacionais para assegurar que os dados pessoas não sejam atribuídos para uma pessoa natural identificada ou identificável" (EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679:** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Brussels: European Union, 2016. Não paginado).

[371] Embora não seja objeto do presente estudo, interessante questão a ser futuramente estudada é aquela a respeito da possibilidade de utilização das bases de dados para estudos que, a despeito de serem de interesse público, não sejam vinculados diretamente a questões de saúde pública.

[372] Exemplificativamente, podem-se citar dentre as diversas técnicas de utilização possível para anonimização de dados a supressão de dados, a generalização de dados, a agregação de dados e a criptografia de dados (OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. **University of California Law Review**, v. 57, p. 1701-1777, 2010. p. 1715).

[373] De acordo com o Andreas Pfitzmann e Marit Hansen, estudiosos da Universidade de Dresden: "Para permitir o anonimato de um sujeito, sempre é necessário que exista um conjunto apropriado de sujeitos com os mesmos atributos. [...] 'Anonimato" de um sujeito significa que o sujeito não é identificável dentre o conjunto de sujeitos, o 'conjunto de anonimato'. Tradução livre. Original em Inglês: "To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes. […]. Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set" (PFITZMANN, Andreas; HANSEN, Marit. **A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management.** Dresden: Faculty of Computer Science, 2010. p. 9).

pessoais devem sempre levar em consideração em seus planejamentos o fato de que não existe técnica de anonimização perfeita. É relevante que se perceba também que a segurança e confiabilidade das medidas adotadas para a anonimização são igualmente dependentes das tecnologias, recursos e informações auxiliares à disposição de um agente eventualmente interessado em obter as informações pessoais[374].

Ao contrário da anonimização, a pseudonimização permite que o valor original seja deliberadamente recuperado caso necessário por algum motivo legítimo[375]. De forma geral, esta técnica pode ser usada sempre que a identidade do titular dos dados pessoais não seja absolutamente necessária para o tratamento de dados pretendido. Em resumo, o agente que interage com outro sob pseudônimo confia que o processo do qual resultou a pseudonimização é legítimo e regular. Assim, embora não saiba efetivamente com quem interage, sabe que ela possui os atributos mínimos para realizar o relacionamento ou transação que deseja.

3.4 SÍNTESE DESTA SEÇÃO

O desenvolvimento do pensamento a respeito da regulação de tecnologias de informação e comunicação feito, de forma marcante, por juristas estadunidenses influenciou profundamente as discussões sobre o assunto nos países ocidentais, especialmente no hemisfério norte. Da reflexão destes estudiosos, agentes públicos e privados envolvidos nesta área gradativamente desencadearam um intenso diálogo acerca da melhor forma para proteção da privacidade dos indivíduos diante de um cenário em que sistemas eletrônicos cada vez mais coletavam e tratavam rotineiramente dados pessoais para as mais diversas finalidades.

Num primeiro momento, postulou-se o fortalecimento de medidas jurídicas sancionatórias, notadamente a responsabilidade civil, como forma de salvaguardar o interesse dos titulares das informações objeto de abuso. Todavia, a facilidade com que a informação transita por inúmeras jurisdições por meio da rede mundial de computadores acabou tornando inviável a dependência exclusiva nessa espécie de clássica de regulação estatal. Igualmente, as características econômicas intrínsecas de não-rivalidade e não-exclusividade da informação são

---

[374] OHM, op. cit., p. 1723-1730.

[375] Conforme Pfitzmann e Hansen: "A pseudonym is an identifier of a subject other than one of the subject's real names. […]. Pseudonymity is the use of pseudonyms as identifiers". Original em Inglês. Tradução livre: "Um pseudônimo é um identificador de um sujeito diferente de seu nome verdadeiro.[...]. Pseudonimização é o uso de pseudônimos como identificadores." (Idem, p. 21-22).

significativamente exacerbadas no meio digital em virtude do reduzido custo de reprodução existente nesse ambiente.

Assim, preocupados com o fato de a redução da privacidade de indivíduos ser capaz de gradativamente afetar o exercício de outras liberdades fundamentais, cientistas e engenheiros de computação passaram a propor e desenvolver medidas tecnológicas voltadas a reduzir o risco de exposição de dados pessoais a exposições indevidas ou ilegítimas. Contudo, a despeito de diversas iniciativas terem sido concebidas nesta seara, não chegaram a obter os resultados pretendidos. Dentre alguns dos diversos motivos apontados para isto, alguns pesquisadores apontaram indicaram que a proteção à privacidade não depende apenas da tecnologia em si, mas também de questões organizacionais relacionadas ao ambiente no qual é desenvolvida. Além disso, também se verificou que a ausência de adesão significativa por parte de agentes relevantes do mercado estaria vinculada ao fato de seu próprio modelo de negócios depender da coleta e tratamento de dados pessoais, sendo difícil que modificassem suas condutas sem a existência de incentivos institucionais para isso.

Buscando atender às particularidades deste cenário, passou-se a propor a adoção de abordagens mais holísticas, capazes de proporcionar não apenas a necessária proteção dos dados pessoais sob um viés tecnológico, mas também de induzir a tomada de medidas organizacionais que ampliassem a responsabilidade de instituições públicas e privadas durante todo o ciclo de utilização das informações de indivíduos. Denominadas de *privacy by design*, essas abordagens foram também o resultado da evolução normativa oriunda do extenso diálogo feito por agentes reguladores desde a década de 70.

Por certo, os relatórios produzidos por comissões independentes encomendados por órgãos reguladores estadunidenses durante os debates que precederam a edição do *Privacy Act* em 1974 delinearam princípios fundamentais a serem observados quando da coleta e tratamento de dados pessoais. A partir do *Code of Fair Information Practices*, autoridades da OCDE e, posteriormente, do Conselho da Europa, elaboraram instrumentos jurídicos voltados a estimular a padronização das metodologias existentes para proteção da privacidade no âmbito do fluxo transfronteiriço de dados pessoais. Com isso, buscavam ao mesmo tempo estimular o crescimento de um setor econômico estratégico e evitar que a incompatibilidade regulatória entre seus países membros prejudicasse os esforços de integração econômica e expansão do comércio internacional.

Neste contexto de esforços de uniformização normativa, foi a União Europeia quem afinal estabeleceu os diplomas mais influentes no que diz respeito à disseminação do *privacy by design*. Inicialmente, por meio da Diretiva 46, publicada em 1995, a comunidade de países europeu buscou estabelecer um robusto arcabouço jurídico voltado a uniformizar a proteção dos dados pessoais. Muito embora este primeiro diploma não contivesse menções expressas ao *privacy by design* em si, já havia o reconhecimento a respeito da importância da tomada de medidas técnicas e organizacionais tanto na fase de concepção do sistema quanto durante a coleta e processamento de dados.

Não obstante tenha sido um ponto importante no panorama jurídico da proteção de dados pessoais, a Diretiva 46 rapidamente tornou-se ultrapassada. Em 1995, quando foi editada, a internet ainda estava em sua infância. Além disso, tecnologias hoje corriqueiras como *smartphones*, banda larga, redes sociais, serviços de *streaming*, entre outros também sequer seriam concebíveis para o legislador da época. Em razão deste vácuo normativo, os esforços isolados em regulamentar estas novas questões por diferentes países estava gradativamente transformando o cenário regulatório europeu em uma colcha de retalhos, o que efetivamente prejudicava os esforços de integração do mercado comum. Como forma de resolver esta crescente insegurança jurídica e incentivar outros países fora do bloco a adotar seus padrões normativos, a União Europeia promoveu um extenso debate de reforma de seu arcabouço jurídico de proteção de dados. Finalmente, deste processo legislativo acabou resultando a edição, em 2016, do *General Data Protection Regulation*, o qual até o momento da redação deste texto é provavelmente o mais robusto e influente instrumento jurídico destinado à proteção da privacidade de indivíduos e seus dados pessoais.

Fruto do amadurecimento das discussões sobre o assunto não apenas no âmbito do espaço acadêmico, mas também de setores públicos e privados, o GDPR buscou implementar mecanismos que incentivassem a proteção de dados pessoais durante todo o ciclo de vida de uma tecnologia de informação e comunicação. Deste modo, a partir de seu artigo 25, intitulado *data protection by design and by default*, delineou obrigações de implementação de medidas técnicas e organizacionais para salvaguarda das informações coletadas e tratadas por sistemas eletrônicos.

Devido à importância de assegurar uma neutralidade tecnológica capaz de manter a proteção dos dados mais ampla o possível e menos suscetível ao constante cenário de mudanças tecnológicas, o legislador europeu evitou delimitar um conceito legal expresso sobre o que seria o *privacy by design* – ou, na denominação que utilizou – *data protection by design*. Em virtude

disso, adotou como estratégia apenas desenhar uma estrutura regulatória capaz de assegurar um quadro normativo a ser posteriormente desenhado pelas autoridades de proteção de dados nacionais e uniformizado pelos mecanismos de harmonização internacional também criados pelo GDPR. Igualmente, a ausência de uma definição legal mais clara também buscou conferir maior margem de atuação para os agentes privados envolvidos no desenvolvimento de tecnologias voltadas à coleta e ao tratamento de dados pessoais.

Por força destas questões, bem como pelo fato do texto do GDPR ainda possuir pouco tempo desde o seu início de vigência, o *European Data Protection Supervisor* preferiu também evitar apresentar um conceito delimitado, optando no lugar por descrever quatro "dimensões" do *privacy by design* que, juntas, se descreveriam as exigências normativas do diploma. De início, a primeira dimensão estaria vinculada à fase da concepção do projeto da tecnologia de informação e comunicação, sendo necessário que esta etapa identifique e inclua dentro de todo o ciclo de vida do sistema a proteção de indivíduos e seus dados pessoais. Na sequência, a segunda dimensão estaria relacionada à identificação dos riscos da coleta e tratamento realizados pelo sistema eletrônico, sendo relevante que os agentes por ele responsáveis levem em conta a evolução tecnológica no setor. Além disso, é necessário que sejam avaliados os riscos organizacionais existentes, identificando-se cada ponto da organização no qual as informações pessoais possam estar expostas a vazamentos ou utilizações indevidas. Em seguida, a terceira dimensão diria respeito ao estabelecimento de medidas tecnológicas e organizacionais apropriadas e efetivas, capazes de assegurar não só o cumprimento da legislação vigente quanto a real internalização dos princípios gerais de proteção de dados pelos agentes responsáveis pelos sistemas eletrônicos desenvolvidos. Nesse sentido, mecanismos de certificação externos e independentes, estimulados pela legislação mais recente, são fundamentais para garantir que as ações tomadas pela organização são de fato confiáveis e aptas a produzir os resultados desejados. Finalmente, a quarta dimensão seria pertinente à integração das medidas planejadas na organização e, em especial, no projeto do sistema eletrônico. Nesta senda, a despeito de existirem diversas metodologias e estratégias para a proteção de dados pessoais durante a coleta e o tratamento, observou-se que legisladores têm escolhido prever expressamente a minimização de dados e a pseudonimização nos diplomas mais recentes.

Como se pode perceber desta seção **3**, o propósito do *privacy by design* é estimular a criação de um ambiente no qual seja possível aos cidadãos efetivamente confiar em tecnologias de informação e comunicação que, cada vez mais, coletam e tratam cotidianamente seus dados pessoais. Nesse sentido, todas as dimensões referidas na subseção **3.3** têm também como plano

de fundo o aprimoramento da transparência da utilização das informações de indivíduos, quer sob a ótica tecnológica ou sob viés organizacional. Assim sendo, a seção **4** a seguir buscará justamente aprofundar o estudo da transparência aplicada ao contexto de algoritmos computacionais, de forma a compreender de que maneira ela se encaixa no âmbito da proteção da privacidade.

4 O INSTITUTO DO *PRIVACY BY DESIGN* E A TRANSPARÊNCIA APLICADA A ALGORITMOS COMPUTACIONAIS: DELIMITAÇÃO, APLICAÇÃO E LIMITES

Em 2012, uma série de reportagens publicadas pelo *The Wall Street Journal* a respeito de práticas comerciais de portais de comércio eletrônico receberam bastante atenção e causaram indignação entre leitores[376]. Buscando verificar se essas plataformas efetivamente ofereciam, conforme prometido, os melhores preços aos consumidores, jornalistas realizaram uma série de testes em sites conhecidos, dentre eles o da empresa multinacional *Staples*, conhecida por ser uma das maiores do ramo de venda de materiais de escritório. Para a surpresa dos repórteres, os preços oferecidos pelo mesmo produto poderiam mudar a depender da localização física de onde o cliente acessava o site. Examinando mais detidamente, chegaram à seguinte hipótese: o algoritmo estaria configurado para reduzir os valores para aqueles consumidores que residissem próximo de lojas concorrentes.

Todavia o que a princípio aparentava ser uma estratégia comercial razoável e extremamente comum no comércio varejista físico, tinha uma consequência eticamente questionável quando transposta para o comércio digital: pessoas que residiam em locais mais pobres, com menos comércios locais, acabavam recebendo ofertas de preços mais caros, a despeito de acessarem o mesmo link para verificar o produto. Após contato pelo jornal e reação negativa da população, a *Staples* informou que modificou seu algoritmo para evitar prejudicar pessoas em locais demograficamente mais pobres, corrigindo, em tese, o problema. Não obstante, alguns consumidores ainda apresentavam reclamações de que o site da empresa continuava a apresentar o mesmo comportamento.

Não é só no setor privado que existem controvérsias e discussões quanto a utilização de novas tecnologias para o tratamento de informações. De acordo com levantamentos mundiais sobre o tema, os EUA possuem a maior população carcerária em termos absolutos no mundo. Conforme dados publicados pelo Escritório das Nações Unidas sobre Drogas e Crime, em 2015 o número de presos do país era superior a dois milhões de pessoas, superando inclusive a

[376] DWOSKIN, Elizabeth. Why You Can't Trust You're Getting The Best Deal Online: A Study Finds Discriminatory Pricing On E-Commerce Sites Is More Widespread Than Thought. **The Wall Street Journal,** 23oct. 2012. Não paginado. VALENTINO-DEVRIES, Jennifer; SINGER-VINE, Jeremy; SALTANI, Ashkan. Websites Vary Prices, Deals Based on Users' Information. **The Wall Street Journal,** 24 dec. 2012. Não paginado.

República Popular da China e a Federação Russa[377], países com pontuação menor no Índice de Desenvolvimento Humano e no Índice de Liberdade Econômica[378]. Assim, diante do elevado custo para manutenção de um sistema prisional deste tamanho, diversos estados estadunidenses passaram a investir em tecnologias de informação e comunicação voltadas a aprimorar a tomada de decisões por magistrados. Dentre esses sistemas eletrônicos, o *Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)*[379], desenvolvido por uma entidade privada com fins lucrativos, é utilizado por juízes para auxiliar na definição de um perfil de risco de reincidência e, assim, facilitar a decisão quanto à dosimetria da pena. Além deste ganho de eficiência, a adoção do *COMPAS* também foi defendida como sendo uma ferramenta que, em tese, reduziria vieses sociais negativos inerentes à pessoa do juiz, tais como preconceitos sobre gênero e raça[380], este último particularmente sensível nos EUA.

Entretanto, a utilização do *COMPAS* não é isenta de controvérsias, existindo diversos casos de questionamentos[381], inclusive judiciais, a seu respeito. Em 2013, Eric Loomis foi preso nos EUA por duas acusações: tentar fugir de autoridades policiais e direção de veículo sem autorização do dono. Em ambas as acusações, Loomis aceitou a oferta da promotoria e se declarou culpado. Tendo em vista as circunstâncias do caso e o baixo grau de ofensividade das condutas, em princípio Loomis não estaria sujeito à pena de reclusão. Porém, em sua decisão, o juiz do caso listou, dentre outros fatores, que o *COMPAS* indicou que Loomis teria um alto risco de reincidência. Assim, condenou-o a uma elevada pena de 11 anos, sendo seis anos em reclusão e cinco anos de liberdade condicional. Tendo em vista que o *COMPAS* não informa a maneira como chegou às conclusões quanto ao risco do agente, os defensores de Loomis entenderam que isso violaria seu direito ao devido processo legal e, deste modo, recorreram até a Suprema Corte estadunidense. Esta, por sua vez, infelizmente se recusou a examinar o caso[382], prevalecendo a decisão da Suprema Corte do Estado de Wisconsin, a qual embora tenha

---

[377] UNITED NATIONS. **Total Prison Population.** New York: United Nations Office on Drugs and Crime, 2015. Não paginado.
[378] THE HERITAGE FOUNDATION. **2019 Index of Economic Freedom.** Washington D.C.: The Heritage Foundation, 2019.
[379] Sigla original em Inglês. Tradução livre: "Administração de Perfis de Criminosos Presos para Sanções Alternativas".
[380] ISRANI, Ellora Thadaney. When an Algorithm Helps Send you to Prison. **New York Times**, 26 out. 2017. Não Paginado. Sobre a existência de indícios de que fatores raciais poderiam afetar decisões judiciais, vide, por exemplo: ABRAMS, S. David; BERTRAND, Mariane; MULLAINATHAN, Sendhil. Do Judges Vary in Their Treatment of Race? **The Journal of Legal Studies,** v. 41, n. 2, p. 347-384, jun. 2012. p. 376-377.
[381] Nesse sentido: ANGWIN, Julia *et alli*. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. **Pro Publica**, 23 may. 2016. Não paginado. LARSON, Jeff *et alli*. How We Analyzed the COMPAS Recidivism Algorithm. **Pro Publica**, 23 may. 2016. Não paginado.
[382] UNITED STATES OF AMERICA. SUPREME COURT. **Loomis v. Wisconsin.** Washington: United States Supreme Court, 2017. Não paginado.

expressado preocupação com a utilização de análises de riscos produzidas por sistemas eletrônicos, reputou que a condenação não se baseou *exclusivamente* nas informações fornecidas pelo *COMPAS*[383].

Conforme se verifica dos dois casos narrados, o acesso a informações sobre o funcionamento dos algoritmos computacionais utilizados foi um dos pontos centrais dos questionamentos sobre a legitimidade de seu uso. Cada vez mais, questões importantes do cotidiano são definidas por processos computacionais definidos como "caixas pretas" cujo funcionamento ou estrutura são desconhecidos pelo público em geral[384]. Por outro lado, tendo em vista que um dos princípios para a utilização legítima de dados pessoais é a sua utilização acordo com a finalidade para a qual foi originalmente coletada, a discussão sobre a transparência acaba se tornando especialmente importante no âmbito da proteção dos dados pessoais e privacidade de indivíduos afetados pelo tratamento.

Com efeito, ao estudar a capacidade regulatória da arquitetura de tecnologias de informação e comunicação, Lawrence Lessig já chamava a atenção sobre o importante papel que a transparência desempenharia neste novo momento da história. Por certo, tendo em vista que códigos de computador nada mais são do que o produto deliberado de um processo de desenvolvimento, este autor postulou que a possibilidade e capacidade de compreender o seu funcionamento poderia acabar por ser um instrumento relevante na defesa de direitos e proteção contra abusos pelos desenvolvedores[385]. Em outros termos, é necessário ter informações para poder efetivamente entender o funcionamento da tecnologia e, assim, deliberar sobre sua regulação.

Somado ao crescente avanço tecnológico que demanda dados para o seu funcionamento, este alerta doutrinário parece indicar que o tema merece maior atenção por parte de juristas brasileiros, particularmente diante da escassez de estudos sobre esta área. Em virtude disso, a presente seção **4** terá como objetivo aprofundar-se na questão da transparência e sua relação com o *privacy by design*. Assim, em primeiro lugar, a subseção **4.1** buscará examinar o conceito de transparência e localizá-lo no âmbito do *privacy by design*, demonstrando, em especial, onde se encontra nos diplomas mais relevantes sobre proteção de dados para os fins deste trabalho. Em seguida, a subseção **4.2** estudará as técnicas aplicáveis para conferir transparência a

---

[383] HARVARD LAW REVIEW. State v. Loomis: Wisconsin Supreme Court Require Warning Before Use of Algorithmic Risks Assessments in Sentencing. **Harvard Law Review**, n. 130, p. 1530-1537. 2017.
[384] WIENER, Norbert. **Cybernetics:** or control and communication in the animal and the machine. 2 ed. Cambridge: The MIT Press, 1965. p. xi.
[385] LESSIG, op. cit., 2006. p. 140-141.

algoritmos computacionais, em particular seus alcances e limites, de forma a entender até onde seria possível chegar com a sua aplicação, em particular no que diz respeito às medidas de disponibilização aberta do código-fonte e da explicação da decisão algoritmica. Por fim, a subseção **4.3** terá como finalidade avaliar a aplicação da transparência no contexto da coleta e tratamento de dados pessoais, descrevendo as possíveis maneiras com que este princípio se encaixa neste cenário.

4.1 DO CONCEITO DE TRANSPARÊNCIA E SUA LOCALIZAÇÃO NO ÂMBITO DO *PRIVACY BY DESIGN*

De fato, sob o ponto de vista político, a capacidade e/ou possibilidade de conhecer a conduta dos demais membros da comunidade é considerada como um fator essencial para tornar responsável perante a comunidade um indivíduo que desempenha um comportamento contrário àquilo que os demais agentes entendem como razoável e esperável[386]. Essa circunstância pode ser também compreendida sob um viés econômico, já que a transparência, ao proporcionar uma redução da assimetria informacional ocasionada pelo aumento de informações disponíveis tende a gerar uma melhoria na confiança entre os agentes envolvidos, sejam eles públicos ou privados [387]. Em resumo, ao permitir conhecer os detalhes de produção, elaboração e interpretação de uma determinada informação, a transparência funciona como um fator capaz de induzir comportamentos éticos de indivíduos ou organizações[388].

Por certo, essa correlação entre conhecimento e poder[389] ajuda a compreender o motivo pelo qual Louis Brandeis, um dos autores do artigo seminal *Right to Privacy*, também desenvolveu importantes trabalhos na área da transparência e acesso à informação, sendo dele a célebre frase "a publicidade é com razão recomendada como remédio para doenças sociais e industriais. A luz solar é considerada como sendo o melhor dos desinfetantes"[390]. Escrita no

---

[386] GOSSERIES, Axel; PARR, Tom. Publicity. **The Stanford Encyclopedia of Philosophy.** Stanford: Stanford University, 2018. Não paginado.
[387] AKERLOF, George A. The Market for "Lemons": Quality Uncertain and the Market Mechanism. **The Quarterly Journal of Economics**, v. 84, n. 3, p. 488-500, ago. 1970. p. 500.
[388] TURILLI, Matteo; FLORIDI, Luciano. The Ethics of Information Transparency. **Ethics and Information Technology,** v. 11, n. 2, p. 105-112, jun. 2009. p. 110.
[389] STIGLER, George J. The Economics of Information. **The Journal of Political Economy**, v. 69, n. 3, p. 213-225, jun. 1961. p. 213.
[390] Tradução livre. Original em Inglês: "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants […]" (BRANDEIS, Louis. **Other People's Money and How Bankers Use it.** New York: Frederick Stokes, 1914. Não paginado).

contexto de uma obra acerca do abuso de poder por grandes instituições financeiras, Brandeis postulava a tomada de medidas regulatórias que tornassem disponíveis aos investidores mais informações a respeito do funcionamento dos bancos e seus serviços. Com isso, acreditava que os agentes de mercado teriam melhores condições de realizar escolhas informadas e, assim, coibir instituições que oferecessem serviços ou tarifas injustas ou abusivas[391]. Tendo em vista a crescente capacidade regulatória de arquiteturas de tecnologias de informação e comunicação, não é particularmente surpreendente que o princípio da transparência tenha sido incluído desde cedo em propostas regulatórias sobre o setor como um dos requisitos a serem observados no desenvolvimento e operação de sistemas eletrônicos que coletam ou tratam dados pessoais.

Em um dos primeiros trabalhos promovidos por entes estatais sobre o tema, realizado pelo governo federal estadunidense em 1973 e que resultou no *Code of Fair Information Practices*, a transparência já era considerada um elemento essencial para o tratamento de informações pessoais. Com efeito, o relatório da comissão coordenada por Willis Ware recomendou que, no que diz respeito à transparência, além de não ser legítima a existência de sistemas eletrônicos que tratem dados pessoais secretamente, o indivíduo também deveria ter o direito de saber quais informações sobre seu respeito estão armazenadas e como estão sendo utilizadas[392]. Deste modo, sugeriu que toda organização que realizasse o tratamento de dados pessoais tivesse uma política institucional que permitisse aos titulares de dados pessoais ter acesso às seguintes informações mínimas[393]: a) o nome do sistema; b) a natureza e propósito do sistema; c) a categoria e o número de pessoas cujos dados são mantidos; d) as categorias de dados armazenados; e) as regras e práticas da organização relacionadas à manutenção dos dados, duração do armazenamento e eliminação destes dados; f) as categorias de fontes dos dados; g) a descrição de todos os tipos de usos dos dados, h) os procedimentos pelos quais o titular pode utilizar para obter acesso aos seus dados e contestá-los; i) o cargo, o nome e o endereço da pessoa imediatamente responsável pelo sistema.

Inegavelmente, tendo em vista a época e o contexto em que foram editadas, pode-se dizer que o conjunto de informações elencadas por Willis Ware e seus colegas até os dias de hoje é

---

[391] Idem.

[392] UNITED STATES OF AMERICA. Department of Health, Education and Welfare. **Records, Computers, and the Rights of Citizens.** Washington: DHEW, 1973. p. xxiii.

[393] Idem, p. xxv-xxvi. Exemplo ilustrativo da influência do relatório do DHEW pode ser verificado na primeira versão do projeto, apresentado em 1990 perante o Conselho das Comunidades Europeias, que veio se tornar posteriormente a Diretiva 46/95 (EUROPEAN UNION. Council of the European Communities. **Proposal For A Council Directive Concerning The Protection Of Individuals In Relation To The Processing Of Personal Data.** Brussels: European Union, 1990. Não paginado).

de interesse dos indivíduos cujos dados pessoais são tratados por sistemas eletrônicos[394]. Por certo, a noção de que o titular de dados pessoais deve poder ter condições de conhecer a forma como se dá o tratamento de suas informações apenas passou a ter um delineamento melhor a partir desses primeiros estudos. Desde então, o acesso à informação sobre tratamento de dados pelo próprio titular passou a despontar como um elemento básico de medidas regulatórias estabelecidas por diplomas de diversos países.

Fato ilustrativo dessa importância dada à transparência no âmbito da proteção da privacidade pode ser localizado nos trabalhos desenvolvidos a respeito do *privacy by design.* Com efeito, ao listar os princípios fundamentais deste conjunto de metodologias voltados a influenciar o desenvolvimento e gerenciamento de tecnologias de informação e comunicação, Ann Cavoukian também incluiu a transparência como um dos requisitos para a administração das informações pessoais de indivíduos. Conforme a autora, este princípio significaria que os componentes tecnológicos e organizacionais de todo o funcionamento de uma operação de coleta e tratamento de dados devem permanecer visíveis tanto aos responsáveis pelo serviço quanto aos seus usuários ou público-alvo. A partir disso, considerava que seria possível iniciar o estabelecimento de uma relação de confiança entre as partes pois a disponibilidade informacional permitiria ao titular de dados eventualmente interessado conferir a veracidade da conduta alegada pela organização.

Numa tentativa de descrever a importância da disponibilidade de informações sobre a coleta e tratamento de dados no *privacy by design*, Cavoukian sintetiza a aplicação de transparência por meio famosa frase utilizada por Ronald Reagan: "trust, but verify"[395]. Em outros termos, compete aos mecanismos de governança do *privacy by design* não só garantir a confiança nos sistemas eletrônicos, mas também permitir a sua auditabilidade.

Sob o ponto de vista da produção de atos normativos, apesar de diversos aspectos listados no primeiro relatório sobre o tema terem sofrido modificações em razão de alterações de contexto ocasionadas pelo avanço tecnológico, muitas das reflexões acerca da transparência na coleta e no tratamento de dados identificadas na legislação mais recente encontram sua inspiração no conjunto de recomendações formulado pela comissão do Departamento de Saúde,

---

[394] MULLIGAN, Deirdre K. The Enduring Importance of Privacy. **IEEE Security & Privacy,** v. 12, n. 3, p. 61-65, mai./jun. 2014. p. 65

[395] Original em Inglês. Tradução livre "confie, mas verifique" (CAVOUKIAN, Ann. **Privacy by Design in Law, Policy and Practice:** a White Paper for Regulators, Decision-Makers and Policy-makes. Ontario: Information and Privacy Commissioner: 2011. p. 29). Historicamente, esta frase, de origem russa (*Doveryai, no proveryai*), foi utilizada em várias oportunidades por Ronald Reagan no contexto das negociações de acordos de desarmamento nuclear com a União Soviética.

Educação e Bem-Estar do governo federal estadunidense. Nesse sentido, por exemplo, é possível constatar a influência do *Code of Fair Information Practices* no texto das Diretrizes da OCDE, cuja primeira versão foi publicada em 1980[396], e na Convenção 108 do Conselho da Europa[397], editada em 1981, as quais também buscam incluir mecanismos de abertura e disponibilização de informações sobre a coleta ou tratamento de dados pessoais ao seu respectivo titular.

Além destes dois diplomas, a noção de transparência enquanto possibilidade de acesso pelo titular de dados a informações relacionadas ao funcionamento e à organização institucional da pessoa jurídica responsável pela coleta ou tratamento foi igualmente importante para o avanço de normas de proteção de dados que exigissem uma maior responsabilização destes agentes[398]. No plano europeu, instrumentos jurídicos mais robustos destinados à proteção da privacidade, tais como a Diretiva 46/95 e, posteriormente, o GDPR possuem previsões normativas quanto ao assunto, possibilitando que o conhecimento das práticas de coleta e tratamento seja utilizado instrumentalmente pelo titular de dados para exercer outros direitos. Definitivamente, sem o acesso a estas informações básicas, outros direitos relacionados ao âmbito da coleta e tratamento de dados pessoais, a exemplo da limitação de finalidade, proibição de tratamento, retificação ou eliminação de dados o mesmo ou direito à indenização por eventuais abusos não seriam operacionalizáveis.

Entretanto, a evolução tecnológica trouxe novas questões a serem avaliadas no âmbito da proteção de dados pessoais. Com efeito, apesar do crescimento da capacidade de processamento de dados até a década 90 ter suscitado debates intensos e acarretado o surgimento de diversos diplomas quanto ao tema, a expansão da rede mundial de computadores modificou diversas das

---

[396] De acordo com as diretrizes, o princípio da transparência significaria que "There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller." Original em Inglês. Tradução livre: "Deve existir uma postura geral de transparência acerca dos acontecimentos, práticas e políticas com relação aos dados pessoais. Devem existir meios facilmente disponíveis para determinar a existência e natureza dos dados pessoais, suas principais finalidades de uso e a identidade e domicílio usual do controlador dos dados" (ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Recommendation of The Council Concerning Guidelines Governing the Protection Of Privacy And Transborder Flows Of Personal Data.** Paris: OECD, 1980. Não paginado).

[397] Principalmente em seu artigo 8º, o qual estabelece salvaguardas adicionais ao titular de dados (COUNCIL OF EUROPE. **Convention 108**: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg: Council of Europe, 1981. Não paginado).

[398] EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 5/2018:** Preliminary Opinion on Privacy by Design. Brussels: EDPS, 2018. p. 13. Conforme o EDPS, "métodos padronizados para garantir e apoiar a transparência incluem o registro e comunicação, a documentação do processamento de dados ou a notificação do usuário" (Idem). Tradução livre. Original em Inglês: "Standard methods for achieving or supporting transparency comprise logging and reporting, documentation of the data processing, or user notifications".

premissas do cenário regulatório. Neste contexto, embora já possível em certa medida anteriormente, o intercâmbio eletrônico de dados e informações se tornou algo corriqueiro e extremamente acessível não só a grandes organizações e conglomerados internacionais, mas também a pessoas comuns e pequenas empresas. Da mesma maneira, computadores individuais e, posteriormente, *smartphones* se tornaram cada vez mais populares e acessíveis. Por fim, novas plataformas eletrônicas, especialmente as redes sociais com centenas de milhões de usuários, aceleraram este processo de troca informacional ao facilitar e até mesmo incentivar o contato entre pessoas.

Em especial, o avanço tecnológico também trouxe mudanças no papel até então mais comumente desempenhado por computadores. De fato, o crescimento da capacidade computacional facilitou a criação de técnicas mais intricadas para a coleta e o processamento de informações. Com o desenvolvimento de algoritmos de computador mais complexos, as máquinas deixaram de ser simples repositórios de informações coletadas por humanos para passar a realizar automaticamente a coleta e o tratamento das informações pessoais cada vez mais disponíveis na internet ou em bancos de dados públicos e privados nela conectados. Longe de serem algo de utilização restrita por um pequeno número de entidades, atualmente cada vez mais se disseminam aplicações que utilizam inteligência artificial tanto para realizar ações que antes eram realizadas manualmente quanto para desenvolver operações cuja realização "manual" simplesmente não seria possível em virtude do esforço massivo necessário.

Contudo, este processo de automatização da tomada de decisões com base em dados pessoais, apesar de acarretar impactos significativos para a eficiência do processo de deliberação, também trouxe efeitos negativos. Realmente, embora a redução ou eliminação do ser humano possa tornar mais rápido o fluxo de informações, as consequências de uma decisão ruim tomada automaticamente também são sentidas de forma mais rápida. Certamente, seres humanos não são oniscientes ou capazes de levar em consideração rigorosa todos os fatores envolvidos numa determinada escolha. Porém, com exceção de casos específicos de algoritmos mais complexos e de difícil desenvolvimento, diversos sistemas eletrônicos utilizados no cotidiano simplesmente não são capazes de incluir novos dados ou realizar novas operações em seu funcionamento se não forem expressamente configurados para isso. Essa situação também faz com que decisões baseadas em algoritmos com erros produzam efeitos – e gerem danos – mais rapidamente do que a decisão de um ser humano potencialmente acarretaria.

Além disso, em razão de serem frutos de um processo de desenvolvimento levado a cabo por um ou mais desenvolvedores humanos, algoritmos computacionais também reproduzem,

de forma deliberada ou não, os vieses cognitivos e sociais de seus criadores. Decorrentes de diversas fontes, tais como origem ou metodologia de coleta dos dados[399], da implementação do código ou mesmo da lógica de programação em si, estes vieses podem gerar impactos profundos nos direitos dos seus usuários ou público-alvo. De fato, com o crescente avanço de decisões automatizadas e programas sofisticados, ganhou força o temor de que o peso dado a estes mecanismos se torne grande demais ao mesmo tempo em que a responsabilidade humana nestes processos se torne reduzida[400]. Conforme exposto no início desta seção **4** durante o relato do caso envolvendo a plataforma da empresa Staples, mesmo condutas ou práticas comerciais legítimas e razoáveis num cenário "analógico" não podem ser realizadas com a mesma segurança e tranquilidade no mundo digital sem que seja feita a devida análise e reflexão sobre suas consequências.

Perante estas circunstâncias, estudiosos e reguladores passaram a se preocupar não só com aspectos preponderantemente organizacionais da proteção da privacidade, mas também com o funcionamento intrínseco dos sistemas eletrônicos em si. Dito de outra forma, o próprio algoritmo ou lógica computacional responsável pela operação da tecnologia de informação e comunicação, particularmente nos casos de funcionamento automatizado, passou a ser objeto direto e expresso de regulação.

Assim, no âmbito da União Europeia, a Diretiva 46/95 pode ser considerada como sendo um dos primeiros diplomas a expressamente abordar a questão da proteção da privacidade no que diz respeito à lógica de programação do sistema eletrônico envolvido no tratamento de dados pessoais. Nesta senda, buscou estabelecer a obrigação para os estados-membros de incluir em suas legislações nacionais, dentre as diversas garantias conferidas ao titular de dados, o acesso às informações sobre o processamento em si, nestes termos[401]:

---

[399] BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review**, v. 104, p. 671-732, 2016. p. 680-693.

[400] EUROPEAN UNION. Commission of the European Communities. **Amended Proposal for a Council Directive:** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Brussels: Commission of the European Communities, 1992. p. 26

[401] Original em Inglês. Tradução livre: "Artigo 12 – Direito de acesso [...] Os Estados-Membros deverão garantir a todos os titulares de dados pessoais o direito de obter do controlador: (a) livremente, em intervalos razoáveis e sem demora ou custos excessivos: [...] – o conhecimento da lógica envolvida em qualquer tratamento automatizado de dados a seu respeito, ao menos no caso das decisões automatizadas referidas no artigo 15 (1)" (EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Directive 95/46/EC:** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Luxembourg, 1995. Não paginado).

> ***Article 12 - Right of access*** *[...] Member States* ***shall guarantee*** *every data subject* ***the right to obtain from the controller****: (a) without constraint at reasonable intervals and without excessive delay or expense: [...] -* ***knowledge of the logic involved in any automatic processing of data concerning him*** *at least in the case of the automated decisions referred to in Article 15 (1);* (grifou-se)

Por sua vez, o artigo 15 (1) do mesmo diploma, ao abordar a questão relativa à realização de decisões automatizadas com base em dados pessoais e esclarecer a hipótese de cabimento do direito de acesso à lógica envolvida no processamento, refere que este se aplica quando as decisões produzirem efeitos legais contra o titular dos dados e sejam baseadas exclusivamente no tratamento automatizado. Nesse sentido, eis o texto do dispositivo[402]:

> ***Article 15 - Automated individual decisions*** *[...] 1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is* ***based solely on automated processing*** *of data* ***intended to evaluate certain personal aspects relating to him****, such as his performance at work, creditworthiness, reliability, conduct, etc.* (grifou-se)

Embora alguns diplomas de nações europeias contivessem previsões relacionadas ao tratamento automatizado de dados[403], a previsão expressa a respeito do direito de acesso à lógica do sistema em nível comunitário significou um considerável avanço na temática[404]. Todavia, a despeito disso a matéria recebeu pouca atenção por parte dos tribunais e órgãos responsáveis por sua fiscalização, o que resultou numa ausência de precedentes e evoluções mais notáveis durante quase uma década de sua vigência[405]. Dentre as diversas hipóteses existentes para

---

[402] Original em Inglês. Tradução livre: "Artigo 15 – Decisões individuais automatizadas [...] 1. Os Estados-Membros deverão garantir o direito a cada pessoa de não ser sujeita a uma decisão que produza efeitos legais a seu respeito ou que a afete significativamente e que seja baseada apenas no tratamento automatizado de dados com a finalidade de avaliar determinados aspectos pessoais a seu respeito, tais como seu desempenho no trabalho, avaliação de crédito, confiabilidade, conduta, etc" (EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Directive 95/46/EC:** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Luxembourg, 1995. Não paginado).

[403] Exemplificativamente, podem-se citar os casos da França (*Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), Espanha (*Ley organica 5/1992 de 29 de octubre 1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*) e Portugal (*Lei nº 10/91 de 12 de Abril 1991, da Protecção de Dados Pessoais face à Informática*).

[404] BYGRAVE, Lee. Minding the machine: art 15 of the EC Data Protection Directive and automated profiling. **Privacy Law and Policy Reporter**, v. 7, n. 4, 2000. Não paginado.

[405] EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: from a "Right to Explanation" to a "Right to Better Decisions"?. **IEEE Security & Privacy**, v. 16, n. 3, p. 46-54, may/jun, 2018. p. 2. WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, 2017.

compreender este pequeno desenvolvimento da matéria nos tribunais, é possível citar a ausência de incentivos econômicos favoráveis à realização de reclamações administrativas e ao ajuizamento de ações judiciais, bem como a complexidade da matéria e a baixa familiaridade da comunidade jurídica quanto a temas técnicos relacionados a tecnologias de informação.

O assunto recebeu nova atenção a partir do início das discussões legislativas relacionadas à substituição e atualização do marco jurídico europeu de proteção de dados. Em um processo desencadeado em 2012 pela Comissão Europeia que acabou culminando com a edição do GDPR em 2016 pelo Parlamento Europeu e pelo Conselho da União Europeia, a comunidade de países europeus buscou revisar todo o seu arcabouço normativo, inclusive no que diz respeito às garantias conferidas aos seus cidadãos quanto à transparência do tratamento de dados por sistemas eletrônicos. Deste modo, o novo diploma abordou inicialmente a questão em seu artigo 15, 1, (h), o qual refere que[406]:

> *1. **The data subject shall have the right to obtain from the controller** […] the following information: […] (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful information about the logic involved**, as well **as the significance** and **the envisaged consequences** of such processing for the data subject*. (grifou-se)

Realmente, o primeiro ponto no qual se pode apontar diferença entre o texto da diretiva e o do GDPR está na própria terminologia utilizada pelo novo marco legal. Com efeito, ao contrário da diretiva, cujo artigo 12 garantia ao titular simplesmente o direito obter do controlador o conhecimento da "lógica envolvida" no tratamento de dados, o GDPR foi além ao reconhecer o direito de ter acesso a "informações *úteis*[407] sobre a lógica envolvida", bem como à "importância e consequências previstas" do processamento.

---

p. 84-89. ZARSKY, Tal Z. Incompatible: The GDPR and the Age of Big Data. **Seton Hall Law Review**, v. 47, n. 4, p. 995-1020, 2017. p. 1016.

[406] Original em Inglês. Tradução livre: "1. O titular de dados deve ter o direito de obter do controlador [...] as seguintes informações: [...] (h) a existência de decisões automatizadas, incluindo a realização de perfis, referida no artigo 22 (1) e (4) e, ao menos nestes casos, informações úteis sobre a lógica envolvida, assim como a importância e as consequências previstas deste processamento para o titular de dados." (EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679:** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Brussels: European Union, 2016. Não paginado).

[407] Na tradução literal da Língua Inglesa, o termo "meaningful" pode ser traduzido diretamente como "significativa". Entretanto, a palavra não é utilizada no sentido mais comum como advérbio de intensidade, mas sim no sentido de "algo que possui significado ou sentido". Na tradução oficial feita para o Português de Portugal, o termo "meaningful" é traduzido como "útil", porém é necessário ressalvar que o conteúdo semântico da palavra naquele país não necessariamente coincide com o uso do Português "brasileiro". Para uma discussão sobre as

Dado à importância e ao alcance das discussões desenvolvidas quanto à questão no panorama da União Europeia, o texto do GDPR acabou novamente por impactar o processo legislativo brasileiro a respeito da proteção de dados. Nesse sentido, de forma semelhante ao legislador europeu, ao editar a Lei nº 13.079, de 14 de agosto de 2018, o Congresso Nacional também procurou regulamentar a matéria. Assim, ao tratar dos direitos do titular de dados, estabeleceu no art. 20, §1º a seguinte previsão[408] [409]:

> **Art. 20.** O titular dos dados tem **direito a solicitar a revisão de decisões** tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. **§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial**. (grifou-se)

A despeito do crescente número de inovações legais quanto ao acesso a informações sobre o tratamento de dados, a novidade do tema e a pouca experiência por parte de juristas acerca do problema da transparência de algoritmos computacionais desencadeou um novo debate quanto à extensão dos novos direitos e respectivos deveres legais a serem observados para assegurar o acesso à informação por parte dos titulares de dados. Por certo, tendo em vista que a matéria envolve não apenas conhecimento jurídico, mas também elementos técnicos oriundos da Ciência da Computação, é razoável e compreensível a relativa escassez de decisões administrativas ou judiciais quanto à temática, particularmente no cenário brasileiro. Deste modo, a seção **4.2** a seguir buscará apresentar e explicar as principais propostas apresentadas pela literatura a respeito da transparência de algoritmos computacionais, assim como as suas respectivas limitações. Antes de partir para a próxima seção, importante ressalvar dois pontos: **a)** a despeito de ser necessária a apresentação de conceitos técnicos, buscar-se-á sempre que possível manter uma linguagem acessível, de modo a facilitar a compreensão daqueles que eventualmente não estejam familiarizados com o assunto; **b)** embora seja necessário avaliar conceitos técnicos, o presente trabalho não possui condições de se aprofundar em questões

---

diferentes versões do texto do GDPR quanto ao assunto, vide: MALGIERI, Gianclaudio; COMANDÉ. Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 4, p. 243-265, nov. 2017. p. 257.

[408] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018.

[409] No momento de conclusão deste trabalho, ainda não havia sido editado qualquer regulamento referente ao dispositivo legal em questão.

intrinsecamente ligadas à Ciência da Computação, porquanto o objetivo deste texto é eminentemente jurídico.

4.2 DAS TÉCNICAS APLICÁVEIS PARA CONFERIR TRANSPARÊNCIA EM ALGORITMOS COMPUTACIONAIS: SEU ALCANCE E LIMITES

O relacionamento de agentes públicos com setores envolvendo alta tecnologia é certamente complexo e marcado por muita incompreensão, fato que acarreta constantes embates entre matérias tecnológicas e a regulação estatal, os quais ocasionalmente resultam em situações caricatas, mas preocupantes. Em 14 de julho de 2017, no curso dos extensos debates públicos envolvendo a extensão da proteção de informações pessoais por meio de técnicas matemáticas baseadas em criptografia, o Primeiro Ministro Australiano atraiu atenção da mídia em virtude de um comentário particularmente ilustrativo quanto ao desconhecimento existente na seara política sobre a questão. Na ocasião, perguntado por um jornalista sobre se a ingenuidade regulatória da Austrália não seria vencida pelas leis da matemática, o político respondeu enfaticamente que: "*The laws of Australia prevail in Australia, I can assure you of that, The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia*"[410]. Além de piadas, a fala do Primeiro Ministro Malcom Turnbull foi recebida por fortes críticas por parte da mídia[411] e da comunidade científica[412], as quais expressaram forte preocupação com decisões políticas tomadas com total desconhecimento de elementos técnicos essenciais da matéria. Verdadeiramente, tendo em vista que também exige conhecimentos técnicos, a transparência de algoritmos computacionais também corre a mesma espécie de risco de incompreensão.

Desde que passou a receber maior atenção, o problema da transparência de sistemas eletrônicos de informação e comunicação tem sido abordado de diversas maneiras por estudiosos preocupados em assegurar que estas tecnologias sejam efetivamente confiáveis para a utilização da sociedade. Todavia, conquanto muitas destas propostas tenham recebido até

---

[410] Original em Inglês. Tradução livre: "As leis da Austrália irão prevalecer na Austrália, Eu posso lhe assegurar disso. As leis da matemática são muito elogiáveis, mas a única Lei que se aplica na Austrália é a Lei da Austrália" (DUCKET, Chris; BARBASCHOW, Asha. The laws of Australia will trump the laws of mathematics: Turnbull. **ZDNET,** 14 jul. 2017. Não paginado).

[411] VILLASENOR, John. Techtank: No the Laws of Australia don't override the Laws of Mathematics. **Brookings.** 17 jul. 2017. Não paginado.

[412] INSTITUTE OF ELECTRIC AND ELECTRONIC ENGINEERS. **IEEE Position Statement:** In Support of Strong Encryption. Piscataway: IEEE Board of Directors, 2018. p. 1

mesmo a adesão e apoio de agentes reguladores, a extensão em que podem ser utilizadas não é ilimitada, existindo uma série de limites para a sua aplicabilidade[413]. Desta forma, serão descritas a seguir as principais técnicas apresentadas e suas respectivas limitações, principalmente aquelas limitações tecnológicas cuja compreensão se entende por necessária mesmo para operadores do Direito buscando auxiliar no processo de aproximação do vocabulário entre as Ciências Jurídicas e a Ciência da Computação[414].

4.2.1 Disponibilização aberta do código-fonte

Seres humanos possuem diversas formas para se comunicar, sendo que cada uma dessas linguagens naturais possui diversas variações de acordo com o contexto geográfico, cultural e social de onde se encontram. Ao contrário dos seres humanos que são capazes de compreender informações pelo contexto, computadores não possuem essa capacidade, requerendo que todas as etapas de uma determinada ação sejam escritas de forma logicamente coerente e absolutamente precisa e definida. Ressalvados casos experimentais e de uso não-comercial, na atualidade os computadores eletrônicos utilizam linguagem binária para compreender os comandos informados por seu usuário, convertendo um conjunto de "0"s e "1"s em impulsos elétricos que serão executados pela parte física (o *hardware*) do computador.

Nos primórdios da Ciência da Computação, entre a década de 1930 até 1950, os programadores que desejassem que o computador executasse alguma tarefa precisavam escrever os códigos desses comandos diretamente em *linguagem de máquina*, isto é, utilizando-se um conjunto de "0"s e "1"s[415]. Deste modo, a simples expressão "linguagem de máquina" escrita na modalidade de código binário desenvolvida pela *American National Standards Institute* pode ser descrita da seguinte maneira[416]:

---

[413] BOOCH, op. cit., 2003. Não paginado.
[414] CHACON, op. cit., 2018, p. 97.
[415] FOROUZAN, Behrouz; MOSHARRAF, Firouz. **Fundamentos da Ciência da Computação.** 2 ed. São Paulo: Cengage Learning, 2011. p. 215-216.
[416] Trata-se de uma entidade que desempenha as mesmas atividades de normalização que a Associação Brasileira de Normas Técnicas.

01101100 01101001 01101110 01100111 01110101 01100001 01100111 01100101
01101101 00100000 01100100 01100101 00100000 01101101 11000011 10100001
01110001 01110101 01101001 01101110 01100001

Todavia, além de cansativo, escrever em linguagem binária torna difícil a identificação de eventuais erros no código escrito, o que gera problemas de escalabilidade para o desenvolvimento de *softwares*. Assim, a partir da década de 1950, cientistas da computação desenvolveram linguagens de programação capazes de serem compreendidas mais facilmente por humanos e, assim, tornar mais eficiente o processo de desenvolvimento. Desta maneira, desenvolvedores passaram a escrever nas chamadas de *linguagens de alto nível*[417] os *códigos-fontes* de seus programas os quais são traduzidos em linguagem binária para serem executados pelo computador[418]. Exemplificativamente, na linguagem de programação *Java* um programa que simplesmente apresente a mensagem "Bom dia" quando executado teria este código-fonte[419]:

```
class BomDia
{
    public static void main(String args[])
    {
        System.out.println("Bom dia ");
    }
}
```

No âmbito do desenvolvimento de *softwares*, existem basicamente duas principais metodologias utilizadas quanto à possibilidade de acesso o teor do código-fonte por terceiros[420]: **a)** o desenvolvimento e disponibilização de código *fechado*, no qual o acesso é restrito apenas àqueles aos quais o próprio desenvolvedor autorizar; **b)** o desenvolvimento e disponibilização de código *aberto*, no qual qualquer interessado pode acessar o seu teor[421], preferencialmente

[417] FOROUZAN; MOSHARRAF, op. cit, p. 217.
[418] Idem.
[419] O código-fonte colacionado abaixo é de produção do autor. Tendo em vista que as normas da ABNT, em especial a NBR 14724, não possuem atualmente um padrão para a exposição de códigos-fontes, optou-se por utilizar o padrão de notação utilizado pela Oracle, mantenedora da plataforma e da linguagem Java (ORACLE. **Java Platform Standard Edition Technical Documentation**. [s.l.]: Oracle, 2019. Não paginado).
[420] HANSEN, Marit; KÖHNTOPP, Kristian; PFITZMANN, Andreas. The Open Source Approach: opportunities and limitations with respect to security and privacy. **Computers & Security**, v. 21, n. 5, p. 461-471, 2002. p. 462.
[421] Numa definição mais complexa, a *Open Source Initiative*, uma das mais importantes organizações dedicadas à promoção de código aberto e software livre, defende que apenas pode ser considerado "aberto" o código que, além de ser acessível, cumpra uma série de requisitos cuja finalidade, em síntese, está em permitir a sua redistribuição,

pela internet[422]. Escolher qual metodologia será utilizada no processo de desenvolvimento não é algo trivial, existindo diversas consequências a serem consideradas pelo responsável do *software* para chegar a uma conclusão quanto ao tema[423].

No que diz respeito à prevenção e à correção de problemas gerais de programas de computador, muitos especialistas defendem que a transparência proporcionada pela metodologia de desenvolvimento em código *aberto* garantiria a produção de *softwares* mais seguros e mais capazes de proteger a privacidade de seus usuários[424]. Sinteticamente, a filosofia por trás dessa defesa é descrita pela seguinte frase, chamada de "Lei de Linus": "*Given enough eyeballs, all bugs are shallow"*[425], ou seja, quanto mais pessoas possuem acesso ao código, mais simples e rápida será a localização e resolução de problemas (ou chamados de "*bugs*" na área de tecnologia da informação) no programa[426]. Portanto, haveria uma maior confiança dos usuários em programas com código-fonte aberto já que este teria a potencial garantia de ter passado pelo escrutínio de centenas ou milhares desenvolvedores, de forma voluntária[427] ou mesmo mediante eventuais recompensas, algo difícil de ser produzido senão por grandes corporações multinacionais. Todavia, existem diversas razões pelas quais códigos-fontes abertos não são necessariamente uma panaceia para os problemas relacionados à arquitetura de tecnologias de informação e comunicação.

A **primeira** razão é eminentemente econômica: com exceção das poucas pessoas com conhecimento[428] e tempo livre para desenvolver os programas que precisa por conta própria, na

---

modificação e livre utilização (OPEN SOURCE INIATIATIVE. **The Open Source Definition.** S.l.: OSI, 2007. Não paginado).

[422] Diversas plataformas eletrônicas existem para divulgação aberta do código-fonte, tais como o Github e Gitlab.

[423] Para uma análise mais detida sobre as implicações legais da adoção de *softwares* de código aberto, vide, exemplificativamente: MCGOWAN, David. Legal Implications of Open-Source Software. **University of Illinois Law Review**, v. 2001, n. 1, p. 241-304, 2001.

[424] Entre outros: Idem, p. 469. LESSIG, op. cit., 2006, p. 142-143. GARFINKEL, Simson *et alli*. Toward Algorithmic Transparency and Accountability. **Communications of the ACM**, v. 60, n. 9, p. 5, set. 2017. p. 5. PASQUALE, Frank. Restoring Transparency to Automated Authority. **Journal on Telecommunications and High Technology Law**, v. 9. p. 235-256, 2011. p. 255. CITRON, Danielle Keats. Technological Due Process. **Washington University Law Review**, v. 85, n. 6, p. 1249-1313, 2008. p. 1308.

[425] Original em Inglês. Tradução livre: "Com olhos o suficiente, todos os erros são simples" (RAYMOND, Eric Steven. **The Cathedral and the Bazaar:** Musings on Linux and Open Source by an Accidental Revolutionary. Sebastobol: O'Reilly, 2001. p. 30). Eric Raymond utiliza o apelido "Lei de Linus" em alusão à Linus Torvalds, responsável por coordenar o desenvolvimento do sistema operacional Linux completamente em código aberto.

[426] Em segurança da informação, essa concepção também é chamada de Princípio de Kerckhoff, em homenagem ao criptografo holandês Auguste Kerckhoff. Ainda no Século XIX, Kerckhoff defendia que, dentre outros requisitos, a segurança de um sistema de informação não deveria depender de seu próprio sigilo (KERCKHOFF, Auguste. La Cryptographie Militaire, **Journal des Sciences Militaries**, v. IX, p. 5-38, jan. 1883. p. 12).

[427] Para um estudo abrangente a respeito das motivações existentes em comunidades de programadores de software aberto, vide: DAVID, Paul A.; SHAPIRO, Joseph S. Community-Based Production of Open Source Software: What Do We Know about the Developers Who Participate? **SSRN**, 23 sep. 2008.

[428] Estudos apontam que mesmo públicos mais específicos, como jornalistas especializados em cobrir questões políticas, enfrentam dificuldade em interpretar dados e realizar análises estatísticas (WIHBEY, John. Journalists

economia atual a maior parte da sociedade depende dos produtos desenvolvidos pela indústria de softwares, a qual investe bilhões anualmente em pesquisa e produção de soluções tecnológicas para atender as mais diversas demandas do mercado. Entretanto, como John Perry Barlow deixa bem claro[429], no mundo conectado pela internet, os custos para a reprodução de informações é praticamente nulo, bastando um simples "ctrl + c" e "ctrl + v" para a produção de uma cópia exata. Assim, iniciativas com fins lucrativos não apenas utilizam mecanismos de propriedade intelectual para fins de assegurar o investimento realizado, mas também metodologias de código-fonte fechado, evitando que pessoas não autorizadas possam reproduzir gratuitamente seus produtos e assim reduzir suas receitas econômicas[430].

Mesmo que superada a questão anterior, (por exemplo, no caso do desenvolvimento de softwares pagos com dinheiro público[431] [432]) existe uma **segunda** razão pela qual a simples disponibilização de código-fonte aberto não é uma solução definitiva para os problemas envolvendo segurança ou proteção de dados pessoais: o fato de existirem centenas ou milhares de programadores e usuários testando o código de um produto não necessariamente significa que ele será identificado a tempo ou mesmo que será possível resolver o problema encontrado. Com efeito, mesmo códigos famosos pelo grande número de revisores e utilizados por milhões de usuários já foram alvo de manchetes em virtude da identificação tardia de erros catastróficos, capazes de colocar em risco à segurança dos dados tratados e a integridade dos sistemas que deles se utilizam[433]. No ambiente relativamente desprovido de autoridade central no qual

---

Know They Need to Get Better with Data and Statistics, but They Have a Long Way to Go. **NiemanLab**. 3 may. 2019. Não Paginado).

[429] BARLOW, op. cit., 1994. Não paginado.

[430] De fato, como bem descrito por Yochai Benkler, é necessario reconhecer que existem iniciativas com fins lucrativos que utilizam metodologias de código-fonte aberto (BENKLER, Yochai. **The Wealth of Networks:** How Social Production Transform Markets and Freedom. New Haven: Yale University Press, 2006. p. 460-473). Entretanto, não é possível concluir se esse modelo é aplicável a qualquer tipo de iniciativa (STRAHILEVITZ, Lior. Wealth without Markets? Reviewing Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom. **Yale Law Review**, v. 116, n. 7, p. 1472-1515, 2007. p. 1514-1515).

[431] Existe um significativo movimento em favor da publicidade de códigos de programas pagos com dinheiro público, cujo lema em inglês é *Public Money, Public Code* (tradução livre: "dinheiro público, código público"). No Brasil, o art. 24, inciso V do Marco Civil da Internet estabelece como diretriz para a atuação do poder público a "adoção *preferencial* de tecnologias, padrões e formatos abertos e livres" (grifou-se) (BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014). Igualmente, vide: BLOCH-WEHBA, Hannah. Access to Algorithms. **Fordham Law Review**, v. 88, p. 1-52, mar. 2019. MOODY, Glyn. If Software Is Funded from a Public Source, Its Code Should Be Open Source. **Linux Journal.** 4 fev. 2019. Não paginado.

[432] Embora não seja o objeto do presente trabalho, uma questão que merece mais atenção diz respeito à propriedade intelectual de sistemas desenvolvidos por entidades privadas mediante contrato com entes públicos. Para tanto, vide: LEVINE, David S. Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure. **Florida Law Review**, v. 59, p. 135-193, 2007.

[433] Exemplificativamente, em 2014 o "bug" chamado *Heartbleed*, encontrado no código de um dos protocolos criptográficos mais utilizados para assegurar comunicações seguras, afetou cerca de 44% dos 100 sites mais acessados na internet e aproximadamente 24% da lista dos 1 milhão de sites mais acessados da rede mundial de

códigos abertos geralmente são desenvolvidos, a ausência de coordenação ou incentivos adequados[434] pode levar a uma redução na quantidade ou perda de foco dos revisores do código, o que, por sua vez, acaba por gerar uma falsa percepção de segurança[435]. Para além disso, existem determinadas categorias de falhas ou defeitos capazes de comprometer a segurança de dados pessoais cuja existência está intimamente relacionada à forma como o *hardware* é construído. Em outras palavras, existem casos em que a própria *estrutura física* do equipamento eletrônico do computador está comprometida, sendo nestes casos completamente irrelevante para a segurança ou privacidade dos dados armazenados o fato do código-fonte estar disponibilizado[436]. Em alguns casos extremos como este, soluções seguras e definitivas para o vazamento de dados podem simplesmente não existir por motivos tecnológicos.

Superadas estas questões, o **terceiro** motivo pelo qual a simples disponibilização aberta de códigos-fontes não é suficiente para garantir a transparência de um algoritmo computacional está no fato de que a maior parte da população de usuários simplesmente *não sabe ler* códigos de computador ou é incapaz de compreender *sozinha* um código escrito com centenas, milhares ou mesmo milhões de linhas. Definitivamente, no panorama atual da economia informacional existe um profundo abismo de conhecimento no que diz respeito a habilidades relacionadas às chamadas "ciências exatas", particularmente no que se refere ao domínio de lógica e matemática, consideradas pré-requisitos para a compreensão de técnicas de ciência da computação[437]. Ademais, códigos-fontes de sistemas mais complexos, para os quais as preocupações com relação à transparência são ainda mais relevantes, frequentemente são o produto do trabalho de dezenas de especialistas de diversas áreas, cada qual responsável por

computadores (DURUMIC, Zakir *et alli*. The Matter of Heartbleed. **Proceedings of the 2014 Conference on Internet Measurement Conference,** p. 475-488, 2014. p. 475. LESK, op. cit., 2014, p. 96).

[434] SCHRYEN, Guido. Is Open Source Security a Myth? **Communications of the ACM**, v. 54, n. 5, p. 130-140, may. 2010. p. 140.

[435] FELTEN, Edward W.; KROLL, Joshua A. Heartbleed Shows Government Must Lead on Internet Security. **Scientific American**, 1 jul. 2014. Não paginado. HANSEN; KOHNTOPP; PFITZMANN, op. cit., 2002, p. 471. Justamente para estabelecer um ambiente que incentive a busca por "bugs" em sistemas de código-aberto, organizações públicas e privadas passaram a adotar como prática o estabelecimento de programas de recompensa, nos quais quaisquer interessados em auditar os sistemas são remunerados caso encontrem e reportem falhas ou erros (HILLENIUS, Gijs. European Parliament increases budget for EU Free and Open Software Auditing. **EU-FOSSA**, 29 oct. 2016. Não paginado).

[436] Exemplificativamente, as vulnerabilidades conhecidas como *meltdown* e *spectre*, identificadas em 2018, são baseadas em aspectos tão elementares do funcionamento de sistemas eletrônicos que algumas estimativas chegam a apontar que praticamente 90% dos computadores produzidos entre 1995 a 2018 sofrem destas falhas de segurança (LIPP, Moritz *et allia*. Meltdown: Reading kernel memory from user space. **Proceedings of the 27th USENIX Conference on Security Symposium**, p. 973-990, 2018. p. 973-974. GREENBERG, Andy. Triple Meltdown: How so many researchers found a 20-year-old chip flaw at the same time. **Wired**, 07 jan. 2018. Não paginado).

[437] UNITED NATIONS EDUCATION, SCIENTIFIC AND CULTURAL ORGANIZATION. Digital Literacy in Education. **Policy Brief**, may. 2017. p. 2. BRACKEN, Mike. AI: the impending tragedy of the Commons. **University College London Institute for Innovation and Public Purpose Blog**, 22 mar. 2018. Não paginado.

um determinado aspecto tecnológico cujo entendimento pleno sob a perspectiva técnica é restrito a poucas pessoas[438]. Em resumo, se a construção de tecnologias de informação e comunicação é uma tarefa cuja complexidade usualmente exige esforços coletivos de dezenas de pessoas, a simples possibilidade de acessar o código-fonte pode não ser suficiente algo suficiente para assegurar transparência adequada para o algoritmo computacional sob análise.

Em **quarto** lugar, ainda na improvável hipótese de um código-fonte não conter quaisquer erros de programação ou mesmo vieses implícitos e explícitos em sua lógica computacional, mesmo assim sua execução pode gerar resultados indesejados em virtude das bases de dados utilizadas para o processamento da informação. De fato, tendo em vista que um algoritmo consiste num processo absolutamente preciso cuja finalidade está em produzir um valor de saída (*output*) em função de um determinado valor de entrada (*input*), os valores de entrada exercem um papel necessário e fundamental em seu funcionamento. Deste modo, problemas eventualmente existentes no conjunto de dados utilizados podem levar a resultados indesejados e não previstos na execução do algoritmo, a despeito de seu código-fonte ter sido desenvolvido com a preocupação de evitá-los.

Por certo, a capacidade do conjunto de dados utilizados afetar negativamente a execução de um algoritmo computacional é particularmente marcante no caso de utilização de técnicas de mineração de dados, as quais se baseiam na utilização de procedimentos estatísticos para separar (e, portanto, discriminar) dados com o intuito encontrar relações estatísticas[439]. Em resumo, técnicas de mineração de dados procuram automatizar o processo de descoberta de padrões úteis, possibilitando transformar uma quantidade pequena de informações em uma quantidade maior de informações[440]. Entretanto, essas técnicas podem enfrentar vários desafios quando de sua aplicação, as quais podem ser, dentre outros[441]: a dificuldade de transcrever o problema de negócio para o algoritmo e localizar os dados capazes de responder ao questionamento; a definição do conjunto de dados a ser utilizado; a estipulação dos valores iniciais a serem usados como exemplo; a abrangência e a representação do conjunto de dados no qual se baseia o processamento.

---

[438] VICENT, James. Tencent says there are only 300,000 AI engineers worldwide, but millions are needed. **The Verge**, 5 dec. 2017. Não paginado.
[439] BAROCAS; SELBST, op. cit., 2016. p. 667.
[440] DOMINGOS, Pedro. A Few Useful Things to Know About Machine Learning. **Communications of the ACM**, v. 55, n. 10, p. 78-87, oct. 2012. p. 81.
[441] BAROCAS; SELBST, op. cit., 2016. p. 679.

Em reforço à criticidade desta situação, é frequente que sistemas mais complexos não utilizem exclusivamente bases de dados próprias, mas sim conjuntos de dados pertencentes a terceiros, sejam eles agentes públicos ou privados. Deste modo, na eventual ausência de um processo adequado e confiável de documentação e registro a respeito da origem, metodologia de coleta e outros aspectos técnicos relacionados a base de dados utilizadas, torna-se difícil identificar a fonte e os motivos pelos quais a execução do algoritmo computacional apresentou um problema. Em outras palavras, ainda que a disponibilização aberta do código-fonte de um determinado programa possa ser positiva sobre vários aspectos, não é uma medida capaz de servir por si só como solução para disponibilizar todas as informações pertinentes a respeito da coleta e tratamento de dados pessoais.

4.2.2 Explicação da decisão algorítmica

Em virtude de todos os motivos citados acima, diversos estudiosos consideram que a simples disponibilização aberta do código-fonte não seria uma medida eficaz para atender às necessidades de transparência da maior parte dos usuários de sistemas e titulares de dados. Em primeiro lugar, no que diz respeito a sistemas desenvolvidos e utilizados por agentes privados, órgãos reguladores, embora considerem a medida positiva, são relutantes em exigi-las como algo obrigatório[442] justamente, dentre outros motivos, em virtude de preocupações relacionadas à proteção da propriedade intelectual. Porém, além desse tipo de preocupação, no caso de algoritmos computacionais que se utilizam técnicas de inteligência artificial para o tratamento de dados, a simples disponibilização do código-fonte é considerada por alguns autores como uma proposta até mesmo "ingênua", pois poderia dar margem, em certos casos, a estratégias de "trapaça" do sistema[443] [444]. Além disso, seria insuficiente no caso de sistemas eletrônicos mais

[442] EUROPEAN UNION. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.** Brussels: Article 29 Data Protection Working Party, 2018. p. 25.

[443] COURTLAND, Rachel. Bias detectives: the researchers striving to make algorithms fair. **Nature**, 20 jun. 2018. Não paginado. COUNCIL OF EUROPE. Committee of Experts on Internet Intermediaries. **Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications.** Brussels: Council of Europe, 2017. p. 37. Por outro lado, há quem refira que a exposição das vulnerabilidades também induziria o desenvolvimento de sistemas melhores e mais robustos (DIAKOPOULOS, Nicholas. Accountability in Algorithmic Decision Making. **Communications of the ACM**, v. 59, n. 2, p. 56-62, feb. 2016. p. 62).

[444] Contudo, ao tratar sobre o assunto, a Estratégia Nacional de Dados do Reino Unido refere que informações como código-fonte e dados de sistemas utilizados pelo poder públicos apenas não devem ser tornadas transparentes nos casos em que forem utilizados para a prevenção de fraudes ou atividades de contra-terrorismo (UNITED KINGDOM. Department for Digital, Culture, Media & Sport. **Data Ethics Workbook.** London: Government Digital Service, 2018. Não Paginado).

complexos que usem metodologias que produzam resultados aleatórios ou sofram atualizações constantes em razão da dinamicidade das fontes de dados[445]. Não obstante, a necessidade de *compreensão* de uma decisão algorítmica permanece, porquanto seres humanos precisam, ao menos sob certa medida, compreender qualitativamente uma decisão para que possam efetivamente *na decisão*[446] e não unicamente depositar sua confiança em seu autor.

Diante dessa questão, pesquisadores como Goodman, Flaxman, Malgieri e Freitas[447] propuseram o desenvolvimento e a adoção de algoritmos computacionais capazes de fornecer explicações acerca de seu funcionamento para seus usuários. Designando esse movimento de "direito à explicação", os autores que defendem seu reconhecimento baseiam seu posicionamento no *GDPR*, o qual possui em seu texto alguns excertos que poderiam, em tese, dar suporte jurídico a essa pretensão. Em especial, são referidos o artigo 15[448], já citado na seção **4.1**, e o artigo 22 do diploma, o qual possui o seguinte teor[449]:

> ***Article 22 - Automated individual decision-making, including profiling***
> *1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*
> *2. Paragraph 1 shall not apply if the decision:*
> *(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
> *(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
> *(c) is based on the data subject's explicit consent.*

---

445 KROLL, Josua *et ali*. Accountable Algorithms. **University of Pennsylvania Law Review**, v. 165, n. 3, p. 633-705, 2017. p. 657-658.

446 RIBEIRO, Marco Tulio; SINGH, Sameer; GUESTRIN, Carlos. "Why Should I Trust You?" Explaining the Predictions of Any Classifier. **Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, p. 1135-1144, ago. 2016. p. 1135-1136.

447 GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithm Decision-Making and a "Right to Explanation". **AI Magazine**, v. 38, n. 3, p. 1-9, 2017. p. 6. MALGIERI; COMANDÉ, op. cit., 2017. p. 265. No Brasil, merece especial destaque o instigante artigo de Juarez Freitas sobre a inteligência artificial e o direito administrativo (FREITAS, Juarez. Direito Administrativo e Inteligência Artificial. **Interesse Público**, Belo Horizonte, ano 21, n. 114, p. 15-29, mar./abr. 2019).

448 SELBST, Andrew; POWLES, Julia. Meaningful Information and the Right to Explanation. **International Data Privacy Law**, v. 7, n. 4, p. 233-242, nov. 2017. p. 242.

449 Original em Inglês. Tradução livre: "Artigo 22 – Decisões individuais automatizadas, incluindo criação de perfis 1. O titular de dados deve ter o direito de não ser sujeitado a uma decisão baseada apenas no processamento automatizado, inclusive a criação de perfis, que produzam efeitos legais a seu respeito ou lhe afete significativamente. 2. O parágrafo 1 não se aplica se a decisão: (a) é necessária para entrar ou realizar um contrato entre o titular de dados e o controlador de dados; (b) é autorizada pela legislação da União ou Estado Membro ao qual o controlador está sujeito e que também estabelece medidas adequadas para garantir os direitos, liberdades e interesses legítimos do titular de dados; ou (c) é baseada no consentimento explícito do titular de dados. 3. Nos casos referidos nos pontos (a) e (c) do parágrafo 2, **o controlador de dados deverá implementar medidas adequadas para garantir os direitos, liberdades e interesses legítimos do titular de dados, pelo menos, o direito de obter intervenção humana da parte do controlador, para expressar seu ponto de vista e contestar a decisão**. " (grifou-se).

> *3. In the cases referred to in points (a) and (c) of paragraph 2,* ***the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision****. (grifou-se)*

Por certo, o texto em questão não menciona expressamente o "direito à explicação" postulado por autores como Goodman e Flaxman[450]. Não obstante, os mesmos autores defendem que o dispositivo colacionado deve ser interpretado em conjunto com o inciso 71 do preâmbulo do GDPR, o qual, a despeito de não possuir força normativa, refere que[451]:

> *[...] such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view,* ***to obtain an explanation of the decision reached after such assessment*** *and to challenge the decision.* (grifou-se)

Diante da complexidade da matéria, a autoridade europeia responsável pela área buscou estabelecer algumas linhas gerais sobre o assunto. Assim, considerando os direitos pessoais do titular de dados, mencionou que[452]:

> *The growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process or profiling works.*
> *The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.*

---

[450] GOODMAN; FLAXMAN, op. cit., 2017, p. 6.

[451] Original em Inglês. Tradução livre: "[…] este processamento deve estar sujeito a salvaguardas adequadas, as quais devem incluir informações específicas para o titular de dados, o direito de obter intervenção humana, de expressar seu ponto de vista, **de obter uma explicação da decisão alcançada após tal avaliação** e de desafiar a decisão" (grifou-se).

[452] EUROPEAN UNION. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.** Brussels: Article 29 Data Protection Working Party, 2018. p. 25. Original em Inglês. Tradução livre: "O crescimento e complexidade do aprendizado de máquina pode tornar desafiador a compreensão de como um processo de decisão automatizado ou produção de perfis funciona. O controlador deve buscar maneis simples de informar ao titular de dados sobre o raciocínio, ou os critérios utilizados, para chegar na decisão. O GDPR exige que o controlador forneça informação útil sobre a lógica envolvida, não necessariamente uma explicação complexa do algoritmo utilizado ou a sua disponibilização completa. A informação fornecida deve, entretanto, ser suficientemente abrangente para permitir ao titular de dados entender as razões para a decisão".

Muito embora este trabalho adote a posição segundo a qual não existe previsão *expressa* quanto ao tema do "direito à explicação" no texto do GDPR[453], é possível, em tese, compreender que se o regulamento europeu estabelece um direito à oposição contra decisões automatizadas, deve também permitir como pressuposto lógico que o indivíduo possa compreender a decisão tomada[454]. De fato, a possibilidade de compreender os motivos de uma decisão é algo necessário para que seja viável realizar uma oposição racional a seu respeito, pois, do contrário, não é possível conceber a existência de um contraditório efetivo. De toda maneira, a despeito da existência ou não de previsão expressa no direito positivo, é necessário avaliar a proposta da explicação algorítmica e suas possíveis limitações, porquanto apenas assim será viável compreender seu alcance enquanto medida de transparência tecnológica.

Nesse sentido, de acordo com a literatura quanto ao tema, existem em síntese duas metodologias de aplicáveis no que diz respeito aos tipos de explicações possíveis de obter frente a algoritmos mais complexos[455]: **a)** explicações baseadas no modelo do algoritmo (*Model-Centric Explanation*); **b)** explicações baseadas no sujeito (*Subject-Centric Explanation*).

Inicialmente, explicações *baseadas no modelo do algoritmo* têm a finalidade de prover informações gerais sobre o funcionamento da tecnologia, sem se adentrar em questões relacionadas a decisões específicas ou ao resultado do tratamento de algum dado em particular. Dentre as possíveis "explicações" que podem ser fornecidas por esta espécie de metodologia se encontram as informações sobre a configuração e os parâmetros do algoritmo, os metadados do treinamento, as métricas de funcionamento, as informações gerais quanto à lógica e informações quanto ao processo de tratamento em si[456]. Justamente em razão da generalidade desta abordagem, cientistas de computação costumam chamar estas soluções de "explicações globais"[457], porquanto buscam esclarecer o "todo" do sistema.

A despeito de explicações baseadas no modelo do algoritmo trazerem informações interessantes, sob o ponto de vista do indivíduo elas podem não ser suficientes para proporcionar de fato uma compreensão mais detalhada ou relevante, porquanto este tipo de explicação não leva em conta os dados pessoais daquele que é afetado por uma decisão específica. Assim sendo, como forma de tentar explicar o funcionamento desses sistemas,

---

[453] EDWARDS; VEALE, op. cit., 2018, p. 2. WACHTER; MITTELSTADT; FLORIDI, op. cit., 2017, p. 79.
[454] SELBST; POWLES, op. cit., 2017, p. 242.
[455] EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a "Right to an Explanation" is Probably not the Remedy you are Looking For. **Duke Law & Technology Review**, v. 16, n. 1, p. 18-81, 2017. p. 55.
[456] Idem, p. 55-56.
[457] Idem, p. 55.

propõe-se como alternativa a utilização de explicações baseadas no próprio "sujeito", isto é, explanações que buscam identificar como o algoritmo reage levando em conta o tratamento de um conjunto de dados específicos e vinculado a um determinado indivíduo.

Ao contrário de explicações baseadas no modelo, as quais apenas poderiam fornecer informações *antes* do processamento, a metodologia de *explicações baseadas no sujeito* é construída com a finalidade de fornecer maiores detalhes *após* o tratamento ser realizado. Deste modo, em virtude de utilizarem apenas um determinado conjunto de dados num recorte específico de tempo, as explicações fornecidas por esta metodologia são chamadas de "locais"[458]. De forma geral, os tipos de explicações que esta abordagem pode fornecer são descritos como sendo: a) baseadas na sensitividade dos dados, identificando quais são os dados para os quais o modelo é mais "sensível"; b) baseadas nos casos utilizados, esclarecendo quais conjuntos de dados utilizados no modelo são mais similares ao do sujeito; c) baseadas na demografia, clarificando quem e quais seriam as respectivas características dos indivíduos que receberam tratamento semelhante ao de um determinado sujeito; d) baseadas na performance, esclarecendo o quão acurado[459] é o resultado.

Todavia, apesar de modelos baseados no sujeito serem possivelmente mais úteis para o indivíduo preocupado em saber como seus próprios dados são tratados pelo modelo, a aplicação desta metodologia de explicação algorítmica esbarra naquilo que é frequentemente chamado de "maldição da dimensionalidade"[460]: quanto maior o número de variáveis, maior será o número de potenciais combinações e interações entre os dados utilizados o que, por sua vez, irá exigir uma quantidade maior de dados para fornecer a mesma acurácia no resultado da operação. Em outras palavras, o simples isolamento de um dado pessoal de um indivíduo afetado para explicar o resultado de uma operação pode tornar matematicamente inviável o fornecimento de uma explicação adequada para aquele indivíduo em virtude da perda de acurácia[461].

---

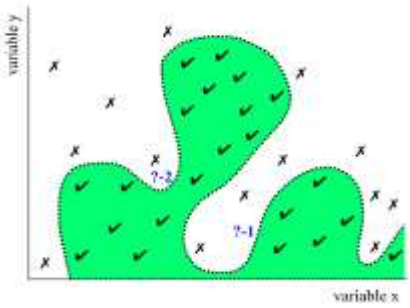
[458] Idem, p. 56. RIBEIRO; SINGH; GUESTRIN, op. cit., 2016. p. 1138.

[459] De acordo com a literatura pertinente, acurácia é o "grau de proximidade de uma estimativa com seu parâmetro" (MONICO, João Francisco Galera *et alli*. Acurácia e Precisão: revendo os conceitos de forma acurada. **Boletim de Ciências Geodésicas.** v. 15, n. 3, p. 469-483, jul-set. 2009. p. 471).

[460] EDWARDS; VEALE, op. cit., 2017, p. 56. CHEN, Lei. Curse of Dimensionality. *In.:* LIU, Ling; OZSU, Tamer (Eds.). **Encyclopedia of Database Systems.** Boston: Springer, 2019. Não paginado.

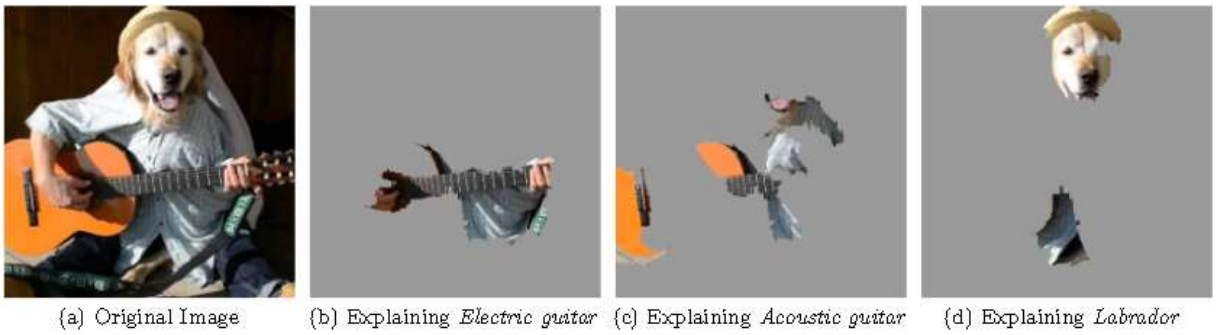
[461] Buscando contornar esta situação, algumas iniciativas por parte da sociedade civil têm procurado incentivar que grandes grupos de voluntários disponibilizem seus dados e respectivas decisões fornecidas pelos algoritmos para tentar descobrir mais informações sobre o sistema mediante engenharia-reversa. Todavia, essas iniciativas são relativamente escassas e sofrem com os problemas inerentes a outras iniciativas voluntárias (CRICHTON, Danny. How Do You Fight an Algorithm You Cannot See? **TechCrunch**, 15 jan. 2019. Não paginado).

Figura 3 – Exemplo de explicação algorítmica de 2 variáveis



Fonte: EDWARDS; VEALE (2017).

Figura 4 - Exemplo de explicação algorítmica em imagens



Fonte: RIBEIRO; SINGH; GUESTRIN (2018)[462]

Para além do problema da acurácia, o simples fato de se possuir acesso aos dados de um determinado indivíduo pode ser insuficiente para o fornecimento de uma explicação útil e capaz de identificar a existência de eventuais discriminações. Com efeito, determinados tipos de distinções negativas e enviesadas não são "perceptíveis" por um único indivíduo isoladamente, mas apenas por meio da análise conjunta de vários indivíduos coletivamente[463]. Nestes termos, salvo na hipótese do indivíduo ter acesso aos dados pessoais de outros que compartilhem características semelhantes às suas (o que, por si só, também pode gerar preocupações quanto à privacidade destas pessoas), será difícil que identifique estar sendo prejudicado. Além disso, em sistemas eletrônicos que utilizam bases de dados alimentadas dinamicamente (em tempo real, por exemplo), o simples isolamento de determinado conjunto de dados pessoais para a análise do "raciocínio" por trás da decisão pode fornecer um resultado que não corresponde à

[462] Na figura 3 acima, o exemplo mostra uma explicação fornecida por um algoritmo para explicar o motivo de ter classificado uma foto de um humano disfarçado como sendo "32% guitarra elétrica", "24% guitarra acústica" e "21% labrador" (RIBEIRO; SINGH; GUESTRIN, op. cit., 2018, p. 5).

[463] MAZUR, Joanna. Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law. **Erasmus Law Review**, n. 3, p. 178-189, dec. 2018. p. 183-184.

realidade ou de difícil análise, pois enquanto as decisões tomadas utilizam dados dinâmicos, a explicação fornecida é baseada em dados estáticos[464].

Entretanto, para além da questão da intrinsecamente relacionada à complexidade da explicação fornecida, existem outros desafios que tanto as metodologias baseadas no modelo quanto aquelas baseadas no sujeito enfrentam no que diz respeito à sua viabilidade enquanto medidas tecnológicas. De fato, tendo em vista que metodologias de explicação aplicáveis a algoritmos também são, elas próprias, algoritmos, elas enfrentam os mesmos desafios de quaisquer outros algoritmos enfrentam no que diz respeito à sua *computabilidade*[465]. Em outras palavras, algoritmos de explicação também precisam preencher os requisitos essenciais de quaisquer algoritmos computacionais, quais sejam: serem funções lógicas, finitas, *eficientes* e *bem-definidas*, que a partir de um valor de entrada específico resultem num valor de saída específico[466]. Todas essas características são fundamentais para que uma função seja computável.

Com efeito, certos problemas e questionamentos jurídicos comuns na aplicação do direito são conceitos jurídicos *indefinidos*, para os quais não é possível no estágio atual da Ciência do Direito encontrar uma definição clara e universal. Definir o significado de conceitos como "justo" ou "discriminatório"[467] não é uma tarefa trivial, sendo fortemente dependente do resultado da análise de custo-benefício feita pelo responsável pela decisão. Entretanto, ocorre que a transposição de conceitos jurídicos indefinidos para um algoritmo computacional acaba por esbarrar justamente no requisito essencial de "definição" para fins computacionais. Ao contrário de problemas relacionados a erros de digitação no código, problemas de definição são problemas *lógicos* para os quais computadores são incapazes de compreender ou perceber sua

---

[464] LEHR, David; OHM, Paul. Playing with the Data: What Legal Scholars Should Learn About Machine Learning. **University of California Law Review**, v. 51, p. 653-717, 2017. p. 707. DESAI, Deven R.; KROLL, Joshua A. Trust but Verify: A Guide to Algorithms and the Law. **Harvard Journal of Law and Technology**, v. 31, p. 1-64, 2018. p. 41.

[465] Para os fins aqui utilizados, "computação" significa a realização de computações numéricas com base em operações aritméticas como adição, subtração, divisão e multiplicação. De fato, os computadores eletrônicos atuais nada mais são do que aplicações práticas da "Máquina de Turing", cujo modelo buscava estabelecer um método lógico pelo qual fosse possível identificar se uma função era ou não computável (COPELAND, Jack B. The Church-Turing Thesis. In.: ZALTA, Edward N. (ed.) **The Stanford Encyclopedia of Philosophy.** Stanford: Stanford University, 2019. Não paginado).

[466] KNUTH, op. cit., 1997. p. 4-6.

[467] De fato, conforme demonstrado por Sam Cobert-Davies e outros, mesmo a análise estatística de casos de discriminação pode resultar em conclusões diferentes de acordo com o critério matemático utilizado, sendo necessário escolher expressamente, numa análise de custo-benefício, qual resultado priorizar (CORBET-DAVIES, Sam *et allia*. Algoritmic Decision Making and the Cost of Fairness. **Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, p. 797-806, ago. 2017. p. 804-805). Nesse mesmo sentido: ABITEBOUL, Serge; STOYANOVICH, Julia. Transparency, Fairness, Data Protection, Neutrality: Data Management Challenges in the Face of New Regulation. **arXiv**, 8 mar. 2019. p. 5.

a existência. Assim, de acordo com a Tese de Turing, se um problema não pode ser descrito de uma forma "mecânica", mediante etapas precisas, um computador (humano ou eletrônico) não terá condições de resolvê-lo[468]. Nestes casos, sem que um ser humano defina *precisamente* a ação a ser realizada, o computador simplesmente será incapaz de tomar uma decisão[469]. Em síntese: no que diz respeito ao problema da explicação de algoritmos, se a explicação para um algoritmo não for *computável*, ele simplesmente não será possível formular um algoritmo computacional para explicá-lo[470].

Para além do problema sobre a definição de um algoritmo explicativo e a sua computabilidade, existe também a questão da "eficiência" da função que define um algoritmo. Em outras palavras, um algoritmo computacional precisa são só ser capaz de resolver uma determinada questão, mas também de ser capaz de fazer isso em tempo razoável e util, chamado de na Ciência da Computação de "tempo polinomial" (ou simplesmente "P"). Todavia, existem problemas complexos, dentre eles o fornecimento de explicações para determinados algoritmos, cuja solução em tempo razoável – tempo polinomial – não é aparentemente possível ou determinável (ou simplesmente "NP"). Diz-se "aparentemente" porque até o presente momento nenhum estudioso ou pesquisador conseguiu resolver o questionamento "P vs NP"[471], o qual consta dentre os 7 "Problemas do Milênio" estabelecidos como desafios para matemáticos de todo o mundo. Em resumo: existem problemas para os quais não existe um algoritmo capaz de fornecer uma explicação em tempo razoável.

Por certo, importante deixar claro que não se defende aqui a impossibilidade de fornecer explicações para a tomada de decisões por meio de algoritmos computacionais. A necessidade de desenvolver mecanismos capazes de aprimorar nossa compreensão sobre o funcionamento desses algoritmos é algo que cada vez cresce em importância diante do vertiginoso avanço dessas tecnologias em cada faceta de nosso cotidiano. Todavia, diante do incremento da atenção dada ao tema, é igualmente relevante ter em mente que, no mesmo no atual cenário de desenvolvimento tecnológico exponencial, a produção de explicações, principalmente em

---

[468] COPELAND, Jack B; SHAGRIR, Oron. The Church-Turing Thesis: Logical Limit or Breachable Barrier? **Communications of the ACM,** v. 62, n. 1, p. 66-74, 2019. p. 66.
[469] KOOPS, Bert-Jaap. The (In)Flexibility of Techno-Regulation and the Case of Purpose-Binding. **Legisprudence**, v. 5, n. 2, p. 171-194, 2011. p. 194.
[470] DESAI; KROLL, op. cit., 2018. p. 33. LIPTON, Zachary C. The Mythos of Model Interpretability. **ACM Queue**, v. 16, n. 3, p. 1-27, may-jun. 2018. p. 20.
[471] Em Inglês, a sigla significa "Polynominal vs "Nondeterministic Polynomial time" (COOK, Stephen. **The P versus NP Problem.** Peterborough: Clay Institute of Mathematics, 2018. p. 1).

sistemas de inteligência artificial, esbarra em problemas fundamentais da própria Ciência da Computação para os quais ainda não existem soluções simples em um horizonte próximo[472].

Parece restar claro que apenas com o estabelecimento de uma relação de confiança efetiva para com as novas tecnologias de informação de comunicação é que a população em geral se sentirá segura em utilizá-las e adotá-las em seu dia a dia. Assim sendo, diante de tudo que foi estudado neste trabalho até o presente momento, a seção **4.3** a seguir irá buscar traçar reflexões finais a respeito da transparência aplicada ao contexto de concepção e desenvolvimento de sistemas eletrônicos. Deste modo, ainda que sem a pretensão de esgotar a complexidade da matéria, tentar-se-á indicar alguns dos possíveis pontos pelos quais medidas regulatórias podem ajudar a fornecer mais informações sobre esses novos mecanismos e torna-los instrumentos sociais mais legítimos.

4.3 DA TRANSPARÊNCIA E SUA APLICAÇÃO NO CONTEXTO DE COLETA E TRATAMENTO DE DADOS PESSOAIS

Tecnologias de informação e comunicação são, cada vez mais, elementos indissociáveis do cotidiano, notadamente na vida dos habitantes de grandes centros urbanos. Estas tecnologias, por meio de sistemas eletrônicos, aplicativos e ferramentas afins, paulatinamente se tornam instrumentos de regulação de condutas, influenciando e limitando o atuar dos indivíduos de acordo com os valores introduzidos em sua arquitetura informacional. Diante desta maior relevância, argumentos em prol de maior transparência de tecnologias de informação e comunicação passaram a atrair mais atenção por parte de estudiosos e agentes reguladores preocupados com a proteção a ser conferida aos direitos fundamentais perante estes novos desafios[473].

Dentre as diversas propostas de abordagens regulatórias apresentadas, medidas com viés mais tecnológico, como a disponibilização aberta do código-fonte e o fornecimento de explicações algorítmicas, têm atualmente recebido mais destaque e recepção, notadamente no

---

[472] BURREL, Jenna. How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. **Big Data & Society.** p. 1-12, jan./jun. 2016. p. 10.
[473] CITRON, Danielle; CALO, Ryan. The Automated Administrative State. **The Ethical Machine**, 8 apr. 2019. Não Paginado.

que diz respeito a sistemas eletrônicos utilizados pelo setor público[474]. Entretanto, levando em consideração as questões levantadas acima nas seções **4.2.1** e **4.2.2**, medidas estritamente tecnológicas, conquanto sejam positivas, não são nem podem ser consideradas uma panaceia para os problemas relacionados à falta de transparência no tratamento eletrônico de informações[475]. Em especial, no que diz respeito à implementação específica de determinados requisitos no código-fonte de um sistema eletrônico, como por exemplo o fornecimento uma explicação, a inflexibilidade de uma regra inscrita no código pode acarretar grandes dificuldades se ela eventualmente precisar ser aplicada frente a casos concretos com características muito distintas[476].

Com efeito, diante do avanço da defesa em prol da adoção de medidas de transparência com viés tecnológico, alguns autores têm buscado alertar para os possíveis riscos de se exigir um padrão exageradamente elevado e pouco realístico, em especial se comparado com o funcionamento da decisão humana[477]. Nesta senda, a despeito de concordarem com a relevância da preocupação quanto à opacidade interna das decisões automatizadas, John Zerilli e outros autores apontam que ainda que o agente responsável por uma decisão humana seja bem-intencionado e busque esclarecer e justificar ao máximo as suas motivações, a sua compreensão e descrição completa, de acordo com o atual estágio de evolução da neurologia e psicologia, simplesmente ainda é não é possível[478]. Com efeito, trançando um paralelo com as exigências feitas por alguns autores quanto ao funcionamento de sistemas eletrônicos, a descrição completa dos processos químicos e biológicos que envolvem uma decisão humana seria, no geral, incompreensível e sem utilidade para a maior parte da população, porém não é por causa disso

---

[474] Conforme lembra Fernanda Campagnucci, desde 2016 a França, a partir da *Loi nº 1321 du 7 octobre 2016 pour une République numérique,* tem gradativamente realizado um levantamento e disponibilizado o código-fonte e explicações técnicas sobre sistemas eletrônicos utilizados pelo governo Francês (CAMPAGNUCCI, Fernanda. Algoritmos Públicos: Como a França está fazendo e por que deveríamos fazer também. **Um Dado a Mais**, 20 abr. 2019. Não paginado). Além da França, o Canadá (CANADA. **Directive on Management of Information Technology.** Ottawa: Government of Canada, 2018) e o País Basco (HILLENIUS, Gijs. Basque Country's open source law invites other European administrators. **Joinup – European Commission,** 14 ago. 2012. Não paginado) também contam com regulamentos semelhantes, os quais também impõem como padrão a disponibilização aberta do código-fonte de sistemas utilizados pelo poder público.

[475] HOUSE OF LORDS. Select Committee on Artificial Intelligence. **AI in the UK:** ready, willing and able? London: House of Lords, 2018. p. 38.

[476] KOOPS, op. cit., 2011. p. 193. KOOPS, Bert-Jaap; LEENES, Ronald. Privacy Regulation Cannot be Hardcoded. A critical comment on the "privacy by design" provision in data-protection law. **International Review of Law, Computers & Technology**, v. 28, n. 2, p. 159-171, 2014. p. 166-167.

[477] ZERILLI, John *et alli.* Transparency in Algorithmic and Human Decision-Making: Is There a Double Standard? **Philosophy & Technology**, p. 1-23, set. 2018. p. 1. MUEHLHAUSER, Luke. Transparency in Safety-Critical Systems. **Machine Intelligence Research Institute**, 25 ago. 2013. Não paginado.

[478] ZERILLI, op. cit., 2018. p. 10.

que pessoas deixam de se basear em decisões humanas[479]. Deste modo, justamente para poder confiar mais na decisão, busca-se conferir mais publicidade e transparência ao processo de decisão em si e dos elementos institucionais que o compõe.

De fato, considerando os estudos e reflexões feitos por Lawrence Lessig no que diz respeito às modalidades de regulação – a chamada "Nova Escola de Chicago" –, existem vários caminhos, que podem ser utilizados para se atingir um determinado objetivo regulatório, sendo a intervenção direta na arquitetura de informação apenas um deles. Nesse sentido, se levarmos em conta que o processo de desenvolvimento de sistemas eletrônicos envolve a atividade de diversos agentes desde o processo de concepção e execução do projeto até a sua efetiva disponibilização, todas essas etapas podem estar sujeitas a algum tipo de influência por parte das diferentes modalidades de regulação. Por certo, ainda que com adaptações, as reflexões de Joel Reidenberg sobre as abordagens a serem utilizadas para influenciar no *design* de tecnologias seguem válidas[480] Assim, se o objetivo final de uma atuação regulatória é fomentar mais transparência às tecnologias e, deste modo, disponibilizar mais informações sobre o tratamento de dados pessoais realizado por determinada algoritmo computacional, não só mecanismos arquitetônicos podem ser utilizados, mas também instrumentos que modifiquem aspectos econômicos, sociais e jurídicos do processo de desenvolvimento tecnológico[481]. Desta maneira, objetivos e princípios juridicamente valorizados pela sociedade podem ser protegidos e preservados por sistemas eletrônicos escritos sob influência de um *design* mais transparente e responsável[482].

Nesta senda, considerando que parte da opacidade e incompreensão na qual estão envoltos algoritmos computacionais está intimamente relacionado às capacidades e habilidades da população em geral em compreender tecnologias de informação e comunicação[483], a primeira estratégia a ser abordada está vinculada ao aspecto *social* da regulação exposto por Lessig. De fato, a mitigação do abismo de conhecimento técnico sobre o funcionamento de

---

[479] CASTELVECCHI, Davide. Can we open the black box of AI? **Nature**, v. 538, n. 7623, p. 21-23, oct. 2016. p. 23.
[480] REIDENBERG, op. cit., p. 588.
[481] GASSER, Urs; ALMEIDA, Virgílio A. F. A Layered Model for AI Governance. **IEEE Internet Computing**, v. 21, n. 6, p. 58-62, nov./dez. 2017. p. 61.
[482] ABITEBOUL; STOYANOVICH, op. cit., 2019. p. 8.
[483] BURREL, op. cit., 2016. p. 4. LEE, Irene *et alli.* Computational Thinking for Youth in Practice. **ACM Inroads**, v. 2, n. 1, p. 32-37, mar. 2011. p. 36-37. ANANNY, Mike; CRAWFORD, Fate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New Media and Society**, v. 20, n. 3, p. 973-989, 2018. p. 981. ZAMBONELLI, Franco *et allia.* Algorithmic Governance in Smart Cities: the conundrum and the potential of pervasive computing solutions. **IEEE Technology and Society Magazine.** v. 37, n. 2, p. 80-87, jun. 2018. p. 85.

tecnologias, embora seja medida de implementação complexa, é algo extremamente necessário para que seja possível modificar o relacionamento da sociedade em geral para com os cada vez mais onipresentes sistemas eletrônicos e seus algoritmos computacionais. Nesse sentido, muito embora parcela relevante desta questão resida, principalmente no caso brasileiro, sob responsabilidade de entes públicos[484], agentes privados também possuem papel a desempenhar nesta questão, notadamente no que diz respeito à formação e capacitação de usuários no uso de tecnologias de informação e comunicação, ainda que num primeiro momento deem enfoque às suas ferramentas. Diversas empresas de tecnologia, tais como Microsoft, Amazon, Google, entre outros, possuem plataformas eletrônicas para educação digital de usuários, com conteúdos pagos ou gratuitos abrangendo desde habilidades básicas até questões avançadas e complexas. Por certo, a indução e o investimento em políticas nesse sentido por agentes públicos e privados podem auxiliar a preencher o vazio de conhecimento tão necessário para a adequada compreensão e utilização de tecnologias, reduzindo a hipossuficiência técnica existente de modo disseminado na sociedade.

Embora políticas educacionais sirvam como mecanismos regulatórios sob o ponto de vista da indução de modificações em normas sociais, certamente não são as únicas medidas a serem adotadas para a redução da opacidade e aprimoramento da transparência tecnológica. Por certo, partindo das reflexões feitas na seção **3** deste trabalho quanto ao instituto do *privacy by design*, em especial na seção **3.3** quanto à sua operacionalização, é possível concluir que o estabelecimento de uma política de proteção à privacidade nos moldes em que proposto no GDPR – e também da LGPD – pode conferir significativa melhoria na transparência do processo de coleta e tratamento de dados pessoais, sem o prejuízo da adoção de medidas estritamente tecnológicas. Nesta senda, partindo das contribuições feitas por Ann Cavoukian, é importante estabelecer que a finalidade do princípio da visibilidade e transparência em um programa de *privacy by design* é a de assegurar que todas as partes interessadas tenham condições de saber que as promessas feitas pela organização estão sendo efetivamente

[484] Justamente em buscando atender este problema, e reconhecendo a importância de conhecimentos em tecnologias para a proteção da privacidade, a Comissão Europeia desenvolveu um "Plano de Ação para Educação Digital (EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan.** Brussels: European Commission, 2018. p. 3). Do mesmo modo, o Reino Unido também estuda ativamente e implementa políticas públicas na área (HOUSE OF LORDS, op. cit., 2018. p. 133).

cumpridas[485]. Em outras palavras, é necessário estabelecer um ambiente em que seja possível a auditoria da tecnologia e do seu processo de desenvolvimento[486].

Assim sendo, a primeira medida está relacionada à documentação adequada do funcionamento organizacional da entidade responsável pela coleta e tratamento dos dados[487]. De fato, ser capaz de compreender como funciona a operação envolvendo dados pessoais, as pessoas nela envolvidas e as tarefas que desempenham dentro da organização é um elemento essencial não apenas sob o ponto de vista empresarial, mas também para a promoção de uma atuação responsável por parte dos agentes envolvidos. Realmente, um processo de documentação bem feito permite identificar pontos de falha e desenvolver as soluções necessárias em tempo hábil, evitando a ocorrência de vazamentos ou sanando-os antes que os danos se tornem graves. Nesses termos, embora as necessidades de documentação possam variar de acordo com o tamanho da organização responsável pela coleta e tratamento ou conforme os tipos de dados envolvidos[488], sua realização é importante para assegurar uma maior maturidade institucional no cuidado com a privacidade.

Para além desta finalidade "interna", a documentação do funcionamento organizacional também é relevante para os titulares dos dados pessoais eventualmente coletados e tratados pela entidade. Ainda que isto não signifique de forma obrigatória revelar e deixar disponíveis ao público todos os detalhes internos de funcionamento da organização[489], um nível de conhecimento adequado a respeito da utilização de métodos reconhecidos pela operação é algo importante, já que isto permite aos interessados adequar sua conduta frente a estas informações. Deveras, ao estabelecer a necessidade de realização de uma análise de impacto à privacidade, tanto o GDPR (em seu artigo 35) quanto a Lei Geral de Proteção de Dados brasileira (em seu artigo 38), estão justamente proporcionando a criação de um cenário mais favorável à disponibilização de informações a respeito da operação e ao desenvolvimento de relações de confiança entre os agentes envolvidos[490]. Da mesma maneira que o processamento, a publicização e transparência de informações quanto às pessoas, naturais e jurídicas,

---

[485] CAVOUKIAN, op. cit., 2012. p. 2.
[486] DIAKOPOULOS, op. cit., 2016. p. 62.
[487] KOOPS; LEENES, op. cit., 2014. p. 167.
[488] EUROPEAN DATA PROTECTION BOARD. **POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR.** Brussels: European Union, 2018.
[489] Para uma análise acerca das estratégias regulatórias envolvendo a disponibilização de informações e os efeitos destas no mercado, vide: SUNSTEIN, Cass. The Welfare Effects of Information. **Harvard Public Law Working Paper**, n. 18, dec. 2018.
[490] SCHNACKENBERG, Andrew K.; TOMLINSON, Edward C. Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. **Journal of Management**, v. 42, n. 7, p. 1784-1810, 2014. p. 1796.

responsáveis pela coleta e tratamento dos dados pessoais é algo importante, já que a simples ciência de um processamento irregular é insuficiente sem que seja possível estabelecer a adequada responsabilização daqueles eventualmente culpados por isso[491]. Justamente em razão disso, e consagrando as recomendações feitas pela comissão coordenada por Willis Ware na década de 1970, o GDPR (no artigo 15) e a LGDP (no artigo 41) também exigem que essa categoria de informações esteja ativamente disponível para os interessados.

Igualmente, além da transparência acima referida, é importante que em determinados casos a organização responsável pela coleta ou tratamento dos dados pessoais tome medidas adicionais para fazer chegar ao titular dos dados informações relevantes que possam vir a ser de seu interesse[492]. Deveras, este dever de manter uma postura proativa no que diz respeito ao fornecimento de informações é particularmente importante quando o acesso à informação pode prevenir ou, ao menos, reduzir a concretização de danos ao indivíduo titular dos dados pessoais. No caso do GDPR, o art. 34 do diploma impõe ao controlador responsável pela coleta ou tratamento o dever de comunicar, em linguagem acessível e em tempo hábil, o titular de dados nos casos em que houver vazamento de dados pessoais[493]. Obrigação semelhante está prevista no artigo 48 da Lei Geral de Proteção de Dados brasileira[494]. Considerando que em condições normais o mercado não necessariamente forneceria este tipo de informação[495], a intervenção regulatória em prol deste tipo de transparência se mostra relevante.

De fato, tomando como base o modelo regulatório proposto por Lessig, estratégias voltadas a reduzir a assimetria informacional entre os agentes de mercado também podem servir para induzir o processo de desenvolvimento de tecnologias mais transparentes. De início, a existência de mais informações sobre os sistemas eletrônicos disponíveis facilita a escolha dos agentes responsáveis pela demanda, contribuindo para a escolha dos produtos desenvolvidos

---

[491] HOUSE OF LORDS, op. cit., 2018. p. 135. De fato, tendo em vista a novidade do tema, tem-se cada vez mais estudado o tema da responsabilidade civil de desenvolvedores de sistemas eletrônicos, em particular de sistemas que utilizam inteligência artificial, numa tentativa de induzir a produção de algoritmos mais transparentes (HOUSE OF LORDS, op. cit., p. 135). Nesse mesmo sentido, vide: Lauren Scholz (SCHOLZ, Lauren Henry. Algorithmic Contracts. **Stanford Law Review**, v 20, n. 2, p. 128-169, fall 2017. p. 169) e Matthew Scherer (SCHERER, Matthew U. Regulating Artificial Intelligence Systems: Risks, Challenges, Competences, and Strategies. **Harvard Journal of Law & Technology**, v. 29, n. 2, p. 353-400, spring. 2016. p. 397-398).

[492] CALO, Ryan. Code, Nudge, or Notice? **Iowa Law Review**, v. 99, n. 2, p. 773-802, 2014. p. 799.

[493] EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679:** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Brussels: European Union, 2016. Não paginado

[494] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018.

[495] STIGLITZ, Joseph E. Government Failure vs. Market Failure: Principles of Regulation. In.: BALLEISEN, Edward J.; MOSS, David A. (eds.). **Governments and Markets:** Toward a New Theory of Regulation. Cambridge: Cambridge University Press, 2010. p. 26.

por organizações mais preocupadas em preservar a privacidade de seus usuários. Do lado da oferta, a existência de um regime de incentivos à coleta e ao tratamento transparente de informações pessoais poderia induzir mais organizações a competir pelo oferecimento de tecnologias mais atentas a estas necessidades[496].

Conforme salientado Danilo Doneda e Virgílio Almeida[497], a transparência não é algo necessariamente natural a tecnologias de informação e comunicação, sendo salutar a implementação de medidas de governança que induzam a redução da opacidade de algoritmos computacionais. Nesse cenário, estruturas de certificação e órgãos multisetoriais compostos por membros das sociedade civil, governo e agentes da indústria podem desempenhar um importante papel para a atenuação deste problema[498], em particular se considerarmos que nenhum destes setores possui capacidade para enfrentar a questão sozinho[499]. Levando em conta que o ambiente de alta tecnologia é complexo e marcado por um processo de mudança, a existência de espaços participativos que permitam reduzir assimetrias informacionais e possibilitem a aproximação de interesses em direção a um consenso é de extrema importância para uma atividade regulatória coerente[500].

Nesta senda, estruturas de certificação bem desenhadas podem ser fundamentais para incentivar o fornecimento de informações mais detalhadas quanto ao funcionamento de sistemas eletrônicos, possibilitando aos usuários compreender com mais profundidade o tratamento de seus dados pessoais[501], sem, contudo, prejudicar questões relacionadas à propriedade intelectual das tecnologias envolvidas. Ademais, estas mesmas ferramentas de certificação podem ser instrumentais no fortalecimento de medidas regulatórias baseadas em normas sociais, porquanto a obtenção de selos de certificação pode ser delineada de maneira a incentivar o desenvolvimento de sistemas mais transparentes e abertos.

---

[496] Conquanto não seja possível determinar se este é o motivo determinante, existem indícios de que grandes empresas passaram a competir mais fortemente em favor de demandas de transparência e responsabilidade no tratamento de dados pessoais a partir da edição do GDPR (PORTER, Jon. Google's Sundar Pichai snipes at Apple with privacy defense. **The Verge**, 8 may. 2019. Não paginado).

[497] DONEDA; ALMEIDA, op. cit., 2016, p. 62.

[498] REIDENBERG, op. cit., p. 588. HOUSE OF LORDS, op. cit., 2018. p. 138.

[499] Essa situação é reconhecida inclusive pela *Federal Trade Commission*, autoridade estadunidense responsável por regular questões relacionadas às políticas de direito do consumidor e antitruste (BRILL, Julie. **Scalable Approaches to Transparency and Accountability in Decisionmaking Algorithms**. Washington: Federal Trade Commission, 2015. p. 3).

[500] GASSER; ALMEIDA, op. cit., 2017. p. 58. COUNCIL OF EUROPE. Committee on Experts on Internet Intermediaries. **Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications.** Brussels: Council of Europe, 2017. p. 43-44.

[501] KELLEY, Patrick Gage. Designing a Privacy Label: Assisting Consumer Understanding of Privacy Practices. **Human Factors in Computing Systems.** p. 3347-3352, apr. 2009. p. 3352.

Em virtude das estratégias elencadas acima, a operação de coleta e tratamento de dados pessoais realizados por organizações também acaba, diante do estabelecimento de mecanismos de certificação e órgãos multisetoriais, por ser objeto de auditoria. Entretanto, para além das informações relacionadas à operação, é igualmente importante que se coletem dados e informações sobre o uso dos sistemas eletrônicos, em especial se estes sistemas são utilizados para a tomada de decisões por parte de agentes estatais[502]. Por certo, se um agente policial ou um magistrado utilizam algoritmos computacionais para decidir ou auxiliar na escolha da melhor decisão a ser utilizada frente a um determinado caso, é importante colher elementos que permitam posteriormente compreender a utilização destas ferramentas. Com base nestas informações, é possível identificar e tornar mais claros os vieses dos próprios agentes que utilizam estas tecnologias para decidir aspectos cada vez mais importantes do cotidiano e, assim, tomar as medidas adequadas e realizar eventuais correções quando necessário e, em sendo caso, penalizar eventuais os eventuais responsáveis caso estas medidas não sejam tomadas.

Não obstante todas as estratégias listadas acima, é importante ressaltar que o ideal de transparência *completa*, assim entendido como o acesso a todas as informações referentes à coleta e ao tratamento de dados pessoais, pode simplesmente não ser possível de atingir em sua plenitude, quer por motivos técnicos estritamente técnicos ou sociológicos[503]. Em especial nos casos envolvendo algoritmos de inteligência artificial, a exigência de maior transparência na forma de uma explicação pode, de acordo com parte dos pesquisadores[504], inclusive representar uma redução na qualidade das decisões fornecidas.

Diante deste cenário, faz-se necessário que nossa sociedade faça a devida reflexão entre os custos e benefícios de ter sistemas eletrônicos e algoritmos computacionais mais eficientes e eficazes para resolver problemas relevantes e urgentes que afetam nossas vidas ou ter algoritmos capazes de fornecer melhores explicações[505]. Deveras, existem indícios de que sistemas computacionais complexos podem ser muito uteis para enfrentas questões e desafios

---

[502] COURTLAND, op. cit., 2018, não paginado. SCASSA, Teresa. Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges. **Scripted**, v. 12, n. 2, p. 239-284, dec. 2017. p. 282-283.
[503] ANANNY; CRAWFORD, op. cit., 2018. p. 977-982.
[504] Conforme seção **4.2.2** acima.
[505] WEINBERGER, David. Optimization over Explanation. **Berkman Klein Center Collection**, 28 jan. 2018. Não paginado.

experimentados globalmente [506]. Todavia, estes mesmos algoritmos podem causar danos significativos a direitos individuais e coletivos, notadamente no que diz respeito à privacidade.

Definitivamente, o presente trabalho não tem a pretensão de apresentar uma solução final sobre esta questão, a qual inclusive não é o objeto desta pesquisa. Independentemente disso, é importante asseverar que, no que se refere à sua faceta de promoção da transparência e acesso a informações, uma política de *privacy by design* tem como efeito permitir a responsabilização e sanção das organizações e desenvolvedores responsáveis pelo desenvolvimento de sistemas eletrônicos que afetem de forma prejudicial os direitos fundamentais dos titulares de dados. Assim sendo, a despeito de entendermos como imperioso o investimento permanente em esforços para tornar as tecnologias de informação e comunicação mais transparentes, o estabelecimento de uma estrutura adequada de incentivos com o fortalecimento de sanções para os casos de violações de direitos é uma etapa essencial sem a qual a criação de algoritmos computacionais que respeitem direitos fundamentais não será possível [507]. Portanto, a transparência e o acesso à informação resultante implementação de um programa de *privacy by design*, neste caso, servem como medida instrumentalizante de direitos.

[506] Exemplificativamente, a Organização das Nações Unidas tem buscado utilizar e incentivar o uso de ferramentas de inteligência artificial com a finalidade de alcançar os objetivos de desenvolvimento sustável (UNITED NATIONS. **United Nations Activities on Artificial Intelligence.** New York: United Nations, 2018. p. v).
[507] UNITED NATIONS. General Assembly. **Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.** Washington: United Nations, 2018. p. 23.

5 CONCLUSÕES

O rápido desenvolvimento tecnológico experimentado nos últimos anos tem afetado profundamente a sociedade. De forma cada vez mais intensa, informações pessoais têm sido utilizadas por organizações públicas e privadas como insumo para seus processos e produtos. Neste contexto, tecnologias de informação e comunicação têm se mostrado cruciais para a própria existência e fruição de direitos fundamentais, porquanto o modo como são estruturadas é capaz de conformar, restringir ou efetivamente inviabilizar o exercício destes direitos.

Em virtude disso, a despeito da ausência de qualquer pretensão em esgotar a matéria, este trabalho buscou se aproximar da questão de maneira a buscar trazer subsídios para o debate sobre a regulação necessária para a promoção da transparência e proteção da privacidade. Igualmente, na medida do que é viável para um pesquisador da área do Direito, procurou-se estudar a questão da transparência de algoritmos computacionais sob a ótica da Ciência da Computação, de modo a entender melhor o possível alcance e limitações da regulação jurídica nesta matéria. Sendo assim, foi possível extrair dos estudos realizados neste trabalho as seguintes considerações finais:

- Considerando as reflexões realizadas pela doutrina jurídica estadunidense, constatou-se que a postura, num primeiro momento razoável, de passividade do Direito frente aos efeitos das tecnologias de informação e comunicação já não é a mais apropriada.
- O código-fonte e a arquitetura de tecnologias de informação e comunicação carrega consigo os valores e princípios inseridos, de forma consciente ou não, pelos seus desenvolvedores durante toda a sua vida útil; estes valores e princípios não necessariamente podem ser compatíveis com aqueles constitucionalmente protegidos;
- O processo de desenvolvimento e de *design* tecnológico é um momento estratégico para a intervenção do Direito porquanto é nele em que serão inseridos no código-fonte os valores e princípios de seus desenvolvedores;
- Embora as primeiras reflexões doutrinárias sobre a regulação de tecnologias tenham sido verificadas em solo estadunidense, pode-se dizer que na seara da proteção da privacidade a paulatina construção e consagração do *privacy by design* é fruto do trabalho constante dos legisladores europeus;

- Este processo de desenvolvimento e *design* de tecnologias pode ser influenciado de diversas maneiras, sendo algumas delas voltadas a atingir e influenciar o contexto organizacional e institucional onde o sistema é produzido e outras voltadas a atingir diretamente questões tecnológicas;
- Dentre as principais formas de intervenção regulatória, a transparência e o acesso a informações organizacionais e tecnológicas relacionadas ao processo de coleta e tratamento de dados pessoais é fundamental para a proteção da privacidade de grupos e indivíduos;
- A despeito de algumas diferenças, tanto o *General Data Protection Regulation* europeu como a Lei Geral de Proteção de Dados brasileira instrumentalizam a transparência e o acesso a informações como mecanismos indutores da proteção de dados pessoais e promoção do direito à privacidade;
- Estes diplomas buscaram fortalecer a auditabilidade do funcionamento organizacional e de todo o ciclo de vida de uma tecnologia de informação e comunicação, conferindo ao titular de dados pessoais o direito de acessar informações organizacionais e tecnológicas a respeito do processo de coleta e de tratamento de seus dados;
- Em especial, sob a perspectiva tecnológica, estes diplomas buscam promover, ainda que com limitações, a transparência do código-fonte de sistemas e das próprias decisões tomadas por, ou com base em, algoritmos computacionais; estas medidas transparência são particularmente relevantes na seara pública, tendo em vista a natureza da relação entre indivíduos e entes estatais;
- Conquanto estas medidas de transparência tecnológica sejam positivas, seu alcance esbarra em limites aos quais a Ciência da Computação ainda não possui soluções simples ou prontas;
- Diante deste cenário em que a transparência sob viés tecnológico é incapaz de resolver completamente o problema, vislumbra-se como necessário fortalecer a transparência sob o ponto de vista organizacional e institucional das entidades públicas e privadas que utilizam estes sistemas; com o acesso a estas informações, torna-se importante responsabilizar civil e, eventualmente, criminalmente os agentes e organizações responsáveis pelo desenvolvimento ou manutenção de sistemas eletrônicos que gerem danos a direitos fundamentais de grupos e indivíduos;

Não obstante estas conclusões, deve-se também levar em conta que atualmente problemas sociais e ambientais se tornam cada vez mais gravosos e urgentes. Em razão de sua extensão e gravidade, estes problemas talvez não possam mais ser relegados às próximas gerações. Neste cenário, tecnologias como inteligência artificial e algoritmos computacionais complexos podem, de acordo com o ponto de vista, representar uma promessa de solução para estas demandas que, em muitos casos, podem representar riscos existenciais para toda a humanidade. Diante disso, e ponderando o atual estágio da Ciência da Computação, talvez seja forçoso que nossa sociedade tenha que decidir entre: a) algoritmos mais transparentes, capazes de explicar suas decisões; b) algoritmos precisos, capazes resolver problemas complexos para os quais o cérebro humano não é capaz processar a quantidade massiva de dados necessária para a sua resolução.

REFERÊNCIAS

‘God of the Internet’ is dead. **BBC News**, London, 19 oct. 1998. Não paginado. Disponível em: <http://news.bbc.co.uk/2/hi/science/nature/196487.stm>. Acesso em: 01 mar. 2018.

ABITEBOUL, Serge; STOYANOVICH, Julia. Transparency, Fairness, Data Protection, Neutrality: Data Management Challenges in the Face of New Regulation. **arXiv**, 8 mar. 2019. Disponível em: < https://arxiv.org/abs/1903.03683>. Acesso em: 14 maio. 2019.

ABRAMS, S. David; BERTRAND, Mariane; MULLAINATHAN, Sendhil. Do Judges Vary in Their Treatment of Race? **The Journal of Legal Studies,** v. 41, n. 2, p. 347-384, jun. 2012. Disponível em: <http://www.jstor.org/stable/10.1086/666006>. Acesso em: 05 mar. 2019.

ACKERMAN, Evan. 60 Years of DARPA’s Favorite Toys: The Past and Future of Cutting-edge technology was on display at DARPA’s 60th anniversary conference. **IEEE Spectrum**, 26 set. 2018. Não paginado. Disponível em: < https://spectrum.ieee.org/tech-talk/aerospace/military/60-years-of-darpas-favorite-toys>. Acesso em: 05 mar. 2019.

ACQUISTI, Alessandro; FRIEDMAN, Allan; TELANG, Rahul. Is There a Cost to Privacy Breaches? An Event Study. **Proceedings of the 27th International Conference on Information Systems**. December 2006. Disponível em: <https://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf>. Acesso em: 22 out. 2018.

ADLER, Jonathan H. Most-cited law faculty, 2010-2014. **The Washington Post**, 19 may. 2016. Não paginado. Disponível em: <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/05/19/most-cited-law-faculty-2010-2014/?utm_term=.29c8fcd73aec>. Acesso em: 10 jun. 2018.

AKERLOF, George A. The Market for “Lemons”: Quality Uncertain and the Market Mechanism. **The Quarterly Journal of Economics**, v. 84, n. 3, p. 488-500, ago. 1970. Disponível em: < https://www.jstor.org/stable/1879431>. Acesso em: 13 fev. 2019.

ANGWIN, Julia *et ali*. Machine Bias: There’s software used across the country to predict future criminals. And it’s biased against blacks. **Pro Publica**, 23 may. 2016. Não paginado. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 17 abr. 2019.

ANANNY, Mike; CRAWFORD, Fate. Seeing without knowing: Limitations of the transparency ideal an its application to algorithmic accountability. **New Media and Society**, v. 20, n. 3, p. 973-989, 2018. Disponível em: < https://doi.org/10.1177%2F1461444816676645>. Acesso em: 12 maio. 2019.

BACH, David; NEWMAN, Abraham L. The European regulatory state and global public policy: micro-institutions, macro influence. **Journal of European Public Policy**, v. 14, n. 6, p. 827-846, 2007. Disponível em: <https://doi.org/10.1080/13501760701497659>. Acesso em: 04 fev. 2019.

BALDING, Christopher; CLARKE, Donald C. Who Owns Huawei? **SSRN**, 17 apr. 2019. Disponível em: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669>. Acesso em: 23 abr. 2019.

BANKSTON, Kevin. Facebook's New Privacy Changes: The Good, The Bad and The Ugly. **Electronic Frontier Foundation**, 9 dec. 2009. Não paginado. Disponível em: <https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>. Acesso em: 07 nov. 2018.

BARLET, Robert. Developments in the Law: The Law of Cyberspace. **Harvard Law Review**, v. 112, p. 1574-1704, 1999. Disponível em: <https://scholarship.law.berkeley.edu/facpubs/2386/>. Acesso em: 03 out. 2018.

BARLOW, John Perry. **A Declaration of the Independence of Cyberspace.** Davos: [.s.n.], 1996. Não paginado. Disponível em: <https://www.eff.org/cyberspace-independence>. Acesso em: 01 mar. 2018.

BARLOW, John Perry. The Economy of Ideas. **Wired**, 01 mar. 1994. Não paginado. Disponível em: <https://www.wired.com/1994/03/economy-ideas/>. Acesso em: 02 mar. 2018

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review**, v. 104, p. 671-732, 2016. Disponível em: < https://dx.doi.org/10.2139/ssrn.2477899>. Acesso em: 13 mar. 2019.

BECKER, Gary. Crime and Punishment: An Economic Approach. **Journal of Political Economy,** v. 76, n. 2, p. 169-217. mar./apr. 1968. Disponível em: <https://www.journals.uchicago.edu/doi/10.1086/259394>. Acesso em: 05 set. 2018.

BECKER, Gary S.; STIGLER, George J. Law Enforcement, Malfeasance, and Compensation of Enforcers. **The Journal of Legal Studies**, v. 3, n. 1, p. 1-18, jan. 1974. Disponível em: <http://www.jstor.org/stable/724119>. Acesso em: 05 set. 2018.

BELING, Graig T. Transborder Data Flows: International Privacy Protection and the Free Flow of Information. **Boston College International and Comparative Law Review**, v. 6, n. 2, p. 591-624, 1983. Disponível em: <https://lawdigitalcommons.bc.edu/iclr/vol6/iss2/9/>. Acesso em: 19 nov. 2018.

BELLOVIN, Steven M. *et allia.* It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law. **Harvard Journal of Law & Technology**, v. 30, n. 1, p. 1-101, fall. 2016. Disponível em: <http://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf>. Acesso em: 10 maio. 2019.

BENKLER, Yochai. **The Wealth of Networks:** How Social Production Transform Markets and Freedom. New Haven: Yale University Press, 2006. Disponível em: <http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf>. Acesso em: 20 mar. 2019.

BENTHAM, Jeremy. **The Works of Jeremy Bentham:** Published Under the Superintendence of his Executor John Bowring. Edinburgh: William Tait, 1838. 11v. em 4. Disponível em: <http://lf-oll.s3.amazonaws.com/titles/1925/0872.04_Bk.pdf>. Acesso em: 11 jun. 2018.

BERNERS-LEE, Tim. **Information Management:** a Proposal. Geneva: *Conseil Européen pour la Recherche Nucléaire*, 1989. Não paginado. Disponível em: <https://www.w3.org/History/1989/proposal.html>. Acesso em: 27 fev. 2018.

BINNS, Reuben. Data Protection Impact Assessments: a meta-regulatory approach. **International Data Privacy** Law, v. 7, n. 1, p. 22-35, 2017. Disponível em: <https://doi.org/10.1093/idpl/ipw027>. Acesso em: 18 jan. 2018.

BLACK, Henry Campbell. **Black's Law Dictionary.** 4. ed. rev. Saint Paul: West Publishing, 1968. Disponível em: <http://heimatundrecht.de/sites/default/files/dokumente/Black%27sLaw4th.pdf>. Acesso em: 11 jun. 2018.

BLOCH-WEHBA, Hannah. Access to Algorithms. **Fordham Law Review**, v. 88, p. 1-52, mar. 2019. Disponível em: < https://ssrn.com/abstract=3355776>. Acesso em: 03 maio. 2019.

BODÓ, Balázs; GIANNOPOLOU, Alexandra. The Logics of Technology Decentralization: the case of distributed ledger technologies. **Amsterdam Law School Legal Studies Research Papers**, n. 5, 2019. Disponível em: <https://ssrn.com/abstract=3330590>. Acesso em: 06 mar. 2019.

BOOCH, Grady. The Limits of Technology. **IBM Developer Works**, 13 jan. 2003. Disponível em: <https://www.ibm.com/developerworks/rational/library/2082-pdf.pdf>. Acesso em: 15. Jun. 2018.

BORSDOK, Paulina. How Anarchy Works. **Wired**, 01 oct. 1995. Não paginado. Disponível em: <https://www.wired.com/1995/10/ietf/>. Acesso em: 11 jun. 2018.

BRACHA, Oren; PASQUALE, Frank. Federal Search Commission: Access, Fairness, and Accountability in the Law of Search. **Cornell Law Review**, v. 93, n. 6, p. 1149-1210, 2008. Disponível em: < https://scholarship.law.cornell.edu/clr/vol93/iss6/11/>. Acesso em: 22 abr. 2019.

BRACKEN, Mike. AI: the impending tragedy of the Commons. **University College London Institute for Innovation and Public Purpose Blog**, 22 mar. 2018. Não paginado. Disponível em: < https://medium.com/iipp-blog/ai-the-impending-tragedy-of-the-commons-a972f91d9ecd>. Acesso em: 17 abr. 2019.

BRADFORD, Anu. The Brussels Effect. **Northwestern University Law Review**, v. 107, n. 1, p. 1-68, 2012. Disponível em: <https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss1/1/>. Acesso em: 04 fev. 2019.

BRANDEIS, Louis. **Other People's Money and How Bankers Use it.** New York: Frederick Stokes, 1914. Não paginado. Disponível em: <http://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-chapter-v>. Acesso em: 17 fev. 2018.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 8.503, de 2017**. Altera a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), para tornar expresso o direito de obter informações relativas à aquisição e funcionamento de softwares, hardwares e códigos mediadores de funções públicas e tornar obrigatória a disponibilização dos códigos-fonte dos algoritmos utilizados para a distribuição de processos nos órgãos do Poder Judiciário. Brasília: Câmara dos Deputados, 2017. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1594810&filename=PL+8503/2017>. Acesso em: 10 maio. 2018.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 mar. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 17 dez. 2018.

BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília: Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 22 jan. 2019.

BRILL, Julie. **Scalable Approaches to Transparency and Accountability in Decisionmaking Algorithms**. Washington: Federal Trade Commission, 2015. Disponível em: <https://www.ftc.gov/system/files/documents/public_statements/629681/150228nyualgorithms.pdf>. Acesso em: 15 maio. 2019.

BROWNSWORD, Roger. Code, Control, and Choice: why East is East and West is West. **Legal Studies**, v. 25, n. 1, p. 1-21, apr. 2006. Disponível em: < https://doi.org/10.1111/j.1748-121X.2005.tb00268.x>. Acesso em: 06 maio. 2019.

BROWNSWORD, Roger. In the Year 2061: from law to technological management. **Law, Innovation and Technology,** v. 7, n. 1, p. 1-51, jul. 2015. Disponível em: < https://doi.org/10.1080/17579961.2015.1052642>. Acesso em: 12 maio. 2019.

BURK, Dan L. Virtual Exit in the Global Information Economy. **Chicago-Kent Law Review**, v. 73, n. 4, p. 943-995, 1998. Disponível em: <http://scholarship.kentlaw.iit.edu/cklawreview/vol73/iss4/3/>. Acesso em: 10 abr. 2018.

BURREL, Jenna. How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. **Big Data & Society.** p. 1-12, jan./jun. 2016. Disponível em: <https://doi.org/10.1177%2F2053951715622512>. Acesso em: 03 maio. 2019.

BYGRAVE, Lee A. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. **Oslo Law Review**, v. 4, n. 2, p. 105-120, 2017. Disponível em: <https://ssrn.com/abstract=3035164>. Acesso em: 10 dez. 2018.

BYGRAVE, Lee. Minding the machine: art 15 of the EC Data Protection Directive and automated profiling. **Privacy Law and Policy Reporter**, v. 7, n. 4, 2000. Não paginado. Disponível em: <http://www5.austlii.edu.au/au/journals/PrivLawPRpr/2000/40.htm>. Acesso em: 24 fev. 2019.

CALO, Ryan. Code, Nudge, or Notice? **Iowa Law Review**, v. 99, n. 2, p. 773-802, 2014. Disponível em: < https://ssrn.com/abstract=2217013>. Acesso em: 14 maio. 2019.

CALORE, Michael. April 22, 1993: Mosaic Browser Lights Up Web With Color and Creativity. **Wired**, 22 apri. 2010. Não paginado. Disponível em: <https://www.wired.com/2010/04/0422mosaic-web-browser/>. Acesso em: 04 fev. 2019.

CAMARILLO, G. (ed.). **Request For Comments 5694:** Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability. Finland: Network Working Group, 2009. Disponível em: < https://tools.ietf.org/html/rfc5694>. Acesso em: 15 abr. 2019.

CAMPAGNUCCI, Fernanda. Algoritmos Públicos: Como a França está fazendo e por que deveríamos fazer também. **Um Dado a Mais**, 20 abr. 2019. Não paginado. Disponível em: < http://umdadoamais.com/algoritmos-publicos-como-a-franca-esta-fazendo-e-por-que-deveriamos-fazer-tambem/>. Acesso em: 22 abr. 2019.

CAMPBELL, Katherine et alli. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. **Journal of Computer Security.** v. 11, n. 3, p. 431-448, mar. 2003. Disponível em: <https://dl.acm.org/citation.cfm?id=876669>. Acesso em: 22 out. 2018.

CANADA. **Directive on Management of Information Technology.** Ottawa: Government of Canada, 2018. Disponível em: <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249>. Acesso em: 06 maio. 2019.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória da Internet no Brasil:** Do Surgimento das Redes de Computadores à Instituição dos Mecanismos de Governança. 2006. 239 f. Dissertação (Mestrado em Ciências de Engenharia de Sistema e Computação) – Faculdade de Engenharia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

CARVALHO, Welinton. Funções do Direito Comparado. **Revista de Informação Legislativa**, v. 44, n. 175, p. 139-145, 2007. Disponível em: <http://www2.senado.leg.br/bdsf/handle/id/140971>. Acesso em: 17 jul. 2018.

CASTELVECCHI, Davide. Can we open the black box of AI? **Nature**, v. 538, n. 7623, p. 21-23, oct. 2016. Disponível em: < https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731>. Acesso em: 14 maio. 2019.

CAVOUKIAN, Ann. **Operationalizing Privacy by Design:** a Guide to Implementing Strong Privacy Practices. Ontario: Information and Privacy Commissioner, 2012. Disponível em: <http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf>. Acesso em: 17 out. 2018.

CAVOUKIAN, Ann. **Privacy by Design**. Ontario: Information and Privacy Commissioner, 2009. Disponível em: <http://www.ontla.on.ca/library/repository/mon/23002/289982.pdf>. Acesso em: 24 jan. 2019.

CAVOUKIAN, Ann. **Privacy by Design in Law, Policy and Practice:** a White Paper for Regulators, Decision-Makers and Policy-makes. Ontario: Information and Privacy Commissioner: 2011. Disponível em: <http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf>. Acesso em: 05 jan. 2019.

CAVOUKIAN, Ann. **Privacy Risk Management:** Building Privacy Protection into a Risk Management Framework. Ontario: Information and Privacy Commissioner, 2010. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/2010/04/privacy-risk-management-building-privacy-protection-into-a-risk-management-framework-to-ensure-that-privacy-risks-are-managed.pdf>. Acesso em: 22 jan. 2019.

CAVUSOGLU, Huseyin; MISHRA, Birendra; RAGHUNATHAN, Srinivasan. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. **International Journal of Electronic Commerce**, v. 9, n. 1, p. 69-104, 2004. Disponível em: <https://doi.org/10.1080/10864415.2004.11044320>. Acesso em: 22 out. 2018.

CERF, Vinton G. Building an Internet Free of Barriers. **New York Times**, New York, 27 jul. 1997. Não paginado. Disponível em: <https://partners.nytimes.com/library/cyber/week/072797cerf.html>. Acesso em: 01 mar. 2018.

CERF, Vinton G.; KAHN, Robert E. A Protocol for Packet Network Intercommunication. **IEEE Transactions on Communications**, v. 22, n. 4, p. 637-648, may. 1974. Disponível em: <https://www.cs.princeton.edu/courses/archive/fall08/cos561/papers/cerf74.pdf>. Acesso em: 27 fev. 2018.

CHARETTE, Robert N. Why Software Fails: We waste billions of dollars each year on entirely preventable mistakes. **IEEE Spectrum**, 2 set. 2005. Não paginado. Disponível em: <https://spectrum.ieee.org/computing/software/why-software-fails>. Acesso em: 12 mar. 2019.

CHACON, Eduarda Moraes. Resistência do Direito à Tecnologia: uma análise teubiana de comunicação e regulação. **The Law, State and Telecommunications Review**, v. 10, n. 2, p. 67-102, oct. 2018. Disponível em: < https://doi.org/10.26512/lstr.v10i2.21494>. Acesso em: 10 maio. 2019.

CHAUM, David. Achieving Electronic Privacy. **Scientific American,** p. 96-101, ago. 1996. Disponível em: <https://chaum.com/publications/ScientificAmerican-AEP.pdf>. Acesso em: 03 out. 2018.

CHAUM, David. Security Without Identification: Transactions Systems to Make Big Brother Obsolete. **Communications of the ACM**, v. 28, n. 10, p. 1030-1044, oct. 1985. Disponível em: <https://dl.acm.org/citation.cfm?id=4373>. Acesso em: 02 out. 2018.

CHEN, Lei. Curse of Dimensionality. *In.:* LIU, Ling; OZSU, Tamer (Eds.). **Encyclopedia of Database Systems.** Boston: Springer, 2019. Não paginado. Disponível em: <https://doi.org/10.1007/978-0-387-39940-9>. Acesso em: 08 abri. 2019.

CHURCHILL, Winston. House of Commons Rebuilding. **Commons Sitting**, 28 oct. 1943. Disponível em: <https://api.parliament.uk/historic-hansard/commons/1943/oct/28/house-of-commons-rebuilding>. Acesso em: 10 maio. 2018.

CITRON, Danielle; CALO, Ryan. The Automated Administrative State. **The Ethical Machine**, 8 apr. 2019. Não Paginado. Disponível em: <https://ai.shorensteincenter.org/ideas/2019/4/3/the-automated-administrative-state>. Acesso em: 03 maio. 2019.

CITRON, Danielle Keats. Technological Due Process. **Washington University Law Review**, v. 85, n. 6, p. 1249-1313, 2008. Disponível em: < https://ssrn.com/abstract=1012360>. Acesso em: 22 mar. 2019.

CLANCY, Thomas K. The Importance of James Otis. **Mississippi Law Journal**, v. 82, n. 2, p. 487-523, 2013. Disponível em: <https://ssrn.com/abstract=2111601>. Acesso em: 03 jul. 2018.

CLARK, David D. **Views of the Future:** A Cloudy Crystal Ball – Visions of the Future. [s.l.]: *I*nternet Engineering Task Force, 1992. Disponível em: <https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf>. Acesso em: 01 mar. 2018.

CLARKE, Roger. Privacy Impact Assessment: Its Origins and Development. **Computer Law & Security Review**, v. 25, n. 2, p. 123-135, 2009. Disponível em: <https://doi.org/10.1016/j.clsr.2009.02.002>. Acesso em: 18 jan. 2019.

COASE, Ronald H. **Prize Lecture**: The Institutional Structure of Production. Stockholm: Nobel Foundation, 1991. Não paginado. Disponível em: <https://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/1991/coase-lecture.html>. Acesso em: 10 maio. 2018.

COASE, Ronald H. The Problem of Social Cost. **Journal of Law and Economics**, v. 3, p. 1-44, 1960. Disponível em: <http://www.jstor.org/stable/724810?origin=JSTOR-pdf>. Acesso em: 10 maio. 2018.

COMMISSION OF THE EUROPEAN COMMUNITIES. **Commission Declaration:** on the protection of individuals in relation to the processing of personal data in the Community and Information security. Brussels: European Community, 1990. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990DC0314&from=EN>. Acesso em: 06 dez. 2018.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Methodology for Privacy Risk Management.** Paris: CNIL, 2018. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>. Acesso em: 22 jan. 2019.

COOK, Stephen. **The P versus NP Problem.** Peterborough: Clay Institute of Mathematics, 2018. Disponível em: < http://www.claymath.org/sites/default/files/pvsnp.pdf>. Acesso em: 11 abri. 2019.

COPELAND, Jack B. The Church-Turing Thesis. In.: ZALTA, Edward N. (ed.) **The Stanford Encyclopedia of Philosophy.** Stanford: Stanford University, 2019. Não paginado. Disponível em: < https://plato.stanford.edu/archives/spr2019/entries/church-turing/>. Acesso em: 09 abri. 2019.

COPELAND, Jack B; SHAGRIR, Oron. The Church-Turing Thesis: Logical Limit or Breachable Barrier? **Communications of the ACM,** v. 62, n. 1, p. 66-74, 2019. Disponível em: <https://cacm.acm.org/magazines/2019/1/233526-the-church-turing-thesis/pdf>. Acesso em: 09 abri. 2019.

CORBET-DAVIES, Sam *et allia*. Algoritmic Decision Making and the Cost of Fairness. **Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, p. 797-806, ago. 2017. Disponível em: < https://doi.org/10.1145/3097983.3098095>. Acesso em: 14 maio. 2019.

CORMACK, Andrew. Can CSIRTs Lawfully Scan for Vulnerabilities? **Scripted**, v. 11, n. 3, p. 308-319, dec. 2014. Disponível em: < https://script-ed.org/wp-content/uploads/2014/12/cormack.pdf>. Acesso em: 12 maio. 2019.

COTTON, Michelle. *et alli.* **Request for Comments 8126:** Guidelines for Writing an IANA Considerations Section in RFC. Los Angeles: Internet Engineering Task Force, 2017. Disponível em: < https://tools.ietf.org/html/bcp26>. Acesso em: 22 abr. 2019.

COUNCIL OF EUROPE. Committee of Experts on Internet Intermediaries. **Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications.** Brussels: Council of Europe, 2017. Disponível em: < https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a>. Acesso em: 14 maio. 2019.

COUNCIL OF EUROPE. **Convention 108**: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg: Council of Europe, 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>. Acesso em: 05 dez. 2018.

COUNCIL OF EUROPE. COMMITTEE OF MINISTERS. **Resolution (73) 22**. On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector. Strasbourg: Council of Europe, 1973. Disponível em: <https://rm.coe.int/native/0900001680502830>. Acesso em 05 dez. 2018

COUNCIL OF EUROPE. EUROPEAN COMMITTEE ON LEGAL CO-OPERATION. **Addendum I to the Report on the 19th meeting of the CCJ.** Strasboug: Council of Europe, 1973. Disponível em: <https://rm.coe.int/09000016806ce693>. Acesso em: 05 dez. 2018.

COUNCIL OF EUROPE. **Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Data.** Strasbourg: Council of Europe, 1981. Disponível em:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434>. Acesso em: 05 dez. 2018.

COURTLAND, Rachel. Bias detectives: the researchers striving to make algorithms fair. **Nature**, 20 jun. 2018. Não paginado. Disponível em: < https://www.nature.com/articles/d41586-018-05469-3>. Acesso em: 06 maio. 2019.

CRICHTON, Danny. How Do You Fight an Algorithm You Cannot See? **TechCrunch**, 15 jan. 2019. Não paginado. Disponível em: <https://techcrunch.com/2019/01/15/how-do-you-fight-an-algorithm-you-cannot-see/>. Acesso em: 15 abr. 2019.

DAM, Kenneth W. Self-Help in the Digital Jungle. **Journal of Legal Studies**, v. 28, n. 2, p. 393-412, jun. 1999. Disponível em: <https://www.journals.uchicago.edu/doi/pdfplus/10.1086/468056>. Acesso em: 06 set. 2018.

DAVID, Paul A.; SHAPIRO, Joseph S. Community-Based Production of Open Source Software: What Do We Know about the Developers Who Participate? **SSRN**, 23 sep. 2008. Disponível em: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1286273>. Acesso em: 15 abr. 2019.

DAVIES, Rob; RUSHE, Dominic. Amazon becomes world's second company to be valued at $1tn. **The Guardian**, 4 set. 2018. Não paginado. Disponível em: <https://www.theguardian.com/technology/2018/sep/04/amazon-becomes-worlds-second-1tn-company>. Acesso em: 22 out. 2018.

DESAI, Deven R.; KROLL, Joshua A. Trust but Verify: A Guide to Algorithms and the Law. **Harvard Journal of Law and Technology**, v. 31, p. 1-64, 2018. Disponível em: < https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech1.pdf>. Acesso em: 17 abr. 2019.

DEXE, Jacob. **Constraining the Digital World**: Structuring net neutrality regulation through the lens of Lessig's New Chicago School model. Lund: Lund University, Department of Political Science, 2015. Disponível em: <http://lup.lub.lu.se/student-papers/record/7759234>. Acesso em: 06 mar. 2019.

DIAKOPOULOS, Nicholas. Accountability in Algorithmic Decision Making. **Communications of the ACM**, v. 59, n. 2, p. 56-62, feb. 2016. Disponível em: < https://dl.acm.org/citation.cfm?id=2844110>. Acesso em: 15 maio. 2019.

DIBBEL, Julian. A Rape in Cyberspace: How na Evil Clown, a Haitian Trickster Spirit, Two Wizards and a Cast of Dozens Turned a Database Into a Society. **The Village Voice**, 23 dez. 1993. Não paginado. Disponível em: <http://www.juliandibbell.com/texts/bungle_vv.html>. Acesso em: 18 jun. 2018.

DOMINGOS, Pedro. A Few Useful Things to Know About Machine Learning. **Communications of the ACM**, v. 55, n. 10, p. 78-87, oct. 2012. Disponível em: <https://doi.org/10.1145/2347736.2347755>. Acesso em: 26 mar. 2019.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. What is Algorithm Governance? **IEEE Internet Computing**. v. 20, n. 4, p. 60-63, jul./ago. 2016. Disponível em: <https://doi.org/10.1109/MIC.2016.79>. Acesso em 22 jan. 2019.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

DREYFUSS, Emily. Tech Illiteracy is a Huge Threat to Our Government. **Wired**, 11 may. 2017. Não paginado. Disponível em: <https://www.wired.com/2017/05/real-threat-government-tech-illiteracy/>. Acesso em: 10 jun. 2018.

DUCKET, Chris; BARBASCHOW, Asha. The laws of Australia will trump the laws of mathematics: Turnbull. **ZDNET**, 14 jul. 2017. Não paginado. Disponível em: < https://www.zdnet.com/article/the-laws-of-australia-will-trump-the-laws-of-mathematics-turnbull/>. Acesso em: 10 maio. 2019.

DUCH-BROWN, Néstor. **The Competitive Landscape of Online Platforms.** Brussels: European Commission, 2017. Disponível em: <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc106299.pdf>. Acesso em: 04 fev. 2019.

DURUMIC, Zakir *et alli*. The Matter of Heartbleed. **Proceedings of the 2014 Conference on Internet Measurement Conference,** p. 475-488, 2014. Disponível em: < https://doi.org/10.1145/2663716.2663755>. Acesso em: 21 mar. 2019.

DWOSKIN, Elizabeth. Why You Can't Trust You're Getting The Best Deal Online: A Study Finds Discriminatory Pricing On E-Commerce Sites Is More Widespread Than Thought. **The Wall Street Journal,** 23oct. 2012. Não paginado. Disponível em: <https://www.wsj.com/articles/why-you-cant-trust-youre-getting-the-best-deal-online-1414036862>. Acesso em: 08 jan. 2018.

DYSON, Esther et alli. Cyberspace and the American Dream: A Magna Carta for the Knowledge Age. **The Information Society**, v. 12, n. 3, p. 295-308, 1996. Disponível em: <https://doi.org/10.1080/019722496129486>. Acesso em: 01 mar. 2018.

EASTERBROOK, Frank H. Cyberspace and the Law of the Horse. **The University of Chicago Legal Forum**, p. 207-216, 1996. Disponível em: <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles>. Acesso em: 05 mar. 2018.

EASTERBROOK, Frank H. Cyberspace versus Property Law. **Texas Review of Law and Politics**, v. 4, p. 103-113, 1999. Disponível em: <https://chicagounbound.uchicago.edu/journal_articles/1156/>. Acesso em: 06 mar. 2019.

EDWARDS, Haley Sweetland. How the First Amendment Became a Tool for Deregulation. **Time**, 19 jul. 2018. Não paginado. Disponível em: < http://time.com/5342749/first-amendment-deregulation/>. Acesso em: 10 maio. 2019.

EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: from a "Right to Explanation" to a "Right to Better Decisions"?. **IEEE Security & Privacy**, v. 16, n. 3, p. 46-54, may/jun,

2018. Disponível em: <https://doi.org/10.1109/MSP.2018.2701152>. Acesso em: 01 mar. 2019.

EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a "Right to an Explanation" is Probably not the Remedy you are Looking For. **Duke Law & Technology Review**, v. 16, n. 1, p. 18-81, 2017. Disponível em: < https://scholarship.law.duke.edu/dltr/vol16/iss1/2/>. Acesso em: 05 abr. 2019.

EUROPEAN COMMISSION. Commission outlines next steps towards a European data economy. **European Commission,** 10 jan. 2017. Não paginado. Disponível em: <http://europa.eu/rapid/press-release_IP-17-5_en.htm?locale=en>. Acesso em: 07 nov. 2018.

EUROPEAN COMMISSION. **Commission Staff Working Paper:** Impact Assessment on Regulation Proposal. Brussels: European Union, 2012. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0072>. Acesso em: 10 dez. 2018.

EUROPEAN COMMISSION. **Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy.** Brussels: European Union, 2017. Não paginado. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0228>. Acesso em: 23 jan. 2019.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan.** Brussels: European Commission, 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:22:FIN>. Acesso em: 05 maio. 2019.

EUROPEAN COMMISSION. **Proposal for a Regulation of the European Parliament and of the Council:** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Brussels: European Union, 2012. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0011:FIN>. Acesso em: 12 dez. 2018.

EUROPEAN DATA PROTECTION BOARD. **POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR.** Brussels: European Union, 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422>. Acesso em: 14 maio. 2019.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 5/2018:** Preliminary Opinion on Privacy by Design. Brussels: EDPS, 2018. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf>. Acesso em: 01 out. 2018.

EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Directive 95/46/EC:** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Luxembourg, 1995. Disponível em: <https://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Acesso em: 06 dez. 2018.

EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Directive 99/5/EC:** on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity. Brussels: European Union, 1999. Disponível em: <https://eur-lex.europa.eu/eli/dir/1999/5/oj>. Acesso em: 10 dez. 2018.

EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Directive 2002/58/EC:** concerning the processing of personal data and the protection of privacy in the electronic communications sector. Brussels: European Union, 2002. Disponível em: <http://data.europa.eu/eli/dir/2002/58/oj>. Acesso em: 10 dez. 2018.

EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Regulation (EU) 2016/679:** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Brussels: European Union, 2016. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 10 dez. 2018.

EUROPEAN PARLIAMENT. COUNCIL OF THE EUROPEAN UNION. **Regulation (EC) 765/2008:** setting out the requirements for accreditation and market surveillance relating to the marketing of products. Brussels: European Union, 2008. Disponível em: <http://data.europa.eu/eli/reg/2008/765/oj>. Acesso em: 23 jan. 2019.

EUROPEAN UNION. **Treaty on the Functioning of the European Union.** Rome: European Union, 2012. Não paginado. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT>. Acesso em: 10 dez. 2018.

EUROPEAN UNION. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.** Brussels: Article 29 Data Protection Working Party, 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826>. Acesso em: 06 maio. 2019.

EUROPEAN UNION. Commission of the European Communities. **Amended Proposal for a Council Directive:** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Brussels: Commission of the European Communities, 1992. Disponível em: <http://aei.pitt.edu/10375/1/10375.pdf>. Acesso em: 01 mar. 2019.

EUROPEAN UNION. Council of the European Communities. **Proposal For A Council Directive Concerning The Protection Of Individuals In Relation To The Processing Of Personal Data.** Brussels: European Union, 1990. Não paginado. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51990PC0314(01)>. Acesso em: 18 fev. 2019.

ELECTRONIC FRONTIER FOUNDATION. **About EFF.** San Francisco: Electronic Frontier Foundation, 2018. Não paginado. Disponível em: <https://www.eff.org/about>. Acesso em: 01 mar. 2018.

FELTEN, Edward W.; KROLL, Joshua A. Heartbleed Shows Government Must Lead on Internet Security. **Scientific American**, 1 jul. 2014. Não paginado. Disponível em: <https://www.scientificamerican.com/article/heartbleed-shows-government-must-lead-on-internet-security1/>. Acesso em: 21 mar. 2019.

FOROUZAN, Behrouz; MOSHARRAF, Firouz. **Fundamentos da Ciência da Computação.** 2 ed. São Paulo: Cengage Learning, 2011.

FOUCAULT, Michel. **Discipline & Punish:** The Birth of the Prison. New York: Vintage Books, 1995. Disponível em: <https://monoskop.org/images/4/43/Foucault_Michel_Discipline_and_Punish_The_Birth_of_the_Prison_1977_1995.pdf>. Acesso em: 09 maio. 2018.

FREITAS, Juarez. **A Interpretação Sistema do Direito.** 5. ed. São Paulo: Malheiros, 2010.

FREITAS, Juarez. Direito Administrativo e Inteligência Artificial. **Interesse Público**, Belo Horizonte, ano 21, n. 114, p. 15-29, mar./abr. 2019.

FREITAS, Marcio Luiz Coelho de. Entre tecnodeterminismo e interesse público: limites e possibilidades de regulação da internet. **Revista de Direito, Estado e Telecomunicações,** Brasília, v. 10, n. 1, p. 125-146, maio. 2018. Disponível em: <https://doi.org/10.26512/lstr.v10i1.21503>. Acesso em: 10 maio. 2019.

FRIEDMAN, Batya; NISSENBAUM, Helen. Discerning Bias in Computer Systems. **93 Conference Companion on Human Factors in Computing Systems.** p. 141-142, apr. 1993. Disponível em: <https://dl.acm.org/citation.cfm?id=260152>. Acesso em: 03 nov. 2018.

FRIEDMAN, Batya; NISSENBAUM, Helen. Bias in Computer Systems. **ACM Transactions on Information Systems**. v. 14, n. 3, p. 330-347, jul. 1996. Disponível em: <https://dl.acm.org/citation.cfm?id=230561>. Acesso em: 03 nov. 2018.

FROOMKIN, Michael A. The Internet as a Source of Regulatory Arbitrage. **Symposium on Information, National Policies, and International Infrastructure**, jan. 1996. Não paginado. Disponível em: <http://osaka.law.miami.edu/~froomkin/articles/arbitr.htm>. Acesso em: 03 set. 2018.

FROOMKIM, Michael A. "PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology. **Ohio State Law Journal**, v. 74, n. 6, p. 965-994, 2013. Disponível em: <https://repository.law.miami.edu/fac_articles/66/>. Acesso em: 03 out. 2018.

GARE, Arran. Systems Theory and Complexity Introduction. **Democracy & Nature**, v. 6, n. 3, p. 327-339, 2000. Disponível em: < https://philarchive.org/archive/GARSTA-9>. Acesso em: 06 mar. 2019.

GARFINKEL, Simson *et alli*. Toward Algorithmic Transparency and Accountability. **Communications of the ACM**, v. 60, n. 9, p. 5, set. 2017. Disponível em: <http://dx.doi.org/10.1145/3125780>. Acesso em: 20 mar. 2019.

GASSER, Urs; ALMEIDA, Virgílio A. F. A Layered Model fo AI Governance. **IEEE Internet Computing**, v. 21, n. 6, p. 58-62, nov./dez. 2017. Disponível em: < https://doi.org/10.1109/MIC.2017.4180835>. Acesso em: 14 maio. 2019.

GELLMAN, Robert M. Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions. **Software Law Journal,** v. 6, n. 2, p. 199-238, 1993. Disponível em: <https://www.bobgellman.com/rg-docs/rg-softwarelj.pdf>. Acesso em: 19 nov. 2018.

GELLMAN, Robert. Willis Ware's Lasting Contribution to Privacy: Fair Information Principles. **IEEE Security & Privacy,** v. 12, n. 4, p. 51-54, 2014. Disponível em: <https://ieeexplore.ieee.org/document/6876241>. Acesso em: 12 maio. 2019.

GIBBONS, Llewellyn Joseph. No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. **Cornell Journal of Law and Public Policy**, v. 6, n. 3, p. 475-551, 1997. Disponível em: <http://scholarship.law.cornell.edu/cjlpp/vol6/iss3/1/>. Acesso em: 06 mar. 2018.

GILBERT, Francoise. Privacy v. Data Protection: What is the Difference. **Privacy, Security, and Cloud Computing.** 1 oct. 2014. Não paginado. Disponível em: <https://www.francoisegilbert.com/?m=201410>. Acesso em: 12 dez. 2018.

GILBERT, Jonathan. Computer Bulletin Board Operator Liability for User Misuse. **Fordham Law Review**, v. 54, n. 3, p. 439-454, 1985. Disponível em: <https://repository.jmls.edu/jitpl/vol12/iss2/1/>. Acesso em: 02 mar. 2018.

GIUDICE, James M. Through the Lens of Complex Systems Theory: Why Regulators Must Understand the Economy and Society as a Complex System. **University of Richmond Law Review**, v. 51, p. 101-119, 2016. Disponível em: <https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1142&context=law-student-publications>. Acesso em: 06 mar. 2019.

GHOLAMI, Ali et ali. Privacy Threat Modeling for Emerging Biobank Clouds. **Procedia Computer Science,** v. 37, p. 489-496. 2014. Disponível em: <https://doi.org/10.1016/j.procs.2014.08.073>. Acesso em: 22 jan. 2019.

GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithm Decision-Making and a "Right to Explanation". **AI Magazine**, v. 38, n. 3, p. 1-9, 2017. Disponível em: < https://arxiv.org/abs/1606.08813>. Acesso em: 04 abr. 2019.

GONÇALVES, Eduardo Vicente. **Hacktivism and its Struggle in Changing the World:** The Aaron Swartz Case, Access to Knowledge and Economic Model. 2017. Dissertation (MA in Sociology Research). Department of Sociology, University of Essex, Essex, 2017. Disponível em: < https://cuducos.me/hacktivism/hacktivism-and-its-struggle-in-changing-the-world.pdf>. Acesso em: 25 fev. 2019.

GORSUCH, Neil. Of Lions and Bears, Judges and Legislators, and the Legacy of Justice Scalia. **Case Western Reserve Law Review**, v. 66, n. 4, p. 905-920, 2016. Disponível em: <https://scholarlycommons.law.case.edu/caselrev/vol66/iss4/3/>. Acesso em: 28 jun. 2018.

GOSSERIES, Axel; PARR, Tom. Publicity. **The Stanford Encyclopedia of Philosophy.** Stanford: Stanford University, 2018. Não paginado. Disponível em: <https://plato.stanford.edu/archives/win2018/entries/publicity/>. Acesso em: 05 mar. 2019.

GREENBERG, Andy. Triple Meltdown: How so many researchers found a 20-year-old chip flaw at the same time. **Wired**, 07 jan. 2018. Não paginado. Disponível em: <https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/>. Acesso em: 21 mar. 2019.

GREENLEAF, Graham. The Influence of European data privacy standards outside Europe: implications for globalization of Convention 108. **International Data Privacy Law**, v. 2, n. 2, p. 68-92, 2012. Disponível em: <https://doi.org/10.1093/idpl/ips006>. Acesso em: 23 nov. 2018.

GRIMMELMANN, James. Regulation by Software. **Yale Law Journal**, v. 114, p. 1719-1758, 2005. Disponível em: <https://ssrn.com/abstract=2358693>. Acesso em: 17 set. 2018.

GUAMÁN, Danny. Privacy vs. Data Protection vs. Information Security. **Software and Services Engineering**, 01 nov. 2016. Não Paginado. Disponível em: <http://blogs.upm.es/sse/2016/11/01/privacy-vs-data-protection-vs-information-security/>. Acesso em: 12 dez. 2018.

GURSES, Seda; TRONCOSO, Carmela; DIAZ, Claudia. Engineering Privacy by Design. **Conference on Computers, Privacy & Data Protection**, p. 1-25, 2011. Disponível em: <https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf>. Acesso em: 24 jan. 2019.

HAGE, Jaap. **Comparative Law as Method and the Method of Comparative Law**. Maastricht European Private Law Institute Working Paper, n. 11, mar. 2014. Disponível em: <https://dx.doi.org/10.2139/ssrn.2441090>. Acesso em: 22 out. 2018.

HANSEN, Marit; KÖHNTOPP, Kristian; PFITZMANN, Andreas. The Open Source Approach: opportunities and limitations with respect to security and privacy. **Computers & Security**, v. 21, n. 5, p. 461-471, 2002. Disponível em: < https://doi.org/10.1016/S0167-4048(02)00516-3>. Acesso em: 20 mar. 2019.

HARDIN, Garret. The Tragedy of the Commons. **Science**, v. 162, n. 3859, p. 1243-1248, dec. 1968. Disponível em: <http://science.sciencemag.org/content/162/3859/1243/tab-pdf>. Acesso em: 23 mar. 2018.

HARVARD LAW REVIEW. State v. Loomis: Wisconsin Supreme Court Require Warning Before Use of Algorithmic Risks Assessments in Sentencing. **Harvard Law Review**, n. 130, p. 1530-1537. 2017. Disponível em: <http://harvardlawreview.org/wp-content/uploads/2017/03/1530-1537_online.pdf>. Acesso em: 03 maio. 2019.

HILLENIUS, Gijs. Basque Country's open source law invites other European administrators. **Joinup – European Commission,** 14 ago. 2012. Não paginado. Disponível em: < https://joinup.ec.europa.eu/news/basque-countrys-open-source>. Acesso em: 06 maio. 2019.

HILLENIUS, Gijs. European Parliament increases budget for EU Free and Open Software Auditing. **EU-FOSSA**, 29 oct. 2016. Não paginado. Disponível em: < https://joinup.ec.europa.eu/news/european-parliament-increases-0>. Acesso em: 05 maio. 2019.

HOEPMAN, Jaap-Henk. Privacy Design Strategies. **Privacy Law Scholars Conference.** Berkeley: Privacy Law Scholars Conference, 2013. Disponível em: <https://arxiv.org/abs/1210.6621v2>. Acesso em: 25 fev. 2019.

HONG, Jason I. et al. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. **DIS '04 Proceedings of the 5th conference on Designing Interactive Systems.** Cambrigde: Association for Computing Machinery, 2004. Disponível em: <https://doi.org/10.1145/1013115.1013129>. Acesso em: 22 jan. 2018.

HOUSE OF LORDS. Select Committee on Artificial Intelligence. **AI in the UK:** ready, willing and able? London: House of Lords, 2018. Disponível em: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>. Acesso em: 05 maio. 2019.

HUGHES, Eric. **A Cypherpunk's Manifesto.** [s.l.: s.n.], 1993. Não paginado. Disponível em: < https://www.activism.net/cypherpunk/manifesto.html>. Acesso em: 03 out. 2018.

HUNT, Reed. The Future of the Net – Comments on Lawrence Lessig's Code and Other Laws of Cyberspace and The Future of Ideas. **Brooklyn Law Review**, v. 68, n. 1, p. 289-308. 2002. Disponível em: <https://brooklynworks.brooklaw.edu/blr/vol68/iss1/5/>. Acesso em: 31 ago. 2018.

INFORMATION AND PRIVACY COMMISSIONER; REGISTRATIEKAMER. **Privacy-Enhancing Technologies:** the path to anonymity. Toronto, The Hague: Information and Privacy Commissioner; Registratiekamer, 1995. Disponível em: <http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf>. Acesso em: 03 out. 2018.

INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS. **History of the Conference.** [s.n.s.l.]: 2018. Não paginado. Disponível em: <https://icdppc.org/the-conference-and-executive-committee/history-of-the-conference/>. Acesso em: 10 dez. 2018.

INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS. **Resolution on Privacy by Design**. Jerusalem: ICDPP, 2010. Disponível em: <https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf>. Acesso em: 10 dez. 2018.

INTERNET ACTIVITIES BOARD. **Request for Comments 1087:** Ethics and the Internet. [s.l.]: Internet Activities Board, 1989. Disponível em: <https://tools.ietf.org/html/rfc1087>. Acesso em: 03 out. 2018.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. **The IANA Functions:** an Introduction to the Internet Assigned Numbers Authority (IANA) Fuctions. Los Angeles: Internet Corporation for Assigned Names and Numbers, 2015. Disponível em: <https://www.iana.org/about/informational-booklet.pdf>. Acesso em: 02 mar. 2018.

INSTITUTE OF ELECTRIC AND ELECTRONIC ENGINEERS. **IEEE Position Statement:** In Support of Strong Encryption. Piscataway: IEEE Board of Directors, 2018. Disponível em: <http://globalpolicy.ieee.org/wp-content/uploads/2018/06/IEEE18006.pdf>. Acesso em: 10 maio. 2019.

ISRANI, Ellora Thadaney. When an Algorithm Helps Send you to Prison. **New York Times**, 26 out. 2017. Não Paginado. Disponível em: <https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html>. Acesso em: 11 fev. 2019.

JAHN, Gabriele; SCHRAMM, Mathias; SPILLER, Achim. The Reliability of Certification: Quality Labels as a Consumer Policy Tool. **Journal of Consumer Policy**, v. 28, n. 1, p. 53-73, 2005. Disponível em: <https://doi.org/10.1007/s10603-004-7298-6>. Acesso em: 23 jan. 2019.

JOHNSON, Bobbie. Privacy is no Longer a Social Norm, Says Facebook Founder. **The Guardian**, 11 jan. 2010. Não paginado. Disponível em: <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>. Acesso em: 07 nov. 2018.

JOHNSON, David R.; POST, David. And How Shall the Net be Governed? A Meditation on the Relative Virtues of Decentralized Emergent Law. In: KAHIN, Brian; KELLER, James H (eds.). **Coordinating the Internet.** Cambridge: MIT Press, 1997. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6275249>. Acesso em: 05 mar. 2018.

JOHNSON, David R.; POST, David. Chaos Prevailing in Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems. **Chicago-Kent Law Review**, v. 73, n. 4, p. 1055-1099, 1998. Disponível em: <http://scholarship.kentlaw.iit.edu/cklawreview/vol73/iss4/5/>. Acesso em: 05 mar. 2018.

JOHNSON, David R.; POST, David. Law and Borders: The Rise of Law in Cyberspace. **Stanford Law Review**, v. 48, p. 1367-1402, 1996. Disponível em: <https://ssrn.com/abstract=535>. Acesso em: 05 mar. 2018.

JOHNSON, David R.; POST, **David. The New 'Civic Virtue' of the Internet:** A Complex Systems Model for the Governance of Cyberspace. [s.l.]: The Emerging Internet, 1998. Disponível em: <http://www.temple.edu/lawschool/dpost/Newcivicvirtue.html>. Acesso em: 05 mar. 2018.

KANG, Cecilia. Tech Industry Pursues a Federal Privacy Law, on Its Own Terms. **The New York Times,** 26 ago. 2018. Não paginado. Disponível em: <https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html>. Acesso em: 19 nov. 2018.

KATZ, Michael L.; SHAPIRO. Systems Competition and Network Effects. **The Journal of Economic Perspectives.** v. 8, n. 2, p. 93-115, 1994. Disponível em: <http://www.jstor.org/stable/2138538>.Acesso em: 03 out. 2018.

KATZ, Michael L.; SHAPIRO, Carl. Network Externalities, Competition, and Compatibility. **The American Economic Review**, v. 75, n. 3, p. 424-440. jun. 1985. Disponível em: <https://www.jstor.org/stable/1814809>. Acesso em: 03 out. 2018.

KELLEY, Patrick Gage. Designing a Privacy Label: Assisting Consumer Understanding of Privacy Practices. **Human Factors in Computing Systems.** p. 3347-3352, apr. 2009. Disponível em: < https://dl.acm.org/citation.cfm?id=1520484>. Acesso em: 06 maio. 2019.

KERCKHOFF, Auguste. La Cryptographie Militaire, **Journal des Sciences Militaries**, v. IX, p. 5-38, jan. 1883. Disponível em: <https://www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf>. Acesso em: 17 abr. 2019.

KNUTH, Donald Erving. **The Art of Computer Programming:** fundamental algorithms. 3 ed. Reading: Addison-Weiley, 1997. Disponível em: <http://broiler.astrometry.net/~kilian/The_Art_of_Computer_Programming%20-%20Vol%201.pdf>. Acesso em: 25 mar. 2019.

KOOPS, Bert-Jaap; LEENES, Ronald. Privacy Regulation Cannot be Hardcoded. A critical comment on the "privacy by design" provision in data-protection law. **International Review of Law, Computers & Technology**, v. 28, n. 2, p. 159-171, 2014. Disponível em: <https://doi.org/10.1080/13600869.2013.801589>. Acesso em: 25 fev. 2019.

KOOPS, Bert-Jaap. The (In)Flexibility of Techno-Regulation and the Case of Purpose-Binding. **Legisprudence**, v. 5, n. 2, p. 171-194, 2011. Disponível em: < https://doi.org/10.5235/175214611797885701>. Acesso em: 12 maio. 2019.

KROENER, Inga; WRIGHT, David. A Strategy for Operationalizing Privacy by Design. **The Information Society**, v. 30, p. 355-365, 2014. Disponível em: <https://doi.org/10.1080/01972243.2014.944730>. Acesso em: 24 jan. 2019.

KROLL, Josua *et ali*. Accountable Algorithms. **University of Pennsylvania Law Review**, v. 165, n. 3, p. 633-705, 2017. Disponível em: <https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/>. Acesso em: 01 abr. 2019.

LANDES, William M.; POSNER, Richard A. The Independent Judiciary in an Interest-Group Theory. **The Journal of Law and Economics**, v. 18, n. 3, p. 875-901. dec. 1975. Disponível em: <https://www.jstor.org/stable/725070>. Acesso em: 05 set. 2018.

LARSON, Jeff *et alli*. How We Analyzed the COMPAS Recidivism Algorithm. **Pro Publica**, 23 may. 2016. Não paginado. Disponível em: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. Acesso em: 17 abr. 2019.

LEINER, Barry M. *et alli*. **Brief History of the Internet.** Reston: Internet Society, 1997. Disponível em: <https://cdn.prod.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf>. Acesso em: 26 fev. 2018.

LESK, Michael. Trust, but Verify. **IEEE Security & Privacy**, v. 12, n. 6, p. 94-96, nov./dec. 2014. Disponível em: < https://ieeexplore.ieee.org/document/7006407>. Acesso em: 05 maio. 2019.

LESSIG, Lawrence. **Code 2.0.** New York: Basic Books, 2006. Disponível em: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 09 maio. 2018.

LESSIG, Lawrence. **Governance.** [s.l.]: CPSR Conference on Internet Governance, 1998. Disponível em: <https://cyber.harvard.edu/works/lessig/cpsr.pdf>. Acesso em: 28 ago. 2018

LESSIG, Lawrence. Open Code and Open Societies: Values of Internet Governance. **Chicago-Kent Law Review**, v. 74, p. 101-116. 1999 Disponível em: <https://cyber.harvard.edu/works/lessig/final.PDF>. Acesso em: 28 ago. 2018.

LESSIG, Lawrence. The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulations. **Common Law Conspectus**, v. 5, p. 181-191, 1997. Disponível em: <http://scholarship.law.edu/commlaw/vol5/iss2/5/>. Acesso em: 03 jun. 2018.

LESSIG, Lawrence. The New Chicago School. **The Journal of Legal Studies**, v. 27, n. 2, p. 661-691, 1998. Disponível em: <http://www.jstor.org/stable/10.1086/468039>. Acesso em: 05 jun. 2018.

LESSIG, Lawrence. The Path of Cyberlaw. **Yale Law Journal**, v. 104, p. 1743-1755, 1995. Disponível em: <http://chicagounbound.uchicago.edu/journal_articles/7777/>. Acesso em: 10 abr. 2018.

LESSIG, Lawrence. The Zones of Cyberspace. **Stanford Law Review**, v. 48, p. 1403-1411, 1996. Disponível em: <http://www.jstor.org/stable/1229391>. Acesso em: 02 jun. 2018.

LEVINE, David S. Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure. **Florida Law Review**, v. 59, p. 135-193, 2007. Disponível em: < https://ssrn.com/abstract=900929>. Acesso em: 12 maio. 2019.

LICKLIDER, Joseph Carl Robnett. **Memorandum for Members and Affiliates of the Intergalactic Network.** Washington: Advanced Research Projects Agency, 1963. Não paginado. Disponível em: <http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network>. Acesso em: 26 fev. 2018.

LIPP, Moritz *et allia*. Meltdown: Reading kernel memory from user space. **Proceedings of the 27th USENIX Conference on Security Symposium**, p. 973-990, 2018. Disponível em: <https://meltdownattack.com/meltdown.pdf>. Acesso em: 21 mar. 2019.

LIPSHUTZ, Brian. Justice Thomas and the Originalist Turn in Administrative Law. **Yale Law Journal Forum**, v. 127, p. 94-103, 2015. Disponível em: <https://ssrn.com/abstract=2633211>. Acesso em: 28 jun. 2018.

LEE, Irene *et alli.* Computational Thinking for Youth in Practice. **ACM Inroads**, v. 2, n. 1, p. 32-37, mar. 2011. Disponível em: < https://users.soe.ucsc.edu/~linda/pubs/ACMInroads.pdf>. Acesso em: 03 maio. 2019.

LEHR, David; OHM, Paul. Playing with the Data: What Legal Scholars Should Learn About Machine Learning. **University of California Law Review**, v. 51, p. 653-717, 2017. Disponível

em: < https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Lehr_Ohm.pdf>. Acesso em: 15 abr. 2019.

LEMLEY, Mark A.; MCGOWAN, David. Legal Implications of Network Economic Effects. **California Law Review**, v. 86, n. 3, p. 481-611, 1998. Disponível em: <http://dx.doi.org/https://doi.org/10.15779/Z38T42N>. Acesso em: 04 out. 2018.

LIPTON, Zachary C. The Mythos of Model Interpretability. **ACM Queue**, v. 16, n. 3, p. 1-27, may-jun. 2018. Disponível em: < https://dl.acm.org/citation.cfm?id=3236386.3241340>. Acesso em: 10 maio. 2019.

LYNSKEY, Orla. Regulation by Platforms: the Impact on Fundamental Rights. In.: BELLI, Luca; ZINGALES, Nicolo (ed.). **Platform Regulations:** How Plataforms are Regulated and How they Regulate Us. Rio de Janeiro: Fundação Getúlio Vargas, 2017. Disponível em: <http://hdl.handle.net/10438/19402>. Acesso em: 04 out. 2018.

MALGIERI, Gianclaudio; COMANDÉ. Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 4, p. 243-265, nov. 2017. Disponível em: <https://academic.oup.com/idpl/article/7/4/243/4626991>. Acesso em: 10 maio. 2019.

MALKIN, Gary Scott (ed.). **Request for Comments 1983:** Internet Users' Glossary. Burlington: 1996. Disponível em: < https://tools.ietf.org/html/rfc1983>. Acesso em: 25 fev. 2019.

MARKOFF, John. Willis Ware, 93, Engineer at Dawn of Computer Age, Dies. **The New York Times**, 01 dez. 2013. Não paginado. Disponível em: <https://www.nytimes.com/2013/12/02/technology/willis-ware-who-helped-build-blueprint-for-computer-design-dies-at-93.html>. Acesso em: 26 nov. 2018.

MAZUR, Joanna. Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law. **Erasmus Law Review**, n. 3, p. 178-189, dec. 2018. Disponível em: < http://www.erasmuslawreview.nl/tijdschrift/ELR/2019/01/ELR_2018_011_003_004>. Acesso em: 23 abri. 2019.

MCCULLAGH, Declan. Lessig Suffers from Bad Code. **Wired,** 06 out. 1999. Não paginado. Disponível em: < https://www.wired.com/1999/10/lessig-suffers-from-bad-code/>. Acesso em: 29 ago. 2018.

MCCULLOCH, Gretchen. Coding is for Everyone – As Long as You Speak English. **Wired**, 08 apr. 2019. Não paginado. Disponível em: < https://www.wired.com/story/coding-is-for-everyoneas-long-as-you-speak-english>. Acesso em: 09 abri. 2019.

MCCULLAGH, Declan. What Larry Didn't Get. **Cato Unbound**, 4 may. 2009. Não paginado. Disponível em: <https://www.cato-unbound.org/2009/05/04/declan-mccullagh/what-larry-didnt-get>. Acesso em: 10 maio. 2018.

MCGOWAN, David. Legal Implications of Open-Source Software. **University of Illinois Law Review**, v. 2001, n. 1, p. 241-304, 2001. Disponível em: < https://illinoislawreview.org/wp-content/uploads/2000/12/McGowan.pdf>. Acesso em: 17 abr. 2019.

MCKNIGHT, Lee W.; BAILEY, Joseph P. An Introduction to Internet Economics. **Journal of Electronic Publishing** v. 1, n. 1&2, jan. 1995. Não paginado. Disponível em: < http://dx.doi.org/10.3998/3336451.0001.123>. Acesso em: 10 maio. 2019.

MILLER, Arthur R. Personal Privacy in the Computer Age: The Challenge of a New Technology. **Michigan Law Review,** v. 67, n. 6, p. 1089-1246, apr. 1969. Disponível em: <https://www.jstor.org/stable/1287516>. Acesso em: 23 nov. 2018.

MITCHELL, William J. **City of Bits:** space, place, and the infobahn. Cambrigde: MIT Press, 1996. Disponível em: <https://mitpress.mit.edu/books/city-bits>. Acesso em: 10 jun. 2018.

MOCKAPETRIS, Paul. **Request for Comments 882:** Domain Names – Concepts and Facilities. [s.l.]: Network Workink Group, 1983. Disponível em: <https://tools.ietf.org/html/rfc882>. Acesso em: 27 fev. 2018.

MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. "Não existe o que panoramicamente vemos no céu": o ponto-cego do direito (políticas públicas sobre regulação em ciência e tecnologia. In.: SAAVEDRA, Giovani Agostini; LUPION, Ricardo (orgs.). **Direitos Fundamentais:** direito privado e inovação. Porto Alegre: EdiPUCRS, 2012.

MONICO, João Francisco Galera *et alli*. Acurácia e Precisão: revendo os conceitos de forma acurada. **Boletim de Ciências Geodésicas.** v. 15, n. 3, p. 469-483, jul-set. 2009. Disponível em: < https://revistas.ufpr.br/bcg/article/view/15513/10363>. Acesso em: 08 abri. 2019.

MONTORO, André Franco. **Introdução à Ciência do Direito.** 27. ed. rev. atual. São Paulo: Revista dos Tribunais, 2008.

MOODY, Glyn. If Software Is Funded from a Public Source, Its Code Should Be Open Source. **Linux Journal.** 4 fev. 2019. Não paginado. Disponível em:< https://www.linuxjournal.com/content/if-software-funded-public-source-its-code-should-be-open-source>. Acesso em: 05 maio. 2019.

MOORE, Gordon E. Cramming More Components onto Integrated Circuits. **Electronics**, p. 114-117, april. 1965. Disponível em: <http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf>. Acesso em: 15 fev. 2018.

MUEHLHAUSER, Luke. Transparency in Safety-Critical Systems. **Machine Intelligence Research Institute**, 25 ago. 2013. Não paginado. Disponível em: <https://intelligence.org/2013/08/25/transparency-in-safety-critical-systems/>. Acesso em: 02 maio. 2019.

MULLIGAN, Deirdre K. The Enduring Importance of Privacy. **IEEE Security & Privacy,** v. 12, n. 3, p. 61-65, mai./jun. 2014. Disponível em: <https://ieeexplore.ieee.org/document/6824537>. Acesso em: 12 maio. 2019.

MURRAY, Andrew; SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. **Modern Law Review**, v. 65, n. 4. P. 491-516, jul. 2002. Disponível em: <https://doi.org/10.1111/1468-2230.00392>. Acesso em: 03 set. 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Risk Management Framework for Information Systems and Organizations.** Washington: NIST, 2018. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>. Acesso em: 22 jan. 2019.

NETANEL, Neil Weinstock. Cyberspace 2.0. **Texas Law Review**, v. 79, p. 447-491, dez. 2000. Disponível em: <https://ssrn.com/abstract=252557>. Acesso em: 01 mar. 2018.

NETANEL, Neil Weinstock. Cyberspace Self-Governance: a Skeptical View from a Liberal Democracy Theory. **California Law Review**, v. 88, n. 2, p. 395-498, 2000. Disponível em: <http://scholarship.law.berkeley.edu/californialawreview/vol88/iss2/8/>. Acesso em: 23 mar. 2018.

NISSENBAUM, Helen. Values in the Design of Computer Systems. **Computers and Society**. p. 38-39, mar. 1998. Disponível em: < https://doi.org/10.1145/277351.277359>. Acesso em: 03 nov. 2018.

NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus**, v. 140, n. 4, p. 32-48, 2011. Disponível em: <http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf>. Acesso em: 03 nov. 2018.

NISSEMBAUM, Helen. Respecting Context to Protect Privacy: Why Meaning Matters. **Science and Engineering Ethics**, v. 24, n. 3, p. 831-852, 2015. Disponível em: <https://doi.org/10.1007/s11948-015-9674-9>. Acesso em: 03 nov. 2018.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anounymization. **University of California Law Review**, v. 57, p. 1701-1777, 2010. Disponível em: < https://www.uclalawreview.org/pdf/57-6-3.pdf>. Acesso em: 06 fev. 2019.

OLSON JUNIOR, Mancur. **The Logic of Collective Action**: Public Goods and the Theory of Groups. Cambridge: Harvard University Press, 1971.

OPEN SOURCE INIATIATIVE. **The Open Source Definition.** S.l.: OSI, 2007. Não paginado. Disponível em: < https://opensource.org/osd>. Acesso em: 21 mar. 2019.

ORACLE. **Java Platform Standard Edition Technical Documentation**. [s.l.]: Oracle, 2019. Não paginado. Disponível em: <https://www.oracle.com/technetwork/java/javase/documentation/index.html>. Acesso em: 25 mar. 2019.

ORBACH, Barak. What is Regulation? **Yale Journal on Regulation Online**, v. 30, n. 1, p. 1-10, 2012. Disponível em: <https://ssrn.com/abstract=2143385>. Acesso em: 11 jun. 2018.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Recommendation Of The Council Concerning Guidelines Governing The Protection Of**

Privacy And Transborder Flows Of Personal Data. Paris: OECD, 1980. Disponível em: < http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. Acesso em: 26 out. 2018.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Digital Economy Outlook 2017.** Paris: OECD, 2017. Disponível em: <http://dx.doi.org/10.1787/9789264276284-en>. Acesso em: 22 out. 2018.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Science, Technology and Innovation Outlook 2016.** Paris: OECD, 2016. Disponível em: <http://www.oecd.org/sti/oecd-science-technology-and-innovation-outlook-25186167.htm>. Acesso em: 18 jul. 2018.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Digital Security Risk Management for Economic and Social Prosperity.** Paris: OECD, 2015. Disponível em: < https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>. Acesso em: 01 out. 2018.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Managing Digital Security and Privacy Risk.** Paris: OECD, 2016. Disponível em: <https://dx.doi.org/10.1787/5jlwt49ccklt-en>. Acesso em: 06 mar. 2019.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines.** Paris: OECD, 2013. Disponível em: <https://doi.org/10.1787/20716826>. Acesso em: 10 dez. 2018.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD Privacy Framework.** Paris: OECD, 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 01 out. 2018.

PAGALLO, Ugo. On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In.: GURVITS, S. et alli (eds.). **European Data Protection**: in good health?. Amsterdam: Springer, 2012. Disponível em: < http://dx.doi.org/10.1007/978-94-007-2903-2_16>. Acesso em: 25 fev. 2019.

PASQUALE, Frank. Restoring Transparency to Automated Authority. **Journal on Telecommunications and High Technology Law**, v. 9. p. 235-256, 2011. Dispinível em: <https://ssrn.com/abstract=1762766>. Acesso em: 20 mar. 2019.

PELTZMAN, Sam. Toward a More General Theory of Regulation. **The Journal of Law and Economics**, v. 19, n.2, p. 211-240, 1976. Disponível em: <https://www.journals.uchicago.edu/doi/10.1086/466865>. Acesso em: 05 set. 2018.

PERRIT JUNIOR, Henry H. Book Review: Lawrence Lessig, Code and Other Laws of Cyberspace. **Connecticut Law Review**, v. 32, p. 1061-1064, mar. 2000. Disponível em: <http://scholarship.kentlaw.iit.edu/fac_schol/446>. Acesso em: 29 ago 2018.

PFITZMANN, Andreas; HANSEN, Marit. **A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management.** Dresden: Faculty of Computer Science, 2010.

Disponível em: <https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf>. Acesso em: 31 jan. 2019.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL. Biblioteca Central Ir. José Otão. **Modelo de Referências Elaborado pela Biblioteca Central Irmão José Otão**. Disponível em: <http://www.pucrs.br/biblioteca/modelos>. Acesso em: 01 mar; 2018.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL. Biblioteca Central Ir. José Otão. **Modelo para apresentação de citações em documentos elaborado pela Biblioteca Central Irmão José Otão.** 2011**.** Disponível em: <http://www.pucrs.br/biblioteca/modelos>. Acesso em: 05 mar. 2018.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL. Biblioteca Central Ir. José Otão. **Modelo para apresentação de trabalhos acadêmicos, teses e dissertações elaborado pela Biblioteca Central Irmão José Otão**. 2011. Disponível em: <www.pucrs.br/biblioteca/trabalhosacademicos>. Acesso em: 28 fev. 2018.

PORTER, Jon. Google's Sundar Pichai snipes at Apple with privacy defense. **The Verge**, 8 may. 2019. Não paginado. Disponível em: <https://www.theverge.com/2019/5/8/18536604/google-sundar-pichai-privacy-op-ed-nyt-regulation-apple-cook-advertising-targeting-user-data>. Acesso em: 14 maio. 2019.

POSNER, Eric. Why Originalism is So Popular. **The New Republic**, 14 jan. 2011. Não paginado. Disponível em: <https://newrepublic.com/article/81480/republicans-constitution-originalism-popular>. Acesso em: 28 jun. 2018.

POSNER, Richard A. Theories of Economic Regulation. **The Bell Journal of Economics and Management Science**, v. 5, n. 2, p. 335-258, 1974. Disponível em: <http://www.jstor.org/stable/3003113>. Acesso em: 11 jun. 2018.

POST, David G. Against "Against Cyberanarchy". Berkeley Technology Law Journal, v. 17, p. 1366-1387, 2002. Disponível em: <https://ssrn.com/abstract=334581>. Acesso em: 05 mar. 2018.

POST, David G. Anarchy, State, and the Internet: an Essay on Law-Making in Cyberspace. **Journal of Online Law**, 1995. Disponível em: <http://www.temple.edu/lawschool/dpost/Anarchy.html>. Acesso em: 02 mar. 2018.

POST, David G. Governing Cyberspace. **Wayne Law Review**, v. 43, p. 155-171, 1996. Disponível em: <https://ssrn.com/abstract=11477>. Acesso em: 05 mar. 2018.

POST, David G. What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace. **Stanford Law Review**, v. 52, p. 1439-1459, may. 2000. Disponível em: <https://ssrn.com/abstract=251014>. Acesso em: 05 mar. 2018.

POST, David G. The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed. **Indiana Journal of Global Legal Studies**, v. 5, n. 2, p. 521-543, 1998. Disponível em: <https://www.repository.law.indiana.edu/ijgls/vol5/iss2/8/>. Acesso em: 03 abr. 2018.

POSTEL, Jon. **Request for Comments 349:** Proposed Standard Socket Numbers. Los Angeles: Network Working Group, 1972. Disponível em: <https://tools.ietf.org/html/rfc349>. Acesso em: 01 mar. 2018.

POSTEL, Jon. **Request for Comments 1591:** Domain Name Structure and Delegation. Marina Del Rey: Network Working Group, 1994. Disponível em: <https://www.ietf.org/rfc/rfc1591.txt>. Acesso em: 01 mar. 2018.

PROSSER, Tony. Two Visions of Regulation. **Regulation in the Age of Crisis.** Dublin: University Colledge Dublin, 2010. Disponível em: <http://regulation.upf.edu/dublin-10-papers/1H1.pdf>. Acesso em: 10 maio. 2019.

RADIN, Margaret Jane; WAGNER, R. Polk. The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace. **Chicago-Kent Law Review**, v. 73, p. 1295-1317, 1998. Disponível em: <http://scholarship.law.upenn.edu/faculty_scholarship/744/>. Acesso em: 23 mar. 2018.

RAYMOND, Eric Steven. **The Cathedral and the Bazaar:** Musings on Linux and Open Source by an Accidental Revolutionary. Sebastobol: O'Reilly, 2001. Disponível em: <https://monoskop.org/images/e/e0/Raymond_Eric_S_The_Cathedral_and_the_Bazaar_rev_ed.pdf>. Acesso em: 20 mar. 2019.

REED, Chris. How to Make Bad Law: Lessons from Cyberspace. **Modern Law Review**, v. 73, n. 6, p. 903-932, 2010. Disponível em: <https://dx.doi.org/10.1111/j.1468-2230.2010.00824.x>. Acesso em: 12 maio. 2019.

REIDENBERG, Joel R. The Privacy Obstacle Course: Hurding Barriers to Transnational Financial Services. **Fordham Law Review**, v. 60, n. 6, p. 137-177, 1992. Disponível em: < https://ir.lawnet.fordham.edu/flr/vol60/iss6/9/>. Acesso em: 10 maio. 2019.

REIDENBERG, Joel. Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? **Federal Communications Law Journal**, v. 44, n. 2, p. 196-243, 1992. Disponível em: <https://ir.lawnet.fordham.edu/faculty_scholarship/800/>. Acesso em: 19 nov. 2018.

REIDENBERG, Joel R. Governing Networks and Rule-Making in Cyberspace. **Emory Law Journal**, v. 45, p. 911-930, 1996. Disponível em: <https://ir.lawnet.fordham.edu/faculty_scholarship/29/>. Acesso em: 03 abr. 2018.

REIDENBERG, Joel R. Lex Informatica: The Formulation of Information Policy Rules through Technology. **Texas Law Review**, v. 76, n. 3, p. 553-593, fev. 1998. Disponível em: <http://ir.lawnet.fordham.edu/faculty_scholarship/42/>. Acesso em: 06 mar. 2018.

RIBEIRO, Marco Tulio; SINGH, Sameer; GUESTRIN, Carlos. "Why Should I Trust You?" Explaining the Predictions of Any Classifier. **Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**, p. 1135-1144, ago. 2016. Disponível em: < https://arxiv.org/pdf/1602.04938.pdf>. Acesso em: 08 abri. 2019.

RICHARDS, Neil M.; SOLOVE, Daniel J. Prosser's Privacy Law: A Mixed Legacy. **California Law Review,** v. 98, p. 1887-1924, 2010. Disponível em: <https://ssrn.com/abstract=1567693>. Acesso em: 03 out. 2018.

ROBERTS, Lawrence G. The Evolution of Packet Switching. **Proceedings of the IEEE**, v. 66, n. 11, p. 1307-1313, nov. 1978. Disponível em: <http://www.packet.cc/files/ev-packet-sw.html>. Acesso em: 27 fev. 2018.

ROCHET, Jean Charles; TIROLE, Jean. Two-Sided Markets: a progress report. **The RAND Journal of Economics**, v. 37, n. 3, p. 645-667, 2006. Disponível em: <http://www.jstor.org/stable/25046265>. Acesso em: 04 out. 2018.

RODRIGUES, Rowena; WRIGHT, David; WADHWA, Kus. Developing a Privacy Seal Scheme (that works). **International Data Privacy Law**, v. 3, n. 2, p. 100-116, 2013. Disponível em: < https://doi.org/10.1093/idpl/ips037>. Acesso em: 23 jan. 2019.

RODRIGUES, Rowena et al. The Future of Privacy Certification in Europe: an Exploration of Options under Article 42 of the GDPR. **International Review of Law, Computers & Technology**, v. 30, n. 3, p. 248-270, 2016. Disponível em: <https://doi.org/10.1080/13600869.2016.1189737>. Acesso em: 23 jan. 2019.

ROTENBERG, Marc. Fair Information Practices and the Architecture of Privacy: What Larry Doesn't Get. **Stanford Technology Law Review**, v. 1, 2001. Disponível em: <http://stlr.stanford.edu/STLR/ Articles/01_STLR_1/index.htm>. Acesso em: 31 ago. 2018.

RUSSEL, Andrew L. 'Rough Consensus and Running Code' and the Internet-OSI Standards War. **IEEE Annals of the History of Computing**, v. 28, n. 3, p. 48-61, jul./set. 2006. Disponível em: <https://doi.org/10.1109/MAHC.2006.42>. Acesso em: 12 jun. 2018.

RUSSEL, Andrew L. OSI: The Internet that Wasn't. **IEEE Spectrum**, 30 jul, 2013. Disponível em: < https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt>. Acesso em: 06 mar. 2019.

RUSTAD, Michael L; KOENIG, Thomas H. Towards a Global Data Privacy Standard. **Suffolk University Legal Studies Research Paper Series,** n. 18, p. 1-89, set. 2018. Disponível em: <https://ssrn.com/abstract=3239930>. Acesso em: 23 nov. 2018.

SALMON, Felix. Musk, Zuckerberg, Bezos, and Ethically Iffy 'Philanthropy". **Wired**, 15 may. 2018. Não paginado. Disponível em: <https://www.wired.com/story/musk-zuckerberg-bezos-and-ethically-iffy-philanthropy/>. Acesso em: 10 jun. 2018.

SALTZER, J.H.; REED, D.P.; CLARK, D.D. End-to-end Arguments in System Design. **ACM Transactions on Computer Systems,** v. 2, n. 4, p. 277-288, 1984. Disponível em: <https://dl.acm.org/citation.cfm?id=357402>. Acesso em: 18 jun. 2018.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. rev. atual. ampl. Porto Alegre: Livraria do Advogado, 2015.

SCALIA, Antonin. Originalism: The Lesser Evil. **University of Cincinnati Law Review**, n. 57, p. 849-856, 1989. Disponível em: <https://web.archive.org/web/20160919161713/https://www.law.uc.edu/sites/default/files/Scalia%201988%20Taft%20Lecture.pdf>. Acesso em: 28 jun. 2018.

SCASSA, Teresa. Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges. **Scripted**, v. 12, n. 2, p. 239-284, dec. 2017. Disponível em: <https://script-ed.org/wp-content/uploads/2017/12/scassa.pdf>. Acesso em: 12 maio. 2019.

SCHERER, Matthew U. Regulating Artificial Intelligence Systems: Risks, Challenges, Competences, and Strategies. **Harvard Journal of Law & Technology**, v. 29, n. 2, p. 353-400, spring. 2016. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>. Acesso em: 14 maio. 2019.

SCHNACKENBERG, Andrew K.; TOMLINSON, Edward C. Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. **Journal of Management**, v. 42, n. 7, p. 1784-1810, 2014. Disponível em: <https://doi.org/10.1177%2F0149206314525202>. Acesso em: 15 maio. 2019.

SCHOLZ, Lauren Henry. Algorithmic Contracts. **Stanford Law Review**, v 20, n. 2, p. 128-169, fall 2017. Disponível em: < https://ssrn.com/abstract=2747701>. Acesso em: 14 maio. 2019.

SCHRYEN, Guido. Is Open Source Security a Myth? **Communications of the ACM**, v. 54, n. 5, p. 130-140, may. 2010. Disponível em: < http://doi.org/10.1145/1941487.1941516>. Acesso em: 21 mar. 2019.

SCHWARTZ, Paul M. Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices. **Wisconsin Law Review**, v. 2000, n. 1, p. 743-788. 2000. Disponível em: <https://scholarship.law.berkeley.edu/facpubs/423/>. Acesso em: 31 ago. 2018.

SELBST, Andrew; POWLES, Julia. Meaningful Information and the Right to Explanation. **International Data Privacy Law**, v. 7, n. 4, p. 233-242, nov. 2017. Disponível em: < https://academic.oup.com/idpl/article/7/4/233/4762325>. Acesso em: 17 abr. 2019.

SHELANSKI, Howard A. Information, Innovation, and Competition Policy for the Internet. **University of Pennsylvania Law Review**, v. 161, n. 3, p. 1663-1705, 2013. Disponível em: <https://scholarship.law.upenn.edu/penn_law_review/vol161/iss6/6/>. Acesso em: 04 out. 2018.

SHENK, David; SHAPIRO, Andrew J.; JOHNSON, Steven. **Technorealism**. [s.l., s.n.]: 1998. Não paginado. Disponível em: <http://www.technorealism.org/>. Acesso em: 29 ago. 2018.

SMITS, Jan M. Comparative Law and its Influence on National Legal Systems. In.: REIMANN, Mathias; ZIMMERMANN, Reinhard (eds.), **The Oxford Handbook of Comparative Law**. Oxford: Oxford University Press, 2006. Disponível em: <https://ssrn.com/abstract=965389>. Acesso em: 22 out. 2018.

SNEED, Annie. Moore's Law Keeps Going, Defying Expectations. **Scientific American**, 19. maio. 2015. Não paginado. Disponível em: <https://www.scientificamerican.com/article/moore-s-law-keeps-going-defying-expectations/>. Acesso em: 26 fev. 2018.

SOLOVE, Daniel J. A Taxonomy of Privacy. **University of Pennsylvania Law Review**, v. 154, n. 3, p. 477-560, jan. 2006. Disponível em: <https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf>. Acesso em: 13 dez. 2018.

SOLUM, Lawrence; CHUNG, Minn. The Layers Principle: Internet Architecture and the Law. **University of San Diego School of Law Research Paper**, n. 55, p. 1-114, jun. 2003. Disponível em: < https://dx.doi.org/10.2139/ssrn.416263>. Acesso em: 05 maio. 2019.

SPRENGER, Polly. Sun on Privacy: 'Get Over it". **Wired**, 26 jan. 1999. Não paginado. Disponível em: <https://www.wired.com/1999/01/sun-on-privacy-get-over-it/>. Acesso em: 18 out. 2018.

STIGLER, George J. The Size of Legislatures. **The Journal of Legal Studies**, v. 5, n. 1, p. 17-34, jan. 1976. Disponível em: <https://www.jstor.org/stable/724072>. Acesso em: 05 set. 2018.

STIGLER, George J. The Economic Theory of Regulation. **The Bell Journal of Economics and Management Science,** v. 2, n. 1, p. 3-21, 1971. Disponível em: <http://www.jstor.org/stable/3003160>. Acesso em: 11 jun. 2018.

STIGLER, George J. The Economics of Information. **The Journal of Political Economy**, v. 69, n. 3, p. 213-225, jun. 1961. Disponível em: < https://www.jstor.org/stable/1829263>. Acesso em: 13 fev. 2019.

STIGLITZ, Joseph E. Government Failure vs. Market Failure: Principles of Regulation. In.: BALLEISEN, Edward J.; MOSS, David A. (eds.). **Governments and Markets:** Toward a New Theory of Regulation. Cambridge: Cambridge University Press, 2010. Disponível em: <https://doi.org/10.1017/CBO9780511657504.002>. Acesso em: 14 maio. 2019.

STRAHILEVITZ, Lior. Wealth without Markets? Reviewing Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom. **Yale Law Review**, v. 116, n. 7, p. 1472-1515, 2007. Disponível em: <https://digitalcommons.law.yale.edu/ylj/vol116/iss7/2/>. Acesso em: 20 mar. 2019.

SUNSTEIN, Cass. The First Amendment in Cyberspace. **Yale Law Journal**, v. 104, p. 1757-1804, 1994. Disponível em: <https://chicagounbound.uchicago.edu/journal_articles/8585/>. Acesso em: 28 jun. 2018.

SUNSTEIN, Cass. The Welfare Effects of Information. **Harvard Public Law Working Paper**, n. 18, dec. 2018. Disponível em: < https://dx.doi.org/10.2139/ssrn.3193996>. Acesso em: 02 maio. 2019.

TAVARES, André Ramos. O Dever de Transparência. *In*.: CANOTILHO, José Joaquim Gomes et al (Coods.). **Comentários à Constituição do Brasil.** São Paulo: Saraiva, 2013.

THE HERITAGE FOUNDATION. **2019 Index of Economic Freedom.** Washington D.C.: The Heritage Foundation, 2019. Disponível em: <https://www.heritage.org/index/pdf/2019/book/chapter6.pdf>. Acesso em: 05 mar. 2019.

THIERER, Adam. Code, Pessimism, and the Illusion of "Perfect Control". **Cato Unboud**, 8 may. 2009. Não paginado. Disponível em: <https://www.cato-unbound.org/2009/05/08/adam-thierer/code-pessimism-illusion-perfect-control>. Acesso em: 29 ago. 2018.

TRIBE, Laurence H. **The Constitution in Cyberspace:** Law and Liberty Beyond the Electronic Frontier. Cambrigde: Harvard University Press, 1991. Não paginado. Disponível em: <https://epic.org/free_speech/tribe.html>. Acesso em: 28 jun. 2018.

TSORMPATZOUDI, Pagona; BERENDT, Bettina; COUDERT, Fanny. Privacy by Design: Research and Policy to Practice – the Challenge of Multi-disciplinarity. In.: BERENDT, Bettina *et alli* (Eds.). **Privacy Technologies and Policy.** Luxembourg: Springer, 2015. Disponível em: <https://link.springer.com/content/pdf/10.1007%2F978-3-319-31456-3.pdf>. Acesso em: 17 out. 2018.

TURILLI, Matteo; FLORIDI, Luciano. The Ethics of Information Transparency. **Ethics and Information Technology,** v. 11, n. 2, p. 105-112, jun. 2009. Disponível em: <https://link.springer.com/article/10.1007/s10676-009-9187-9>. Acesso em: 05 mar. 2019.

TUTT, Andrew. An FDA for Algorithms. **Administrative Law Review**, v. 69, p. 83-123, 2017. Disponível em: <https://ssrn.com/abstract=2747994>. Acesso em: 05 maio. 2019.

UNITED KINGDOM. Department for Digital, Culture, Media & Sport. **Data Ethics Workbook.** London: Government Digital Service, 2018. Não Paginado. Disponível em: <https://www.gov.uk/government/publications/data-ethics-workbook/data-ethics-workbook>. Acesso em: 06 maio. 2019.

UNITED NATIONS. General Assembly. **Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.** Washington: United Nations, 2018. Disponível em: <https://freedex.org/wp-content/blogs.dir/2015/files/2018/10/AI-and-FOE-GA.pdf>. Acesso em: 15 maio. 2019.

UNITED NATIONS. Human Rights Council. **Report of the United Nations High Commissioner for Human Rights:** The Right to Privacy in the Digital Age. New York: United Nations, 2018. Disponível em: <https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf>. Acesso em: 01 out. 2018.

UNITED NATIONS. **Total Prison Population.** New York: United Nations Office on Drugs and Crime, 2015. Não paginado. Disponível em: < https://dataunodc.un.org/crime/total-prison-population>. Acesso em: 11 fev. 2019.

UNITED NATIONS. **Technology and Innovation Report 2018:** Harnessing Frontier Technologies for Sustainable Development. Switzerland: United Nations, 2018. Disponível em: <https://unctad.org/en/PublicationsLibrary/tir2018_en.pdf>. Acesso em: 10 maio. 2019.

UNITED NATIONS. **United Nations Activities on Artificial Intelligence.** New York: United Nations, 2018. Disponível em: < https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2018-1-PDF-E.pdf>. Acesso em: 15 maio. 2019.

UNITED NATIONS. **Viena Convention on the Law of Treaties.** Viena: United Nations, 1965. Disponível em: <http://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf>. Acesso em: 04 fev. 2019.

UNITED NATIONS EDUCATION, SCIENTIFIC AND CULTURAL ORGANIZATION. Digital Literacy in Education. **Policy Brief**, may. 2011. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000214485>. Acesso em: 22 mar. 2019.

UNITED STATES OF AMERICA. Department of Health, Education and Welfare. **Records, Computers, and the Rights of Citizens.** Washington: DHEW, 1973. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 26 nov. 2018.

UNITED STATES.SUPREME COURT. **Loomis v. Wisconsin.** Washington: United States Supreme Court, 2017. Não paginado. Disponível em: <https://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/>. Acesso em: 11 fev. 2019.

UNITED STATES OF AMERICA. SUPREME COURT. **Olmstead v. United States.** 227 U.S. 438 (1928). Disponível em: <https://supreme.justia.com/cases/federal/us/277/438/>. Acesso em: 26 jun. 2018.

UNITED STATES OF AMERICA.SUPREME COURT. **Reno v. American Civil Liberties Union.** 521 U.S. 844 (1997). Disponível em: <https://supreme.justia.com/cases/federal/us/521/844/>. Acesso em: 01 mar. 2018.

UNITED STATES OF AMERICA.SUPREME COURT. **Roe v. Wade.** 410 U.S. 113 (1973). Disponível em: <https://supreme.justia.com/cases/federal/us/410/113/>. Acesso em: 13 dez. 2018.

UNITED STATES OF AMERICA. **Amendments to the Constitution of the United States of America**. Washington: Government Publishing Office, 1992. Disponível em: <https://www.gpo.gov/fdsys/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-7.pdf>. Acesso em: 01 jul. 2018.

UNITED STATES OF AMERICA. **Memorandum for the Heads of Executive Departments and Agencies:** Electronic Commerce. Washington: Office of the Press Secretary, 1997. Não paginado. Disponível em: <https://fas.org/irp/offdocs/pdd-nec-ec.htm>. Acesso em: 23 mar. 2018.

UNITED STATES OF AMERICA. **Memorandum for the Heads of Executive Departments and Agencies:** Successes and Further Work on Electronic Commerce. Washington: Office of the Press Secretary, 1998. Não paginado. Disponível em: <https://fas.org/irp/offdocs/pdd-nec-ec98.htm>. Acesso em: 23 mar. 2018.

UNITED STATES OF AMERICA. **Public Law 85-325.** Washington: Office of the Law Revision Counsel, 1958. Disponível em: <http://uscode.house.gov/statutes/pl/85/325.pdf>. Acesso em: 27 fev. 2018.

UNITED STATES OF AMERICA. **Public Law 104-104.** Washington: Government Publishing Office, 1996. Disponível em: <https://www.gpo.gov/fdsys/pkg/STATUTE-110/pdf/STATUTE-110-Pg56.pdf>. Acesso em: 01 mar. 2018.

VALAUSKAS, Edward J. Lex Networkia: Understanding the Internet Community. **First Monday**, v. 1, n. 4, não paginado, oct. 1996. Disponível em: <http://firstmonday.org/ojs/index.php/fm/article/view/490/411>. Acesso em: 06 mar. 2018.

VALENTINO-DEVRIES, Jennifer; SINGER-VINE, Jeremy; SALTANi, Ashkan. Websites Vary Prices, Deals Based On Users' Information. **The Wall Street Journal,** 24 Dec. 2012. Não Paginado. Disponível em: <https://www.wsj.com/articles/SB10001424127887323777204578189391813881534>. Acesso em: 08 jan. 2018.

VALLADÃO, Haroldo. O Estudo e o Ensino do Direito Comparado no Brasil: séculos XIX e XX. **Revista de Informação Legislativa,** v. 8, n. 30, p. 3-14, abr./jun. 1971. Disponível em: <http://www2.senado.leg.br/bdsf/handle/id/180807>. Acesso em: 17 jul. 2018.

VAN BLARKORM, G.W.; BORKING, J.J.; VERHAAR, P. Privacy Enhancing Technologies. In.: HUIZENGA, J. (coord.). **Handbook of Privacy and Privacy-Enhancing Technologies:** the case of Intelligent Software Agents. The Hague: PISA Consortium, 2003. Disponível em: <https://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf>. Acesso em: 03 out. 2018.

VICENT, James. Tencent says there are only 300,000 AI engineers worldwide, but millions are needed. **The Verge,** 5 dec. 2017. Não paginado. Disponível em: <https://www.theverge.com/2017/12/5/16737224/global-ai-talent-shortfall-tencent-report>. Acesso em: 22 mar. 2019.

VILLASENOR, John. Techtank: No the Laws of Australia don't override the Laws of Mathematics. **Brookings.** 17 jul. 2017. Não paginado. Disponível em: < https://www.brookings.edu/blog/techtank/2017/07/17/no-the-laws-of-australia-dont-override-the-laws-of-mathematics/>. Acesso em: 10 maio. 2019.

WALDMAN, Ari Erza. Designing Without Privacy. **Houston Law Review,** v. 55, p. 659-727, 2018. Disponível em: <https://ssrn.com/abstract=2944185>. Acesso em: 01 out. 2018.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy.** Harvard Law Review, v. 4, n. 5, p. 193-220, dec. 1890. Disponível em: <https://www.jstor.org/stable/1321160>. Acesso em: 01 out. 2018.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, 2017. Disponível em: <https://dx.doi.org/10.2139/ssrn.2903469>. Acesso em: 05 mar. 2019.

WEBER, Rolf H. Data Ownership in Platform Markets. In.: BELLI, Luca; ZINGALES, Nicolo (ed.). **Platform Regulations:** How Platforms are Regulated and How they Regulate Us. Rio de Janeiro: Fundação Getúlio Vargas, 2017. Disponível em: <http://hdl.handle.net/10438/19402>. Acesso em: 04 out. 2018.

WEINBERGER, David. Optimization over Explanation. **Berkman Klein Center Collection**, 28 jan. 2018. Não paginado. Disponível em: < https://medium.com/berkman-klein-center/optimization-over-explanation-41ecb135763d>. Acesso em: 15 maio. 2019.

WIENER, Norbert. **Cybernetics:** or control and communication in the animal and the machine. 2 ed. Cambridge: The MIT Press, 1965. Disponível em: <https://uberty.org/wp-content/uploads/2015/07/Norbert_Wiener_Cybernetics.pdf>. Acesso em: 05 mar. 2019.

WIHBEY, John. Journalists Know They Need to Get Better with Data and Statistics, but They Have a Long Way to Go. **NiemanLab**. 3 may. 2019. Não Paginado. Disponível em: <https://www.niemanlab.org/2019/05/journalists-know-they-need-to-get-better-with-data-and-statistics-but-they-have-a-long-way-to-go/>. Acesso em: 03 maio. 2019.

WORLD WIDE WEB CONSORTIUM. **Protocol for Privacy Preferences:** an introduction. [s.l.]: W3C, 2000. Não paginado. Disponível em: <https://www.w3.org/P3P/introduction.html>. Acesso em: 04 fev. 2019.

WRIGHT, David et al. Integrating Privacy Impact Assessment in Risk Management. **International Data Privacy Law**, v. 4, n. 2, p. 155-170, 2014. Disponível em: <https://doi.org/10.1093/idpl/ipu001>. Acesso em: 22 jan. 2019.

WRIGHT, David. Making Privacy Impact Assessment More Effective. **The Information Society International Journal**, v. 29, n. 5, p. 307-315, 2013. Disponível em: < https://www.tandfonline.com/doi/abs/10.1080/01972243.2013.825687>. Acesso em: 21 jan. 2019.

WRIGHT, David. The State of the Art in Privacy Impact Assessment. **Computer Law & Security Review**, v. 28, n. 1, p. 54-61, fev. 2012. Disponível em: <https://doi.org/10.1016/j.clsr.2011.11.007>. Acesso em: 18 jan. 2018.

WU, Timothy. When Code Isn't Law. **Virginia Law Review**, v. 89, n. 4, p. 103-170, 2003. Disponível em: <https://ssrn.com/abstract=414180>. Acesso em: 04 set. 2018.

YOO, Christopher S. Protocol Layering and Internet Policy. **University of Pennsylvania Law Review,** v. 161, n. 6, p. 1707-1771, 2013. Disponível em: <https://scholarship.law.upenn.edu/penn_law_review/vol161/iss6/7/>. Acesso em: 06 maio. 2019.

ZAKRZEWSKI, Cat; HAWKINS, Derek. Tech Executives Voice Support for National Privacy Law. **The Washington Post**, 26 set. 2018. Não paginado. Disponível em: <https://www.washingtonpost.com/politics/2018/09/26/tech-executives-voice-support-national-privacy-law/?noredirect=on&utm_term=.23a734823ccb>. Acesso em: 19 nov. 2018.

ZAMBONELLI, Franco *et allia.* Algorithmic Governance in Smart Cities: the conundrum and the potential of pervasive computing solutions. **IEEE Technology and Society Magazine.** v.

37, n. 2, p. 80-87, jun. 2018. Disponível em: < https://doi.org/10.1109/MTS.2018.2826080>. Acesso em: 14 maio. 2019.

ZARSKY, Tal Z. Incompatible: The GDPR and the Age of Big Data. **Seton Hall Law Review**, v. 47, n. 4, p. 995-1020, 2017. Disponível em: < https://scholarship.shu.edu/shlr/vol47/iss4/2/>. Acesso em: 15 maio. 2019.

ZERILLI, John *et alli.* Transparency in Algorithmic and Human Decision-Making: Is There a Double Standard? **Philosophy & Technology**, p. 1-23, set. 2018. Disponível em: <https://link.springer.com/article/10.1007/s13347-018-0330-6>. Acesso em: 2 maio. 2019.

ZITTRAIN, Jonathan. A History of Online Gatekeeping. **Harvard Technology Law Review,** v. 19, n. 2, p. 253-298, 2006. Disponível em: <https://dash.harvard.edu/handle/1/4455491>. Acesso em: 17 jun. 2018.

Pontifícia Universidade Católica do Rio Grande do Sul
Pró-Reitoria de Graduação
Av. Ipiranga, 6681 - Prédio 1 - 3º. andar
Porto Alegre - RS - Brasil
Fone: (51) 3320-3500 - Fax: (51) 3339-1564
E-mail: prograd@pucrs.br
Site: www.pucrs.br