

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

Larissa Wermann

GOVERNANÇA ALGORÍTMICA E A PROTEÇÃO DE DADOS PESSOAIS

Porto Alegre
2018

Larissa Wermann

GOVERNANÇA ALGORÍTMICA E A PROTEÇÃO DE DADOS PESSOAIS

Trabalho de conclusão de curso de graduação apresentado à Faculdade de Direito da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Dr. Fabiano Menke.

Porto Alegre
2018

Larissa Wermann

GOVERNANÇA ALGORÍTMICA E A PROTEÇÃO DE DADOS PESSOAIS

Trabalho de conclusão de curso de graduação apresentado à Faculdade de Direito da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais.

Aprovada em ____ de janeiro de 2018.

BANCA EXAMINADORA:

Prof. Dr. Fabiano Menke

Prof. Ms. Guilherme Damásio Goulart

Prof.^a Dra. Kelly Bruch

Porto Alegre
2018

À Vó Nina, mulher mais forte que eu já conheci.

AGRADECIMENTOS

Àquela que é fonte de amor, força e segurança: minha mãe, Elis.

Àquele que é fonte de amor, humildade e inspiração: meu pai, Valdir.

Àquele que é fonte de amor, sensibilidade e parceria: meu irmão, Valdir Jr.

Àquela que é e sempre foi minha segunda mãe: minha dinda, Vera.

Àquela que é apoio incondicional há anos: minha amiga, Valesca.

Àquelas que me fazem lembrar que a vida é curta e, por isso, precisamos aproveitar cada momento: minhas amigas Mirela, Natália, Renata e Verônica.

Àquele que tornou possível a conclusão da graduação: meu amigo, Márcio.

Àquele que me ensinou a amar o Direito desde muito cedo: meu amigo, André.

Àquela que é a melhor advogada que eu conheço: minha amiga, Marta.

Àquela que me permite juntar e exercer todos os dias minhas quatro paixões - Direito, tecnologia, inovação e pessoas: minha empresa, ThoughtWorks.

Vocês são muito do que eu preciso saber sobre o amor, sobre a humildade, sobre a persistência e sobre querer ser um ser humano melhor diariamente. Vocês são muito do que eu preciso pra seguir caminhando.

Quanto à "morte do anonimato" por cortesia da internet, ... submetemos à matança nossos direitos de privacidade por vontade própria. Ou talvez apenas consintamos em perder a privacidade como preço razoável pelas maravilhas oferecidas em troca. Ou talvez, ainda, a pressão no sentido de levar nossa autonomia pessoal para o matadouro seja tão poderosa, tão próxima à condição de um rebanho de ovelhas, que só uns poucos excepcionalmente rebeldes, corajosos, combativos e resolutos estejam preparados para a tentativa séria de resistir. (BAUMAN, 2014, p. 35-36)

RESUMO

Esta monografia tem por objetivo apresentar a governança de algoritmos e a legislação de proteção de dados pessoais como forma de tutela da privacidade na sociedade virtual. Para tanto, serão abordados conceitos como privacidade, dados pessoais e algoritmos, com foco na proteção de dados pessoais. Além disso, tratar-se-á dos desafios da utilização de algoritmos, considerando aspectos técnicos, impactos nos indivíduos e na coletividade e consequências jurídicas. Após delinear a matéria em âmbito internacional e nacional, buscar-se-á priorizar pontos que devem ser levados em consideração quando da elaboração de legislação brasileira de proteção de dados pessoais, como forma de efetivar a tutela a direitos fundamentais e contornar ou prevenir problemas causados por algoritmos, por meio de sua governança, sem abrir mão da utilização dos mesmos.

Palavras-chave: Direito à privacidade. Proteção de dados pessoais. Governança Algorítmica. Legislação de proteção de dados.

ABSTRACT

This paper aims to present algorithmic governance and the legislation of protection data as a form of protection of privacy in the virtual society. To this end, it will be discussed the concepts of privacy, personal data and algorithms with focus on protection of personal data. In addition, it will be discussed the challenges of using algorithms, considering technical aspects, impacts on individuals and colectivity and legal consequences. After exploring the issue international and national experience level, will seek to prioritize points which should be taken in consideration when drafting Brazilian legislation for protection of personal data, in order to ensure the protection of fundamental rights and to circumvent or prevent problems caused by algorithms, through its governance, without giving up the use of them.

Keywords: Right to privacy. Protection of personal data. Algorithm governance. Data protection legislation.

SUMÁRIO

2	INTRODUÇÃO	10
3	DIREITO, TECNOLOGIA E SOCIEDADE	13
3.1	A TERCEIRA REVOLUÇÃO INDUSTRIAL	16
3.2	A QUARTA REVOLUÇÃO INDUSTRIAL	17
4	DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS	23
4.1	O CONTEXTO DA PRIVACIDADE	23
4.2	OS DADOS PESSOAIS	30
4.2.1	Banco de Dados e <i>Big Data</i>	34
4.2.2	A democratização da tecnologia e a proteção de dados pessoais	36
5	GOVERNANÇA ALGORÍTMICA	41
5.1	OS ALGORITMOS	41
5.1.1	Desafios relacionados ao uso de algoritmos, responsabilização e proteção de dados pessoais	45
5.1.1.1	Necessidade de ligação à uma base de dados.....	46
5.1.1.2	Opacidade	48
5.1.1.3	A (falta de) neutralidade.....	50
5.2	A NECESSIDADE DA GOVERNANÇA DOS ALGORITMOS	52
6	DA NECESSIDADE DE LEGISLAÇÃO ESPECÍFICA DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL	57
6.1	DOS DISPOSITIVOS JÁ EXISTENTES	58
6.2	DOS PROJETOS DE LEI EM TRAMITAÇÃO	59
6.3	BREVE CONTEXTO INTERNACIONAL	62
6.4	CONSIDERAÇÕES ACERCA DA LEGISLAÇÃO DE PROTEÇÃO DE DADOS PESSOAIS VIÁVEL PARA O BRASIL	64
6.4.1	Abrangência integral de setores	65
6.4.2	Conceito de dado pessoal	65
6.4.3	Relação com outros sistemas de proteção	66
6.4.4	Mecanismo de proteção voltado exclusivamente à pessoa natural	66
6.4.5	Consentimento	67
6.4.6	Legítimo interesse	67
6.4.7	Autoridade de fiscalização do cumprimento da legislação	68
7	CONCLUSÃO	69
	REFERÊNCIAS BIBLIOGRÁFICAS	71

2 INTRODUÇÃO

O Direito, enquanto maneira de tutelar a vida em sociedade, se modifica à medida em que a própria sociedade se altera, sobretudo quando novos processos econômicos e sociais são inseridos. A tecnologia, como fenômeno ainda recente, em especial na sua evolução no período correspondente à Terceira e Quarta Revolução Industrial, tem produzido inúmeras alterações na vida em sociedade, sobretudo no que tange aos processos econômicos e sociais, em uma velocidade e eficiência jamais vista, o que, por si só, já demonstra a necessidade de um olhar atento do Direito.

Nesse contexto, o direito à privacidade, entendido no passado como um direito negativo, correspondente ao direito de estar só, adquire atualmente uma amplitude muito maior, com a sua nova conotação no sentido de os indivíduos terem controle sobre suas próprias informações e sendo, portanto, ferramenta básica para a efetividade do Estado Democrático, sem o controle característico de regimes totalitários.

Na Sociedade da Informação em que se vive hoje, a qual tem como centro a informação, o direito fundamental à privacidade torna-se abrigo direto de dados pessoais, enquanto importante não apenas do ponto de vista individual, mas também mediante interesse ligado à coletividade. Portanto, a proteção de dados pessoais é, em suma, um desdobramento do direito à privacidade.

Para o presente trabalho, destaca-se a ampla utilização da internet, o baixo custo de captação, armazenamento e manipulação de dados pessoais, com eficiência e velocidade muito além da capacidade humana. Ainda que tais dados pessoais pareçam sem valor se analisados individualmente, sua análise coletiva serve inclusive como fonte eficiente de mudança de comportamento dos seres humanos. Entretanto, todo esse processo apenas é possível, tanto no que tange à eficiência quanto no que tange à velocidade, pelo uso de um único meio: os algoritmos.

A ampla utilização de algoritmos e a necessidade de sua tutela pelo direito adquire um caráter ainda mais importante à medida que ocorre a democratização da

tecnologia, na qual um percentual considerável da sociedade acaba por ter fácil acesso a inúmeros dispositivos conectados à internet, os quais, por sua vez, podem coletar uma infinidade de dados de uma maneira instantânea. Nesse sentido, são criados bancos de dados para serem utilizados pelos algoritmos, criando tendências e influenciando nos processos decisórios, a ponto de tirar os seres humanos do centro do mesmo.

O uso de algoritmos apresenta, afora uma infinidade de benefícios em sua aplicação, tanto para o mercado, quanto para o governo e a sociedade em geral, desafios quanto à sua utilização, dos quais destacam-se: a necessidade de ligação à uma base de dados, a opacidade e a falta de neutralidade.

Após tratar tanto da proteção de dados pessoais como um desdobramento direito do direito fundamental à privacidade quanto dos desafios envolvendo a utilização de algoritmos, o presente trabalho passa a analisar alternativas que atuem como um equilíbrio de interesses, voltado à proteção de dados pessoais.

A governança algorítmica surge como primordial nos procedimentos de coleta, armazenamento e tratamento de dados pessoais, à medida em que pode servir como norte na busca pelo equilíbrio de fatores envolvidos no que se refere à utilização de dados pessoais, a partir da criação de algoritmos, em um caráter interdisciplinar.

Passa-se, então, à análise da necessidade de uma legislação específica de proteção de dados pessoais, sobretudo no contexto brasileiro, a partir de uma análise geral do contexto internacional sobre o tema, na qual conclui-se que a criação de uma legislação específica é primordial para a proteção de dados pessoais a partir da utilização de algoritmos.

Em que pese existam hoje alguns dispositivos legais em que depreende-se a proteção de dados pessoais na legislação brasileira, além da existência de projetos de lei sobre o tema ainda em tramitação, o país ainda não confere a tutela necessária à proteção de dados pessoais que evite ofensas à dignidade da pessoa humana. Outrossim, o Brasil é um dos únicos países no mundo que não possui legislação específica sobre dados pessoais, objetivando a sua proteção.

O que se busca por meio do presente trabalho, portanto, é de que forma e com que conteúdo a criação de uma legislação de proteção de dados pessoais pode contornar ou prevenir problemas causados por algoritmos, sem barrar os benefícios produzidos pelos mesmos e proporcionando, ainda, direcionamento à governança algorítmica como meio efetivo de proteção.

3 DIREITO, TECNOLOGIA E SOCIEDADE

O direito, de uma maneira geral, sofre transformações de acordo com as transformações ocorridas na própria sociedade à qual está inserido em uma determinada época, atuando como uma espécie de resposta ou acompanhamento da sua evolução e de seus novos fenômenos. Além disso, segundo Bevilacqua¹, “o direito é uma regra social obrigatória, quer sob a forma de lei, quer sob a forma de costume”.

Entretanto, ainda que o direito seja uma regra social obrigatória, conforme já citado acima, é impossível que o direito tenha a previsão exata de tudo o que possa acontecer numa determinada sociedade em uma determinada época, para que consiga de antemão tutelar por meio da legislação tais eventos específicos. Isso ocorre, inclusive, porque a própria evolução da sociedade é inexata e de difícil – ou, mais do que isso, impossível – previsão integral. Saliente-se que as próprias definições dentro do direito devem ir se atualizando ao longo do tempo, para que faça sentido no contexto em que o mesmo esteja inserido.

Nesse sentido, nos casos em que temos novos fenômenos ainda não regulados por legislação específica até a sua efetiva ocorrência, tem-se basicamente dois pontos centrais: (i) o primeiro deles diz respeito à máxima de que o direito sempre deve ter a solução das controvérsias trazidas para sua apreciação pelo judiciário. Para tanto, existem meios específicos em cada legislação para o suprimento das eventuais lacunas existentes, como, no exemplo do Brasil, a utilização de analogia; (ii) o segundo ponto diz respeito à necessidade de criação de legislação específica baseada em novos fenômenos existentes que ainda não possuem regulação. É certo dizer, ainda, que mesmo que o primeiro ponto sempre deverá ser respeitado, nem sempre o segundo irá ocorrer.

Com base em novos fenômenos da sociedade que acabam por levar à necessidade de criação de legislação específica, tem-se como exemplo o que ficou

¹ BEVILAQUA, C. **Theoria geral do direito civil**. 4. ed. atualizada por Achilles Bevilacqua. Rio de Janeiro: Francisco Alves, 1949. p. 12.

conhecido, no Brasil, como *Lei Carolina Dieckmann*². A lei, que tipifica o crime de delitos informáticos ficou conhecida por esse codinome antes mesmo de ser publicada e sancionada, em razão da repercussão do caso em que Carolina Dieckmann, atriz conhecida no país, teve seu computador invadido e os documentos contidos nele subtraídos, o que culminou com a publicação na rede mundial de computadores de suas fotos íntimas. Tal crime ainda não era tipificado no Código Penal Brasileiro e, dado o risco de exposição geral e as recentes transformações tecnológicas, fez-se necessária a criação de uma lei que dispusesse sobre delitos informáticos.

Há de se reconhecer que uma das maiores – senão a maior – transformação na sociedade se deu – e ainda se dá – com o desenvolvimento da tecnologia. Doneda³ sabiamente estabeleceu essa relação considerando dois elementos capitais.

Estas leituras nos servem a introduzir, respectivamente, dois elementos capitais para nosso estudo, quais sejam: a consciência de que nossa tarefa falhará caso não leve em consideração o direito como um fenômeno que somente atinge sua plena realização após ser aplicado à realidade da arquitetura social; bem como o fato que tal 'realidade' é hoje em boa parte condicionada pelo desenvolvimento tecnológico.

No que tange ao desenvolvimento tecnológico, é possível afirmar que tem-se como marco histórico a Segunda Revolução Industrial, uma vez que tal Revolução consolidou-se tendo como centro a própria tecnologia. Ademais, é a partir desse momento que preocupações acerca do uso da tecnologia como instrumento de controle da sociedade começaram a chamar a atenção das ciências sociais, ficando ainda mais evidente a interdisciplinaridade necessária entre direito e tecnologia para possibilitar a criação de regras, dada a nova forma de viver em sociedade.

Fato é que o desenvolvimento tecnológico passou a ser o centro das novas transformações sociais, uma vez que presente em todas as esferas da vida. Para

² BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 21 nov. 2017.

³ DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 20.

além disso, a tecnologia apresenta uma série de desafios que perduram até os dias de hoje, que Doneda⁴ explica:

[...] a dificuldade em julgar os efeitos da utilização de novas tecnologias – o que já nos dá uma primeira mostra das dificuldades da aplicação do discurso jurídico neste campo. A tecnologia apresenta um caráter de imprevisibilidade que lhe é intrínseco; sua ação costuma-se dar em um universo amplo e complexo a ponto de tornar análises de impacto, projeções e testes, em última análise, de escassa serventia. Suas possibilidades, por sua vez, vão além daquilo que o homem jamais teve possibilidade de administrar anteriormente. Ao mesmo tempo, ela é um produto do homem e de sua cultura, destinada a relacionar-se com ele.

Outro aspecto importante na análise dos impactos da tecnologia na sociedade e, conseqüentemente, no direito, é que suas mudanças ocorrem em uma velocidade jamais vista antes. Em adição, tem-se uma capacidade qualitativa de processamento de informações de importante relevância, o que a faz ter não só um desempenho quantitativo de difícil acompanhamento pelo ser humano, mas também qualitativo – a qualidade de seus resultados poderia ser inclusive inimaginável até não muito tempo atrás e, mesmo hoje, são de difícil previsão até onde chegarão como resultado da sua evolução.

Em um sentido mais técnico-jurídico, “se desejarmos que a nova fronteira digital se torne realmente civilizada, precisamos compreender como o sistema jurídico deve ser aplicado a esse novo domínio da interação humana”⁵.

O desenvolvimento tecnológico, desde aquilo que tem-se como seu marco histórico inicial, qual seja, a Segunda Revolução Industrial, adquiriu escala, velocidade e qualidade, ao passo que hoje pode-se afirmar que vivemos no que chamamos de *Sociedade da Informação*. A Sociedade da Informação, termo utilizado amplamente por sociólogos e economistas, nada mais é do que uma sociedade que tem como ponto central a informação. Nesse sentido, não há como dissociar tal modelo de sociedade do desenvolvimento da tecnologia, dado que apenas a tecnologia permitiu que o custo e capacidade de armazenamento e manipulação dessas informações viabilizassem diretamente a existência desse modelo de sociedade.

⁴ DONEDA, 2006, p. 23.

⁵ LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. p.29.

Especificamente no sentido da imprevisibilidade dos resultados do avanço tecnológico, tem-se a presença da Metáfora de Golem Tecnológico⁶, segundo Doneda⁷:

O Golem, criatura da mitologia hebraica, é um humanoide de argila, feito pelo homem; ele é poderoso e sua força cresce a cada dia. Ele segue as ordens do seu criador, auxilia-o, mas é um pouco tolo e inconsciente de sua força: é capaz, se não for bem comandado, de destruir seu próprio senhor. A ideia de um 'Golem Tecnológico' [...] pode induzir à constatação de que se ele não é, em última análise, responsável pelos seus atos, é, porém, uma criação do gênio humano, por cujos defeitos somos responsáveis – do que surge nossa obrigação de conhecê-lo a fundo.

Tanto é verdade – e atual – a ideia da existência do *Golem Tecnológico* que dado o volume das tecnologias hoje existentes, essas podem facilmente ultrapassar a capacidade de assimilação do ser humano, ainda que tenham sido criadas e evoluídas por ele.

Ademais, nesse contexto e tendo a própria tecnologia como vetor condicionante da sociedade atual, como já indicado no presente trabalho, o desafio para o Direito ganha ainda maiores proporções. A título de exemplificação, a partir do momento que se tornam imprevisíveis os resultados produzidos pelo desenvolvimento tecnológico, tem-se discussões acerca de quem seria a responsabilidade jurídica perante eventual dano causado – seria do desenvolvedor que escreveu tal código? Ou então seria da empresa que colocou tal tecnologia no mercado? Ou, ainda, de ambos? Os questionamentos são muitos e a discussão sobre eles é necessária, levando em consideração, principalmente, a velocidade com que tudo vem ocorrendo e transformando-se.

3.1 A TERCEIRA REVOLUÇÃO INDUSTRIAL

A Segunda Revolução Industrial é considerada o marco histórico de início do desenvolvimento tecnológico, ou seja, deu início a um processo todo voltado para a área tecnológica. Mais tarde, próximo à década de 60, iniciou o que muitos

⁶ WIENER, N. **God, Golem, Inc.:** A comment on Certain Points Where Cybernetics Impinges on Religion. Cambridge: MIT The Press, 1966.

⁷ DONEDA, 2006, p. 24.

estudiosos têm chamado de Terceira Revolução Industrial, também conhecida como Revolução Informacional.

É notória, nessa Revolução, a presença específica de avanços tecnológicos como, por exemplo, o surgimento da internet mais próximo à maneira com que conhecemos hoje e o desenvolvimento de softwares com aplicação aos mais variados ramos da indústria e comércio, impactando ainda mais diretamente na economia.

A Terceira Revolução Industrial possui uma diferença primordial das demais revoluções industriais citadas: o caráter da globalização à continentalização⁸. No primeiro aspecto, importante salientar que enquanto na Primeira e na Segunda Revolução Industrial tinha-se apenas economias nacionais, focadas em modelo de governança de Estado-Nação e por uma divisão geopolítica hierarquizada, a Terceira Revolução Industrial favorece economias em nível continental e uniões políticas, inclusive porque se assim não o for, cada Estado-Nação perderia boa parte de sua força econômica e política.

Há que se falar, ainda, que a continentalização foi mais um dos grandes impactos do desenvolvimento tecnológico: à medida que a internet proporcionou acesso continental para a conexão e troca de informações, tanto para grandes conglomerados quanto para pessoas individuais, passou a ser necessário que o próprio modelo econômico e organização geopolítica mundial tomassem outras formas que atendessem essa nova sociedade e visão de mundo.

3.2 A QUARTA REVOLUÇÃO INDUSTRIAL

Se a Segunda Revolução Industrial é considerada o marco histórico de início do desenvolvimento tecnológico e a Terceira Revolução Industrial, de uma maneira geral, o seguimento de tal desenvolvimento um pouco mais próximo ao que é possível verificar nos dias atuais, tanto no sentido de qualidade e quantidade quanto

⁸ RIFKIN, Jeremy. **A Terceira Revolução Industrial**: Como o poder lateral está transformando a energia, a economia e o mundo. São Paulo: M. Books do Brasil, 2012.

no sentido de velocidade, é bem verdade, também, que atualmente se está diante de um novo fenômeno e, correndo o risco de cometer generalizações, de um novo mundo.

Esse novo mundo está sendo chamado por muitos economistas de a *Quarta Revolução Industrial*, a qual é marcada por novas descobertas simultâneas em uma gama extensa de áreas, que vão desde o sequenciamento genético até energias renováveis à computação quântica, bem como pela convergência de tecnologias e domínios digitais, físicas e biológicas, trazendo, ainda, o potencial de mudar o mundo até então percebido e conhecido por nós⁹.

No cenário da Quarta Revolução Industrial, há que se mencionar que o boom da internet, o qual teve lugar no ao final dos anos 90, introduziu mudanças importantes nos negócios, na sociedade, na política e na economia. Tais mudanças acabaram por levar Brian Solis à criação do conceito de Darwinismo Digital¹⁰, que corresponderia à “evolução do comportamento do consumidor quando a tecnologia evolui mais rápido do que a nossa habilidade de adaptação”¹¹. Para além do caráter econômico do comportamento do consumidor, é imprescindível entender a mudança da sociedade como um todo, que acaba por refletir, por óbvio, no comportamento do consumidor, mas não a se limitar sobre ele.

Esse novo mundo exige uma maior capacidade de adaptação sem sequer podermos nos preparar para tal, uma vez que a extensão, qualidade e velocidade das mudanças não são passíveis de previsão exata e, por muitas vezes, sequer aproximada.

Ainda no ano de 1986, Drucker¹² já adiantava que estávamos,

[...] na verdade, nos estágios iniciais de uma das mais importantes transformações tecnológicas, e de longe mais avassaladora do que os mais arrebatados ‘futurólogos’ poderiam imaginar, indo além das Megatendências ou do Choque do Futuro. Trezentos anos de tecnologia chegam ao fim

⁹ PERASSO, V. O que é a 4ª revolução industrial - e como ela deve afetar nossas vidas. In: **Bbc Brasil**, 2016. Disponível em: <<http://www.bbc.com/portuguese/geral-37658309>>. Acesso em: 22 nov. 2017.

¹⁰ Tradução livre do inglês *Digital Darwinism*.

¹¹ SOLIS, B. **What's the future of Business?** Changing the way businesses create experiences. Hoboken: John Wiley & Sons, Inc., 2013. p. 16.

¹² DRUCKER, P. F. **Inovação e Espírito Empreendedor: Práticas e Princípios**. 1ª ed. São Paulo: Pioneira Thomson, 2002. p. 5.

depois da Segunda Guerra Mundial. Nesses três séculos, o modelo de tecnologia foi de natureza mecânica: saber o que acontece dentro de uma estrela como o sol. [...] Contudo, desde o fim da Segunda Guerra Mundial, o modelo de tecnologia passou a ser o processo biológico, o que acontece dentro de um organismo. E, num organismo, os processos não estão organizados a partir da energia [...] eles estão organizados a partir da informação.

Tanto é verdade que a Quarta Revolução Industrial está a caminho que estudiosos já apresentam suas megatendências, que vão desde a existência de veículos autônomos que não só carros, passando por possibilidade de mapeamento do genoma e inteligência artificial que analisa doenças baseado em dados históricos, inclusive sugerindo tratamento, e tendo, por fim, internet das coisas como ponte do mundo digital para o mundo físico e criptomoedas como moedas oficiais da economia.

Como prováveis impactos da Quarta Revolução Industrial, levando em consideração as suas megatendências e em uma análise mais alto nível, teremos pontos em todas as áreas de mundo como conhecemos hoje: na economia, nos negócios, na política e formas de governo, na sociedade como um todo e no indivíduo, os quais serão melhores detalhados abaixo.

Quando fala-se de economia, por exemplo, pode-se pensar no alto envelhecimento das pessoas, baixando, portanto, o nível de produtividade, que poderá não ser compensado com os baixos índices de natalidade já vistos, por exemplo, em países mais desenvolvidos. Outro possível impacto trata-se da substituição de homens por máquinas ou inteligência artificial – a exemplo do que já aconteceu no passado com a função de datilógrafo – e uma consequente redução da empregabilidade.

Já no âmbito dos negócios, fica clara a necessidade de uma capacidade de rápida adaptabilidade e inovação, qualquer que seja o ramo. Outro ponto importante diz respeito às expectativas dos consumidores, que mudam radicalmente e aumentam, tanto mais à medida que a continentalização oferece uma gama muito maior de acesso a diferentes opções. Já o uso de histórico de dados e informações das pessoas consumidoras torna-se um atrativo interessante do ponto de vista exclusivo de negócio, uma vez que pode fornecer ao mesmo diretrizes e rumos até então não pensados, inclusive dando, para tal, embasamento não apenas empírico e sim com dados oficiais.

No que tange à política e às formas de governo, com a velocidade com que as informações são processadas, novas maneiras de a população auditar contas públicas, por exemplo, estão surgindo. Nesse sentido, tem-se o projeto de tecnologia intitulado *Operação Serenata de Amor*, que consiste no uso de inteligência artificial para auditar contas públicas e combater a corrupção¹³. Salienta-se que tal auditoria até poderia ser feita por seres humanos, entretanto, completamente inviável dado a relação entre esforço humano necessário e resultados atingidos – ponto que a inteligência artificial, tendo como base o uso de dados que já são públicos, resolve em uma velocidade muito grande e em um tempo muito curto.

Por outro lado, as tecnologias digitais também possuem um enorme potencial de afetar positivamente a política, viabilizando e facilitando processos que auxiliem, portanto, a forma de governar. Desafiador, porém, será a criação de regulamentação que propicie a inovação, mas que garanta, ao mesmo tempo, o seguimento de princípios básicos como conhecemos.

Na questão relacionada à sociedade, um dos pontos de atenção que já existe na Terceira Revolução Industrial ficará ainda mais evidente na evolução da Quarta Revolução Industrial: o aumento da desigualdade social. O que principalmente é levado em consideração nisso é que o acesso à tecnologia acaba por se tornar ferramenta básica para que o atingimento da dignidade humana. Sobre a dignidade da pessoa humana e a sua importância intrínseca, André Carvalho Ramos¹⁴ nos ensina:

Tanto nos diplomas internacionais quanto nacionais, a dignidade humana é inscrita como princípio geral ou fundamental [...] é uma categoria jurídica que, por estar na origem de todos os direitos humanos, confere-lhes conteúdo ético [...] a dignidade humana dá unidade axiológica a um sistema jurídico, fornecendo um substrato material para que os direitos possam florescer.

Diferentemente do que ocorre com direitos como liberdade, igualdade, entre outros, a dignidade humana não trata de um aspecto particular da existência, mas sim de uma qualidade inerente a todo ser humano, sendo um valor que identifica o ser humano como tal. Logo, o conceito de dignidade é polissêmico e aberto, em permanente processo de desenvolvimento e construção.

¹³ DATA SCIENCE BRIGADE. **Operação Serenata de Amor**. [S. l.]: [2016?]. Disponível em: <<https://serenatadeamor.org/>>. Acesso em: 26 nov. 2017.

¹⁴ RAMOS, A. de C. **Curso de Direitos Humanos**. 1. ed. São Paulo: Saraiva, 2014. p. 74-75.

Tem-se, entretanto, que ainda que o que chamamos de democratização da tecnologia seja um fenômeno atual, do qual falaremos mais adiante, a tecnologia ainda não é acessível para todas camadas da população e, além disso, não se dá de maneira uniforme inclusive nas camadas afetadas. Ora, pois, se a tecnologia acaba sendo um instrumento para o atingimento da dignidade humana e, ao mesmo tempo, a tecnologia não está disponível para todos e, quando está, se dá de maneiras muito diferentes, temos, como consequência, um aumento da desigualdade social e novas formas de discriminação.

Ainda relacionado à sociedade, cita-se como impacto um novo sentido de comunidade, uma vez que as conexões cada vez dependem menos de contato físico – e, conseqüentemente, não mais necessária a proximidade física – de uma sociedade cada vez mais acostumada com a velocidade demasiada com que as coisas acontecem na rede. O sentimento de pertencimento muda drasticamente, uma vez que para *pertencer* não mais há o limite físico imposto. Essa nova sociedade, será, então, marcada por dinamicidade e fluidez, sempre controlada pela velocidade. Esse novo espectro da sociedade já foi objeto de estudo no passado e, segundo Bauman¹⁵:

‘Indivíduos frágeis’, destinados a conduzir suas vidas numa ‘realidade porosa’, sentem-se como que patinando sobre gelo fino; e ‘ao patinar sobre gelo fino’, observou Ralph Waldo Emerson em seu ensaio Prudence, ‘nossa segurança está em nossa velocidade’. Indivíduos, frágeis ou não, precisam de segurança, anseiam por segurança, buscam a segurança e assim tentam, ao máximo, fazer o que fazem com a máxima velocidade. Estando entre os corredores rápidos, diminuir a velocidade significa ser deixado para trás; ao patinar em gelo fino, diminuir a velocidade também significa a ameaça real de afogar-se. Portanto, a velocidade sobe para o topo da lista dos valores de sobrevivência.

A velocidade, no entanto não é propícia ao pensamento, pelo menos ao pensamento de longo prazo. O pensamento demanda pausa e descanso, ‘tomar seu tempo’, recapitular os passos já dados, examinar mais de perto o ponto alcançado e a sabedoria (ou imprudência, se for o caso) de o ter alcançado.

Pensar tira nossa mente da tarefa em curso, que requer sempre a corrida e a manutenção da velocidade. E na falta do pensamento, o patinar sobre o gelo fino que é uma fatalidade para todos os indivíduos frágeis na realidade porosa pode ser equivocadamente tomado como seu destino.

Por fim, no aspecto individual, os impactos exigirão uma necessidade de adaptação contínua e rápida e, nesse aspecto, é possível que exista uma nova

¹⁵ BAUMAN, Z. **Modernidade líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

desigualdade ontológica, tendo, de um lado, aqueles que aceitam as mudanças e se adequam de acordo com as mesmas; por outro lado, sempre existirão aqueles que não se adaptarão, gerando, portanto, tal desigualdade. A questão cognitiva e a atenção dos indivíduos também tendem a sofrer alterações consideráveis, uma vez que inseridos em uma realidade digital cada vez mais rápida e eficiente, onde muitas das necessidades básicas da vida serão resolvidas apenas com um clique, com boom de informações a todo momento.

Para se ter uma ideia das mudanças tecnológicas já previstas para a Quarta Revolução Industrial, o comitê responsável pelo Fórum Econômico Mundial sobre o Futuro do Software e da Sociedade rodou uma pesquisa¹⁶ com executivos e especialistas da Tecnologia da Informação e Comunicação, na qual a pergunta era quando, na percepção dos respondentes, os *tipping points*¹⁷ ocorreriam. O resultado referente ao ano de 2025 – ou seja, 10 anos após a aplicação da pesquisa, a qual foi feita em 2015, considera grande a probabilidade de que 10% das pessoas utilizem roupas conectadas à internet, por exemplo, assim como cerca da metade das pessoas acreditam que teremos, pela primeira vez, inteligência artificial em um quadro de diretores corporativos.

Ainda no sentido da Quarta Revolução Industrial, importante salientar, por fim, que os impactos citados no estudo indicado, na realidade, tratam-se de impactos de megatendências e não possuem a finalidade de exaurir todos eles, uma vez que, como se sabe, não há sequer como prever todas as invenções que estão por vir e tampouco os seus resultados de maneira exata.

¹⁶ O resultado e análise dessa pesquisa: WORLD ECONOMIC FORUM. Global Agenda Council on the Future of Software & Society. **Deep Shift Technology Tipping Points and Societal Impact**. Survey Report, Sept. 2015. Disponível em: <http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf>. Acesso em: 27 nov. 2017.

¹⁷ Expressão em inglês que significa o *ponto/tempo* em que uma série de pequenas mudanças ou incidentes tornam-se significantes o suficiente para causar uma mudança maior e mais importante.

4 DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS¹⁸

A partir do contexto já trazido no presente trabalho, no que tange a sociedade e a nova forma de economia, política e interações sociais, fica evidente que o ponto central para que toda evolução tecnológica possa produzir os resultados planejados gira em torno de um elemento: a informação. A informação passa a ser, então, um elemento cada vez mais valioso para que o acompanhamento dessas transformações seja feito, para propiciar a inovação e, principalmente, surge como elemento essencial da produção de lucro no mundo capitalista existente na Sociedade da Informação.

Quando se fala em informação, de uma maneira geral, a conexão com a sua proteção jurídica rapidamente pode ser feita associando-a à questão privacidade e a proteção de informações confidenciais. Entretanto, tais conceitos não são novidade no mundo jurídico – eles existem há muito tempo e, é claro, suas próprias definições evoluíram com o passar do tempo, conforme veremos a seguir.

4.1 O CONTEXTO DA PRIVACIDADE

A ideia de privacidade não é recente, ainda que uma preocupação especial relacionada à sua tutela seja própria do nosso tempo. Se traçarmos uma linha evolutiva do seu conceito, teremos que a privacidade com as características hoje presentes começa a surgir a partir do fim do século XIX, tendo, entretanto, se tornado muito mais específica apenas nos anos 90, com o chamado boom da internet.

Nos primórdios, ainda que já existente a ideia de privacidade, a mesma acabava por ser neutralizada pelo ordenamento jurídico da grande maioria dos países, os quais, por muitas vezes, focavam sua regulação em questões mais voltadas para o cunho patrimonial. Assim, sendo a privacidade uma questão ligada

¹⁸ DONEDA, 2006.

diretamente aos seres humanos, e em um contexto de sociedade que não pedia tal tutela específica por suas razões temporais e de desenvolvimento tecnológico ainda não presente, quase nenhum foco era dado para o seu significado.

No ano de 1948, a Declaração Universal dos Direitos Humanos previu, pela primeira vez, um dispositivo específico acerca da tutela da vida privada¹⁹. Ainda, passado um considerável período de tempo a partir dessa Declaração, a Constituição Federal do Brasil instituiu, no ano de 1988, que o direito à vida privada está na categoria de direito humano fundamental²⁰. Entretanto, ainda que ambos instrumentos de regulação tratem da expressão *vida privada*, seu conceito também é mutável.

Nesse mesmo sentido, Marcel Leonardi²¹, ao reconhecer o direito à vida privada como um direito fundamental e, conseqüentemente, o direito à privacidade, ensina que “os direitos fundamentais são, na maior parte dos casos, princípios, ou seja, mandamentos de otimização que devem ser realizados ao máximo, dentre as possibilidades fáticas e jurídicas existentes”.

Em se tratando de uma linha evolutiva desse conceito, imperioso trazer à tona a abrangência da expressão com a Teoria dos Círculos Concêntricos, também conhecida como Teoria das Esferas da Personalidade, nascida na Alemanha. Segundo tal teoria, a vida privada estaria dividida em três esferas, sendo a privacidade a sua circunferência mais externa e, portanto, mais ampla, por abranger um maior número de relações. Em uma camada intermediária, teríamos a intimidade

¹⁹ “Artigo XII. Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” (NAÇÕES UNIDAS. Centro de Informação das Nações Unidas. **Declaração Universal dos Direitos Humanos**. Rio de Janeiro: 2009. Disponível em: <<http://www.onu.org.br/img/2014/09/DUDH.pdf>>. Acesso em: 27 nov. 2017.)

²⁰ “Artigo 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos seguintes termos:

[...]

X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação.” (BRASIL.

Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>.

Acesso em: 21 nov. 2017)

²¹ LEONARDI, 2012, p.107.

e, em último lugar e, conseqüentemente, na área mais interna e protegida do círculo, a esfera do segredo.²²

Entretanto, como qualquer outra teoria, essa foi e ainda é alvo de críticas, principalmente no que tange o fato de que não poderíamos levar em conta apenas a origem dessas informações, como a teoria firma, independentemente da esfera em que estiver inserida – privacidade, intimidade e segredo – mas deveríamos considerar, ainda, a finalidade do uso dessas informações.

Nesse sentido, a relação entre privacidade e dados pessoais fica desde já evidente, tanto que a problemática da proteção de dados pessoais acaba por já ser introduzida, mas levar-se-á mais a fundo este tema em capítulo específico do presente trabalho.

Em um primeiro momento da história, o direito à privacidade foi entendido como o direito de estar só²³. Individualista e, de certa forma, egoísta, essa conotação foi aos poucos dando lugar para a ideia de privacidade como figura elementar no regime democrático, em um sentido de garantia ao indivíduo do controle de suas próprias informações, controle esse que não poderia ser do Estado, tanto mais para o regular funcionamento do regime democrático, uma vez que a privacidade toma forma, ainda, de pré-requisito para que uma série de liberdades fundamentais sejam alcançadas – do contrário, teríamos apenas um regime de supervigilância, dado que controle da informação é característico de regimes totalitários.

Muito embora esse não seja objeto de estudo do presente trabalho, insta salientar, ainda, o perigo de um controle invisível e rastreamento no caso desses regimes totalitários terem acesso a tecnologias que tornem ainda mais possível, de uma maneira rápida e eficiente, a sua supervigilância característica.

²² “Segredo, por definição, é aquela parte do conhecimento cujo compartilhamento com outros é rejeitado ou proibido e/ou controlado. O sigilo, por assim dizer, traça e demarca a fronteira da privacidade, sendo esta a área destinada a constituir o território próprio de alguém, o domínio de sua soberania indivisa.” (BAUMAN, Z. **Danos Colaterais: desigualdades sociais numa era global.** Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013. p. 113)

²³ Tradução livre de *the right to be alone*, amplamente utilizado, na época, pela doutrina e jurisprudência dos Estados Unidos. Tal expressão se propagou após a publicação de Warren e Brandeis no ano de 1890, intitulada *The right to privacy*. (WARREN, S. D.; BRANDEIS, L. D. **Das Recht auf Privatheit – The Right to Privacy.** Harvard Law Review, v. IV. n. 5. Dec. 1890)

Passando-se, então, para a Sociedade da Informação propriamente dita e da maneira hoje existente, a privacidade evoluiu como conceito em um sentido de abrigo direto de dados pessoais, os quais são considerados como projeções dos próprios indivíduos.

Fica claro, portanto, o caráter de privacidade que, apesar de inicialmente individual, acaba por se tornar de interesses ligados à coletividade. Nesse sentido, Stefano Rodotà²⁴ já observava que a estrutura do conceito de privacidade já não mais era em torno do eixo *pessoa-informação-segredo*, mas sim em torno do eixo *pessoa-informação-circulação-controle*.

Autores como Daniel Solove²⁵ já deixaram claro que os ordenamentos jurídicos não mais estão conseguindo adequar-se à nova era, afirmando, ainda, que “*the existing law protecting information privacy has not adequately responded to the emergence of digital dossiers [...] we must rethink privacy for the Information Age*”.

Como já referido, o direito à privacidade não trata de um novo direito incorporado a partir do desenvolvimento tecnológico. Entretanto, é preciso estar atento ao fato de que a sua importância subiu drasticamente à medida que a tecnologia permitiu eficiência, rapidez e infalibilidade no armazenamento e utilização de informações. O que é novidade, aqui, certamente não é a utilidade dessas informações – elas seriam úteis a qualquer tempo; entretanto, a capacidade de armazenamento, processamento e manipulação das informações com alta velocidade, eficiência e a um custo razoável tornou possível a sua utilização.

Todo esse contexto da privacidade e de suas discussões mais recentes, fruto principalmente dos impactos causados pela evolução tecnológica, acrescida das denúncias de espionagem internacional praticada pelos Estados Unidos em meios eletrônicos²⁶, levaram o Brasil e a Alemanha, em conjunto, propor à Organização

²⁴ RODOTÀ, S. **Tecnologie e Diritti**. Bologna: il Mulino, 1995. p. 102.

²⁵ SOLOVE, D. J. **The digital person: technology and privacy in the information age**. New York: New York University Press books, 2004. p. 9. Disponível em: <<http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text.htm>>. Acesso em: 1º dez. 2017.

²⁶ As denúncias foram feitas por Edward Snowden, que até então era consultor da NSA. Segundo os documentos vazados por ele, a NSA tinha acesso a diversas informações, como senhas, e-mails, fotos e dados armazenados dos usuários de nove empresas da internet. (O GLOBO, **O escândalo da espionagem dos EUA**. [S.l.]: 2013. Disponível em: <<https://oglobo.globo.com/mundo/o-escandalo-da-espionagem-dos-eua-10191175>>. Acesso em: 3 dez. 2017)

das Nações Unidas um projeto de resolução sobre o Direito à Privacidade na era digital, o qual foi aprovado pela Assembleia Geral da ONU realizada em dezembro de 2013. Do texto do projeto, destaca-se:

PP5. Reafirmando o direito humano dos indivíduos à privacidade e a não ser submetido a ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, bem como o direito à proteção da lei contra tais ingerências ou ofensas, e reconhecendo que o exercício do direito à privacidade constitui requisito essencial à realização do direito à liberdade de opinião e de expressão sem ingerências e um dos pilares de uma sociedade democrática,

[...]

PP6. Salientando a importância do pleno respeito à liberdade de buscar, receber e difundir informações, inclusive a importância fundamental do acesso à informação e da participação democrática,

[...]

PP9. Observando que, embora preocupações com a segurança pública possam justificar a coleta e a proteção de certas informações confidenciais, os Estados devem assegurar o pleno cumprimento de suas obrigações no âmbito do direito internacional dos direitos humanos,

[...]

2. Reconhece que o rápido avanço das tecnologias da informação e da comunicação, inclusive a natureza global e aberta da Internet, constitui força motriz da aceleração do progresso para o desenvolvimento em suas várias formas;

3. Afirma que os mesmos direitos que as pessoas possuem fora da rede ('offline') devem ser protegidos em rede ('online'), em particular o direito à privacidade.²⁷

Ainda relacionado à proteção da privacidade no âmbito da Organização das Nações Unidas, em março de 2015, foi aprovada resolução para que o Alto Comissariado da Organização das Nações Unidas para os Direitos Humanos faça a criação do cargo de relator especial sobre o direito à privacidade, o qual deverá ter um mandato de três anos²⁸.

Outro ponto importante a ser considerado é que o direito à privacidade surgiu como um direito tipicamente burguês, no período do apogeu do liberalismo clássico. Ainda que em muito a mutabilidade do significado de privacidade tenha evoluído, tal elitismo ainda é presente em sua discussão – não sem motivo, a sua existência

²⁷ BRASIL. Ministério das Relações Exteriores. **Brasil e Alemanha apresentam à ONU projeto de resolução sobre o direito à privacidade na era digital**. Brasília, 2013. Disponível em: <<http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/3424-brasil-e-alemanha-apresentam-a-onu-projeto-de-resolucao-sobre-o-direito-a-privacidade-na-era-digital>>. Acesso em: 6 dez. 2017.

²⁸ NAÇÕES UNIDAS NO BRASIL. **Sob liderança de Brasil e Alemanha, ONU cria mandato de relator sobre privacidade na era digital**. [S.l.]: 2015. Disponível em: <<https://nacoesunidas.org/sob-lideranca-de-brasil-e-alemanha-onu-cria-mandato-de-relator-sobre-privacidade-na-era-digital/>>. Acesso em: 6 dez. 2017.

iniciou em países desenvolvidos e ainda hoje encontra-se incipiente em muitos países subdesenvolvidos, a exemplo do Brasil.

Isso ocorre, principalmente, por tratar-se de um direito, hoje, muito ligado ao desenvolvimento tecnológico, que apesar da sua atual democratização, não está disponível para todas pessoas de maneira igual e, conseqüentemente, a sua preocupação é diferente em cada estrato social.

Ora, pois, em países menos desenvolvidos e heterogêneos, como é o caso do Brasil, torna-se realmente difícil o entendimento e aplicação do sentido de privacidade e, conseqüentemente, da proteção de dados pessoais, quando muitas vezes sequer se tem outros direitos básicos cobertos. Nesse sentido, Doneda²⁹ explica:

Certamente algumas particularidades históricas podem apontar os motivos desta determinada configuração da matéria no Brasil; como o pode, até certo ponto, o próprio perfil social do país – que, dada a existência de problemas estruturais de maior gravidade, poderia sugerir-nos que a proteção de dados pessoais seja, ao menos em termos quantitativos, uma demanda de menor apelo. Uma demanda pela proteção dos dados pessoais não é sentida de forma uniforme por uma população de perfil heterogêneo como a brasileira – pelo simples motivo de que o interesse em sua tutela desenvolve-se somente depois que uma série de outras necessidades básicas sejam satisfeitas.

Ainda que diversas dificuldades venham sendo encontradas ao longo do caminho no que tange à privacidade, ela é um tema com presença constante, principalmente quando se fala em evolução. Sua conotação contemporânea manifesta-se, sobretudo, na ideia de proteção de dados pessoais, ainda que não se limite a isso.

A proteção de dados pessoais adquire essa importância e se torna a principal derivação do direito à privacidade, pois, conforme Doneda³⁰, a informação pessoal está:

[...] quase como ato reflexo, ligada à privacidade por uma equação que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa [...] pode servir como um ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida [...] como um desdobramento da tutela do direito à privacidade.

²⁹ DONEDA, 2006, p. 17.

³⁰ DONEDA, D. O Direito Fundamental à Proteção de Dados Pessoais. In: MARTINS, G. M. (Coord.) et al. **Direito Privado & Internet**. São Paulo: Atlas, 2014. cap. 3. p. 63.

Outrossim, não mais se está falando de uma perspectiva exclusivamente individual, como o direito de estar só citado acima, mas sim de questões de caráter pessoal – direito de personalidade – voltado para a coletividade, ou seja, que se tornam foco de exploração econômica sempre que referem-se a um coletivo.

As informações pessoais, individuais e por si só, podem até não serem tão atrativas do ponto de vista mercadológico. Entretanto, a partir do momento que a tecnologia permite que essas informações individuais (e, muitas vezes, parciais) sejam transformadas em informações de massa, organizadas, passíveis de manipulação e armazenamento ao longo do tempo, transformando, portanto, essa base de dados em valor econômico e importante vetor para o setor dos negócios da sociedade da informação, o cenário muda completamente.

Fica evidente que o debate em torno da privacidade e, conseqüentemente, da proteção de dados pessoais, cresce exponencialmente quando transposto para a era da internet.

Para além dos desafios técnicos produzidos pela tecnologia, dos quais cuidam especialistas da área cujos resultados são muitas vezes impossíveis de prever, a tecnologia traz um desafio ainda maior para o direito, especialmente no tocante a sua adequação para a nova realidade virtual e digital, tendo em vista a sua eficiência, rapidez e infalibilidade, a qual se dá de maneira jamais vista antes na história.

O objetivo específico de determinadas organizações no acesso a tais bases de dados, bem como a sua utilidade para cada setor, seja privado ou público, pode não ser evidente em um primeiro momento.

Por outro lado, ainda que a seu objetivo específico e a sua utilidade não sejam evidentes, é fácil depreender que, a partir do momento que se tem como base dados pessoais, o indivíduo a quem esses dados pertençam deve ser o protagonista dessa relação, desde a decisão consciente de fornecer ou não esses dados, até a manipulação a ser feita.

Isto posto, acrescido do iminente risco de uso indevidos desses dados pessoais, que poderia culminar com a erosão da privacidade – o que, inclusive,

alguns ativistas já entendem como ser fato notório do nosso tempo – é necessário, mais do que nunca, que este tema seja trazido à tona, considerando, ainda, os limites geográficos e espaciais. Ainda que a internet tenha quebrado muitas dessas barreiras físicas através do seu caráter de imediatidade de conexão, os ordenamentos jurídicos ainda as possuem fortemente, sendo necessário que, para além da questão jurídica envolvida, que o tema seja visto de uma perspectiva política e de evolução social.

4.2 OS DADOS PESSOAIS

É inegável que a internet alterou a forma com que as informações são transmitidas e armazenadas. Para além disso, elementos estruturantes do Estado, como território e poder, modificaram-se à medida que limitações geográficas não mais existiam e a soberania acabou perdendo espaço frente à economia globalizada³¹. Nesse sentido, Ricardo Villas Bôas Cueva³² já afirmou que “o rápido desenvolvimento da informática multiplicou as possibilidades de invasão da intimidade”.

O foco do presente trabalho é, sobretudo, a questão relacionada à captação, armazenamento e manipulação de dados pessoais e as suas consequências, tanto mais em um Estado que ainda não possui uma legislação específica de proteção aos dados pessoais, como é o caso do Brasil. Faz-se necessário, para tanto, iniciarmos com a definição do tema.

Primeiramente, importa dizer que dado e informação, embora muitas vezes utilizados pela doutrina como sinônimos, na realidade, possuem definições diferentes. Segundo Setzer³³:

³¹ LIMBERGER, T. **Cibertransparência**: informação pública em rede: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016. p. 17.

³² CUEVA, R. V. B. **A insuficiente proteção de dados pessoais no Brasil**. Justiça & cidadania, Rio de Janeiro, v. 18, n. 195, p. 8-13, nov. 2016. p. 8.

³³ SETZER, V. W. **Dado, Informação, Conhecimento e Competência**. DataGramaZero - Revista de Ciência da Informação, [S. l.], n. zero, dez. 1999. Disponível em: <<https://www.ime.usp.br/~vwsetzer/datagrama.html>>. Acesso em: 30 nov. 2017.

Uma distinção fundamental entre dado e informação é que o primeiro é puramente sintático e o segundo contém necessariamente semântica (implícita na palavra 'significado' usada em sua caracterização). É interessante notar que é impossível introduzir semântica em um computador, porque a máquina mesma é puramente sintática (assim como a totalidade da matemática). Se examinássemos, por exemplo, o campo da assim chamada 'semântica formal' das 'linguagens' de programação, notaríamos que, de fato, trata-se apenas de sintaxe expressa através de uma teoria axiomática ou de associações matemáticas de seus elementos com operações realizadas por um computador (eventualmente abstrato).

Ademais, Valdemar W. Setzer³⁴ esclarece que dados são:

uma seqüência de símbolos quantificados ou quantificáveis. [...] podem obviamente ser armazenados em um computador e processados por ele. [...] um dado é necessariamente uma entidade matemática e, desta forma, puramente sintática. Isto significa que os dados podem ser totalmente descritos através de representações formais, estruturais. Dentro de um computador, trechos de um texto podem ser ligados virtualmente a outros trechos, por meio de contigüidade física ou por 'ponteiros', isto é, endereços da unidade de armazenamento sendo utilizada. Ponteiros podem fazer a ligação de um ponto de um texto a uma representação quantificada de uma figura, de um som, etc.

Ao presente trabalho importam, sobretudo, informações e dados pessoais. Feita a diferenciação entre informação e dado, ressalta-se que não existe uma corrente unitária do que seriam dados e informações pessoais. Importante mencionar, ainda, que em países que já possuem legislação acerca da proteção de dados pessoais, é imprescindível que a conceituação entendida por aquela lei seja especificada no próprio texto legal, a fim de entender o escopo e extensão daquela legislação específica.

Pierre Catala³⁵ entende que se trata de informação pessoal quando o objeto da informação é a própria pessoa:

Mesmo que a pessoa em questão não seja a 'autora' da informação, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade.

De um lado e de uma maneira generalista, pode-se dizer que existe uma corrente que entende que dados pessoais referem-se àqueles dados em que é

³⁴ SETZER, 1999.

³⁵ CATALA, Pierre. Ebauche d'une théorie juridique de l'information. **Informatica e Diritto**, [Paris], ano IX, n. 1, p. 15-31, jan. 1983. p. 20. Disponível em: <http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf>. Acesso em: 3 dez. 2017.

possível identificar uma pessoa de maneira direta³⁶. Para esses, tem-se, em resumo, que dados pessoais são dados referentes a uma pessoa já identificada.

Por outro lado e mais comumente utilizado na doutrina e em legislações sobre proteção de dados pessoais já criadas ao redor do mundo, – e no presente estudo entendida como a mais adequada - há o entendimento de que dados pessoais são aqueles dados que referem-se a pessoas indeneificadas ou identificáveis.

Nesse sentido, tal definição foi adotada, por exemplo, pela Convenção n. 108 do Conselho da Europa, em seu artigo segundo; bem como nas Linhas-Guia da Organização para Cooperação e Desenvolvimento Econômico sobre proteção da privacidade e fluxos transfronteiriços de dados pessoais, em seu artigo primeiro. Ademais, tal entendimento foi assimilado pela Diretiva Europeia 95/46/CE³⁷:

Artigo 2º. Para efeitos da presente diretiva, entende-se por:

a) <<Dados pessoais>>, qualquer informação relativa a uma pessoa singular identificada ou identificável (<<pessoa em causa>>); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica ou cultural.

Já no contexto brasileiro, tal conceituação está presente presente no Decreto nº 8771/2016³⁸:

Art. 14. Para os fins do disposto neste Decreto, considera-se:

I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e

³⁶ LIMBERGER, T. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

³⁷ PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho**, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias, n. L 281, p. 31-39, 23 nov. 1995. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em: 6 dez. 2017.

³⁸ BRASIL. **Decreto nº 8.771**, de 11 de maio de 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Diário Oficial da União, Brasília, DF, 11 maio 2016. Edição extra. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm>. Acesso em: 2 dez. 2017.

II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Esclarece-se, ainda, que dados pessoais são dados concretos ligados diretamente à pessoa. Assim,

[...] a informação pessoal refere-se às suas características ou ações, atribuíveis à pessoa em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então informações diretamente proveniente de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como opiniões que manifesta, e tantas outras.³⁹

Deste modo, importante salientar que dados que não forem concretos ou que são apenas indiretamente ligados à pessoa não são enquadrados como dados pessoais. Nesse sentido, tem-se que opiniões de outros indivíduos sobre uma determinada pessoa ou interpretações decorrentes da cognição de outra pessoa que não o indivíduo que emitiu o pensamento não são dados pessoais, dentre tantas outras situações de vínculo não-direto ou não concreto, ainda que relacionados a uma pessoa específica.

Após a explanação inicial acerca do que são dados e informações pessoais, importante ressaltar a emergente relação da proteção de dados pessoais com a tecnologia.

Em primeiro lugar, esclarece-se que o tratamento de dados não é um fenômeno que surgiu apenas com o desenvolvimento tecnológico. Esse tratamento pode ser feito, inclusive, apenas de forma manual, envolvendo apenas os seres humanos. Se quisermos, por exemplo, entender quais são os principais destinos de pessoas que pegam um trem com várias paradas, bastaria que tivéssemos acesso aos bilhetes físicos emitidos e fizéssemos o tratamento manual desses dados, dividindo por paradas de destino. Entretanto, ainda que possível, há que se reconhecer o esforço envolvido em tal tratamento: seja do ponto de vista de horas

³⁹ BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Caderno de Investigações Científicas. Brasília: Secretaria de Direito Econômico/Departamento de Defesa e Proteção do Consumidor, v. 2, cap. 1. 2010. p. 20. Disponível em: <<http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protECAo-de-dados-pessoais.pdf>>. Acesso em: 2 dez. 2017.

necessárias ou número de pessoas envolvidas nele, seja da dificuldade de ganho de escala.

Assim, facilmente percebe-se que o principal obstáculo à ampla utilização do tratamento de dados antes do desenvolvimento tecnológico não é relacionado à sua falta de utilidade ou importância, mas sim ao esforço envolvido no processo, afetando, para tanto, a sua velocidade e, como consequência, a sua eficiência.

Deste modo, o desenvolvimento tecnológico hoje presente na sociedade rapidamente fez desaparecer o principal obstáculo à utilização, dado que o tratamento e manipulação de dados pode ser feito de maneira veloz, eficiente e a um baixo custo, conforme já vimos ao longo do presente estudo.

4.2.1 Banco de Dados e *Big Data*

O que muito interessa quando fala-se de dados pessoais é o volume dessas informações que sistemas são capazes de captar, para posterior tratamento, manipulação e comunicação. Assim sendo, para viabilizar o tratamento e manipulação de um volume expressivo de informações, faz-se necessário o processamento automatizado de dados, o qual só é possível através de banco de dados automatizados.

Há que se reconhecer, portanto, que tais bancos de dados possibilitaram, ainda, uma gama de oportunidades para uso das informações nele contidas, as quais ainda não eram exploradas.

Segundo Doneda⁴⁰, bancos de dados são:

em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica costuma ser uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações.

Os bancos de dados, por sua vez, aumentam o alcance do número de pessoas que podem ter acesso a dados pessoais sobre terceiros, de maneira

⁴⁰ DONEDA, 2014, p. 65.

precisa e detalhada⁴¹. Nesse sentido, o reconhecimento de que o acesso por esses terceiros pode afetar tanto direta quanto indiretamente a vida dos indivíduos titulares dessas informações é necessário para a compreensão do problema. Novamente, se está diante de uma extensão do princípio da dignidade humana, ao mesmo tempo em que se pode ter inegáveis benefícios econômicos e sociais.

Muito embora *Big Data* não seja o foco do presente trabalho, há que se trazer uma atenção especial para essa forma de armazenamento de dados, muito utilizado no que tange tratamento, manipulação e comunicação de (e entre) dados pessoais. Em resumo, *Big Data* é a forma com que, por meio do uso de tecnologias específicas, pode-se juntar diversas fontes de informação a partir de correlações sistemáticas feitas, as quais, em princípio são dispersas, gerando, então, uma nova informação⁴². Em outras palavras:

One of the main targets of big data analytics is to use data, alone or in combination with other data sets, beyond their original point and scope of collection. The scalability of storage allows for potential infinite space, which means that data can be collected continuously until a new value can be created from insights derived out of them.⁴³

Considerando o potencial de escala, velocidade e eficiência gerado por *Big Data*, esse mecanismo tem se tornado elemento essencial para competitividade dos negócios. Nesse sentido, tem-se, inclusive, estudo feito pela consultoria McKinsey em parceria com MGI⁴⁴:

The amount of data in our world has been exploding, and analyzing large data sets—so-called big data—will become a key basis of competition, underpinning new waves of productivity growth, innovation, and consumer surplus.

⁴¹ DONEDA, 2014, p. 65.

⁴² BRASIL, 2010, p. 20.

⁴³ D'ACQUISTO, G. et al. **Privacy by design in big data**: An overview of privacy enhancing technologies in the era of big data analytics. [S. l.]: European Union Agency for Network and Information Security, Dec. 2015. p. 13. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport>. Acesso em: 7 dez. 2017.

⁴⁴ MANYIKA, J. et al. **Big data**: The next frontier for innovation, competition, and productivity. The McKinsey Global Institute, May 2011. Disponível em: <<https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation>>. Acesso em: 7 dez. 2017.

Em um sentido mais prático da aplicação, com o seu consequente efeito, Goulart⁴⁵ já pontuou que:

É certo que o consumidor, com o uso de tais cartões de fidelidade, consegue descontos e também ofertas personalizadas. Mas qual o custo disso? [...] Muitas instituições, atualmente, possuem um dossiê com todos os produtos que foram comprados por uma pessoa. [...] Alguns desses algoritmos, quando aplicados às compras em supermercados, identificam quando o cliente está diminuindo sua frequência de compras, o que dispara convites e promoções para atrair novamente o cliente. Essas práticas devem promover uma ampla reflexão sobre os impactos que o uso indiscriminado de informações pode causar no livre desenvolvimento da personalidade humana.

Portanto, tratando-se de desenvolvimento tecnológico que permite a análise, tratamento, manipulação e comunicação de dados pessoais em um número massivo, tanto mais à medida em que tornou-se elemento de competitividade dos negócios em um sistema econômico capitalista, a tutela jurídica deve pairar não só sobre os dados pessoais por si só, mas também como as tecnologias utilizadas sobre os mesmos, a exemplo de *Big Data*.

4.2.2 A democratização da tecnologia e a proteção de dados pessoais

Nesse contexto, tem-se, então, o que muitos têm chamado de *o petróleo da nova era*: os dados pessoais. Ainda que passível de muitas críticas a analogia feita entre petróleo e os dados pessoais, considerando que o primeiro se trata de um recurso natural disponível, ainda que limitadamente, e o segundo diga respeito diretamente à pessoa, não se pode negar que os dados pessoais surgem, assim como o petróleo surgiu há algumas décadas, como matéria prima de novos processos econômicos e sociais, desencadeados na Sociedade da Informação.

E, assim sendo, torna-se tanto um bem jurídico quanto um bem econômico, cuja proteção, principalmente por ter relação direto com a pessoa, necessita ser debatida e efetivada pelo direito.

⁴⁵ GOULART, G. D. **Por uma visão renovada dos arquivos de consumo**. Revista de Direito do Consumidor, [S. l.], v. 107/2016, p. 447-482, set./out. 2016.

As possibilidades de tratamento e manipulação de dados tem chamado a atenção tanto do setor privado quanto do setor público, uma vez que diretrizes preciosas surgem a partir dessa análise, seja para os negócios, seja para a governança pública.

Salienta-se que o que tem chamado atenção na questão de tratamento e manipulação dos dados, tanto no setor privado quanto no setor público, não se refere ao dado por si só, individual e específico – o que, obviamente, não tira o valor do dado pessoal independentemente do tratamento, mas sim as diretrizes e informações valiosas que podem surgir a partir da análise massiva desses dados, a qual só é possível quando os bancos de dados, dos quais já falamos anteriormente, são compostos por muitos deles, a ponto de serem verificadas tendências e de onde surgem, muitas vezes, novas informações a partir de um conjunto de informações.

Depreende-se, portanto, que o verdadeiro valor dos dados pessoais parte de uma organização de dados dispersos em dados organizados, transformando-os, tarefa essa que em muito foi e ainda é facilitada pelo desenvolvimento tecnológico. A ideia central disso é relacionada à previsão e modificação do comportamento humano como forma de produzir lucro – tendo como base, evidentemente, o acesso aos dados pessoais.

Para tanto, é inegável o papel fundamental que internet possui na colheita dos dados pessoais. Nesse sentido, importante ressaltar que dados do Instituto Brasileiro de Geografia e Estatística – IBGE, em parceria com o Comitê Gestor da Internet no Brasil – CGI – BR, mostraram que, no ano de 2015, 62% dos domicílios brasileiros utilizavam a internet⁴⁶. Considerando o crescimento acelerado do acesso à internet, facilmente se entende a rápida solidificação da Sociedade da Informação não só de uma perspectiva global, mas também de uma perspectiva nacional.

Nesse contexto, a proteção do acesso à internet – e o que será feito a partir dele – torna-se necessária como tutela jurídica à preservação da dignidade da

⁴⁶ INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. Acesso à Internet e à Televisão e Posse de Telefone Móvel Celular para Uso Pessoal. In: _____. **Pesquisa Nacional por Amostra de Domicílios**. [Rio de Janeiro]: IBGE, 2008, 2011, 2013, 2014, 2015. Suplementos. Disponível em: <http://www.ibge.gov.br/home/xml/suplemento_pnad.shtm>. Acesso em: 8 dez. 2017.

pessoa humana no ambiente virtual⁴⁷. Além disso, devemos considerar que o acesso à internet tornou-se, ainda, direito básico para acesso a uma gama de serviços privados e para facilitação de serviços públicos, a exemplo de comércio eletrônico em geral e emissão de certidões públicas.

Fato é que a democratização da internet, ao mesmo tempo em que traz muitas evoluções positivas na Sociedade da Informação, como o acesso a massivo a conteúdos que antes ficavam restritos a só uma forma de comunicação midiática, traz também inúmeras preocupações que, infelizmente, ainda não atingiram a todos na mesma proporção, como a proteção de dados pessoais. Dentre as maravilhas possibilitadas pelo acesso à internet podemos citar, ainda, a revolução da interação entre as pessoas, ainda que extremamente distantes fisicamente, e as novas formas de entretenimento por ela produzida.

O que tem-se, a partir dessa análise, é um grande desafio: como propiciar a inovação tecnológica sem desrespeitar direitos humanos fundamentais? Nesse sentido, a própria Resolução A/HRC/32/L.20, das Nações Unidas, a qual tem por uma de suas finalidades a proteção dos direitos humanos na internet, diz que “*the same rights that people have offline must also be protected online*”⁴⁸.

O que ocorre, hoje, é que muitas vezes as pessoas precisam optar entre o acesso às maravilhas fornecidas pelo desenvolvimento tecnológico e a proteção de seus dados pessoais. Ainda que os serviços possuam, por exemplo, termos de uso e privacidade, o acesso só é possível quando tais termos são aceitos em sua totalidade. Aplicativos de celular focados em trânsito e navegação, ao mesmo tempo que permitem que cheguemos de maneira mais eficiente ao local de destino, colhem todas informações acerca das nossas localizações e, não raro, podem utilizar essas informações para outros fins que não o de auxílio na navegação de trânsito.

⁴⁷ GOULART, G. D. **O impacto das novas tecnologias nos direitos humanos e fundamentais: o acesso à internet e a liberdade de expressão.** Revista Direitos Emergentes na Sociedade Global, vinculada ao Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria, [Santa Maria], v. 1, n. 1, p. 145-168. jan./jun. 2012. ISSN 2316-3054. Disponível em: <<https://periodicos.ufsm.br/REDESG/article/view/5955#.WVIKR-vyvio>>. Acesso em: 12 dez. 2017.

⁴⁸ UNITED NATIONS. Human Rights Council. **Resolution A/HRC/32/L.20.** The promotion, protection and enjoyment of human rights on the Internet. [Geneva], 27 June 2016. Disponível em: <<https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf>>. Acesso em: 9 dez. 2017.

Inegável, portanto, a proliferação de informações na rede, de maneira rápida e eficiente, e segundo Solove⁴⁹:

We are in the midst of an information revolution, and we are only beginning to understand its implications. The past few decades have witnessed a dramatic transformation in the way we shop, bank, and go about our daily business – changes that have resulted in an unprecedented proliferation of records and data. Small details that were once captured in dim memories or fading scraps of paper are now preserved forever in the digital minds of computers, in vast databases with fertile fields of personal data.

Tem-se, portanto, que faz-se necessária tutela jurídica para que tais condutas, ainda que possibilitadas por consentimento aos termos de uso, sejam cobertas por critérios jurídicos mínimos. Nesse sentido, o regramento existente inclusive em países mais avançados no assunto, como Itália e França, no que tange os limites impostos juridicamente ainda não são capazes de acompanhar a dinamicidade presente na Sociedade da Informação, vivida majoritariamente na rede.

No contexto brasileiro, ainda que existente o Marco Civil da Internet⁵⁰, o qual representou um grande avanço no que tange a regulação do uso da internet no Brasil, não se tem uma cobertura acerca da proteção de dados pessoais, ponto primordial para o respeito à dignidade humana na esfera *online*.

Ademais, o processo de globalização acelera ainda mais as mudanças e evoluções decorrentes do uso da tecnologia e, em especial, da internet. Outro desafio que surge diz respeito a trocas de informações e dados na esfera internacional – ora, pois, se sequer se consegue controlar satisfatoriamente no contexto nacional, há muito o que evoluir em um contexto internacional.

O que tem-se, em resumo, considerando a Sociedade da Informação, a democratização da tecnologia e a massiva perpetração de dados pessoais em rede, é a necessidade de adequação do direito à realidade fática dessa nova forma de organização geral da sociedade, por meio de regulação que foque no resguardo de

⁴⁹ SOLOVE, 2004, p. 1.

⁵⁰ BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Poder Executivo, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 9 dez. 2017.

direitos fundamentais também no mundo *online* e, tanto mais, na dignidade da pessoa humana.

5 GOVERNANÇA ALGORÍTMICA

Que se vive hoje na era digital é inegável, assim como não se pode negar que a coleta, armazenamento e manipulação de dados está ao alcance das pessoas de maneira muito mais fácil do que antigamente em função do desenvolvimento tecnológico, conforme já demonstrado no presente trabalho.

Entretanto, há que se considerar que por trás dessas possibilidades, que muitas vezes apresentam-se como maravilhas para a sociedade – e por muitas vezes realmente o são, tem-se um objeto fundamental: os algoritmos.

À medida que os algoritmos tomam lugares tão importantes na sociedade, inclusive como partes essenciais no desencadeamento de processos sociais e econômicos, é necessário lembrar, ademais, que a existência de uma governança específica para os mesmos torna-se primordial no que diz respeito à proteção de dados pessoais.

5.1 OS ALGORITMOS

O algoritmo pode ser definido como “um conjunto previsto de regras ou instruções bem definidas para a solução de um problema, como o desempenho de um cálculo, em um número finito de etapas”⁵¹. Nesse sentido, podemos afirmar que para que o processamento possa ser feito pelos algoritmos, os mesmos devem receber instruções e informações suficientemente detalhadas, para que possam fazer o processamento.

Ainda que os algoritmos sejam muito mais comumente utilizados no ramo da informática, o seu conceito não necessariamente se esgota nessa área. Em uma interpretação geral, podemos associar à realização de um conjunto de tarefas, a partir de um passo-a-passo que tenha como característica a repetibilidade, cuja

⁵¹ BUTTERFIELD, A.; NGONDI, G. E. **A Dictionary of Computer Science**. 7. ed. New York: Oxford University Press, 2016.

implementação, a depender do contexto, poderá ser realizada, por exemplo, por uma máquina, por um programa de computador ou até mesmo por um ser humano.

Em que pese a tendência de entendimento geral seja a de considerar algoritmos como algo puramente matemático, objetivo e neutro, e, assim sendo, consequentemente natural, essa não condiz estritamente com a realidade. Salienta-se que a visão de quem faz coleta de dados ou os processa por meio de algoritmos nem sempre está focada exclusivamente no objeto de coleta.

Algoritmos são, de fato, matemáticos e objetivos, entretanto, não são neutros e dependendo do tratamento que for dado, podem inclusive causar problemas sociais, como a discriminação e o controle social, ou a alteração de processos econômicos, a exemplo dos preços, o que ocorre de maneira automática em sites de *e-commerce*⁵².

O impacto dos uso de algoritmos vem sendo estudado ao longo do tempo, tanto no sentido positivo quanto no sentido negativo, para além da sua definição e de como como eles funcionam, levando em consideração seus diferentes aspectos – que não só aqueles objetivos.

Nesse sentido, tem-se então que algoritmos são relevantes do ponto de vista jurídico muito mais pela sua aplicação prática e pelas consequências de tal aplicação do que por uma análise singular de seu funcionamento técnico.

Na busca pelo que Pedro Domingos chama de *Algoritmo Mestre*, ele pesquisa e mostra diferentes orientações sobre algoritmos, sempre relacionando-as à forma de conhecimento. Em resumo, existiriam cinco delas.

⁵² “No ano de 2016, houve um acidente aéreo com a aeronave que levava o time de futebol denominado ‘Chapecoense’, da cidade de Chapecó/SC, o qual causou a morte de cerca de setenta pessoas, entre eles, jogadores e empregados do clube. No dia do acidente, as camisas do clube estavam, inicialmente, com pouco mais que a metade do valor do qual encontrava-se no fim do dia, no e-commerce da empresa NetShoes. Acusada de focar na obtenção de lucro com a tragédia, a empresa se pronunciou informando que o valor do início do dia referia-se a um valor promocional, e que assim que as unidades promocionais terminaram, um algoritmo automaticamente retornou ao valor original, que seria o referente ao valor do final do dia.” (MIOZZO, J. **Após rumores de que teria aumentado preço da camisa da Chapecoense, Netshoes se pronuncia**. In: InfoMoney, 29 nov. 2016. Disponível em: <<http://www.infomoney.com.br/negocios/grandes-empresas/noticia/5878682/apos-rumores-que-teria-aumentado-preco-camisa-chapecoense-netshoes-pronuncia>>. Acesso em: 7 dez. 2017.)

A primeira diz respeito ao que o autor chama de *Inductive Reasoning*, para os quais o aprendizado se dá não pela dedução, mas sim pelo inverso dela, utilizando um complexo de ideias da psicologia, lógica e filosofia. A segunda, referente à *Connectionism*, fala sobre o interesse e estudo da chamada *engenharia reversa* do cérebro, em um estudo interdisciplinar entre a física e a neurociência. Na terceira orientação aparecem os *Evolutionary Computation*, com a simulação da evolução no computador, com foco na biologia, especialmente na genética. Tem-se, então, a quarta orientação, com um viés fortemente ligado à estatística, os quais colocam o aprendizado, primordialmente, como uma inferência da probabilidade e são chamados de *Bayes Theorem*. Por último, aparecem os *Analogical Modelling*, para os quais o aprendizado é construído a partir de similaridades detectadas, que produzem, ainda, julgamentos não apenas pelo caráter objetivo, mas também sob influência da psicologia.⁵³

O autor conclui seu estudo dizendo que no caso de existir um algoritmo que junte as características das cinco orientações por ele apresentada – e constituindo, portanto, um sistema complexo – teria o que chamou-se de algoritmo mestre. A partir da existência desse algoritmo mestre, teríamos, como derivada, a totalidade de conhecimentos, os quais incluem todos os espaços temporários (passado, presente e futuro) a partir de dados.⁵⁴

Em um estudo que traz à tona, principalmente, as consequências sociais negativas advindas de algoritmos e da sua ampla utilização, Cathy O’Neil mostra de que forma os algoritmos tornam-se formas de discriminação social, com a discriminação derivada da raça e classe, amplificando, portanto, as desigualdades já existentes no mundo moderno, como consequência do modelo econômico capitalista.

Nesse sentido, um exemplo utilizado ao longo do livro pela autora foi a das consultas feitas por empresas de concessão de crédito, por meio de algoritmos, a fim de verificar a possível (in)viabilidade de tal concessão, considerando a chance

⁵³ DOMINGOS, P. **The Master Algorithm**: How the Quest for the Ultimate Learning Will Remake Our World. *Journal of Computer Science and Technology*, New York, 2015, v. 15, p.157-158.

⁵⁴ DOMINGOS, 2015, p.157-158.

de inadimplência. Essa prática é utilizada em diversas partes do mundo, sendo certo que a partir da identificação de padrões que se repetem, caracterizando algumas tendências – que são o foco desse tipo de algoritmo, ou seja, encontrar similaridades existentes e que geralmente possuem como base dados pessoais - há a posterior criação de perfis (*profile*) de bons ou maus pagadores, o que por muitas vezes acaba levando em consideração a raça ou bairro em que a pessoa mora. A lição de Cathy O’Neil com esse e outros exemplos trazidos ao longo do estudo é no sentido de que quando se tem uma pessoa com baixo poder econômico em busca de empréstimo para custear seus estudos, a partir do momento em que tal empréstimo lhe é negado considerando o bairro em que mora ou a própria raça, o estudo pretendido fica inviável, entrando, portanto, em uma sequência de negação de oportunidades para a pessoa em questão e, conseqüentemente, ampliando a desigualdade.⁵⁵

No caso de a decisão de negação de concessão de crédito ser efetuada, na maioria das vezes isso se dá unicamente com base em um algoritmo ou em um conjunto deles – pode-se dizer que os próprios algoritmos acabam por decidir a quem deverá ser concedido ou não o crédito, de acordo com o risco de inadimplência. Inicialmente, o fato de a decisão ser tomada por um algoritmo pode trazer uma ideia de decisões com tratamento igual para diferentes pessoas, ou seja, tendo como base as mesmas regras, ao passo que o que verdadeiramente ocorre é o contrário, com o endosso e aumento das desigualdades sociais e discriminações, as quais são fruto da opacidade, falta de regulação e possibilidade de ganho de escala dos modelos de algoritmos. Adiciona-se, ainda, o fato de que vieses vão sendo criados nas próprias máquinas ao longo do tempo, aumentando ainda mais a desigualdade e discriminação.⁵⁶

Ao mesmo tempo em que o uso de algoritmos se apresenta como muitas utilidades benéficas para a sociedade em geral, por outro, se não utilizado com ética e de acordo com as legislações, poderá se tornar instrumento de controle social,

⁵⁵ O’NEIL, C. **Weapons of Math Destruction**: How Big Data Increases Inequality and Threatens Democracy. Denver: Crown, 2016.

⁵⁶ DOMINGOS, 2015.

uma vez que há de se reconhecer que a o acesso à informação em muito funciona como elemento primordial da possibilidade de controle social.

O tamanho do risco de tal controle é considerável e já é possível encontrar estudos que afirmam que vivemos, hoje, no que é chamado de *capitalismo de vigilância*. Essa denominação é feita considerando as alterações nos processos econômicos, com graves infrações ao direito de privacidade pela forma de utilização de *big data* (coleta e análise), pela existência de contratos inteligentes a partir da possibilidade de melhor monitoramento, pela customização de ofertas com origem no acesso a dados pessoais como estratégia de marketing (e os consequentes efeitos sobre as capacidades cognitivas dos indivíduos) e, por fim, pela possibilidade de melhoria contínua e veloz desses processos, muitas vezes por meio de aprendizagem automática.⁵⁷

5.1.1 Desafios relacionados ao uso de algoritmos, responsabilização e proteção de dados pessoais

No contexto atual, não raro é ver algoritmos que possuem resultados concretos, a partir de decisões, avaliações e análises feitas, em grande parte, a partir de dados pessoais coletados. O aumento do poder computacional, adicionado da facilidade e escala de obtenção de dados trazem uma magnitude e complexidade inimaginável, com impactos diretos no ponto de vista jurídico.

Tem-se, da mesma forma, aumento dos desafios a serem enfrentados pelo uso dos algoritmos e pelas decisões por ele tomadas, as quais, por muitas vezes, excluem os seres humanos do centro do poder decisório, tornando-os apenas mensageiros das decisões tomadas por máquinas, com critérios próprios.

Ainda que a programação inicial de algoritmos individuais seja feita por seres humanos, seus efeitos nem sempre são mensuráveis por quem os programou, além da dificuldade de tradução minuciosa de passos que algoritmos dão até

⁵⁷ ZUBOFF, S. **Big Other**: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, [S. l.], v. 30, issue 1, p. 75-89, Apr. 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754>. Acesso em: 12 dez. 2017.

produzirem, de fato, algum resultado, a qual será melhor explicada ao longo do presente trabalho.

Salienta-se, ainda, que um dos principais focos de utilidade de algoritmos está relacionado à realização do que não é possível ser feito por padrões humanos, a exemplo da velocidade, escalabilidade e eficiência de análises, o que por si só já demonstra a dificuldade de entendimento do passo-a-passo por humanos, ainda que esse indivíduo seja aquele que os programou.

Ademais, há que se reconhecer que os efeitos dos algoritmos nem sempre se dão de uma maneira individual, a exemplo dos algoritmos de aprendizagem automática, também chamados de algoritmos de autocorreção. Os algoritmos de aprendizagem automática são aqueles que se modificam com base nos dados que estão sendo analisados, isso quer dizer, há o aprendizado pelo próprio algoritmo a partir de determinadas análises, o qual ocorre independentemente de ação humana, de forma que o próprio algoritmo cria novos algoritmos, para que não seja necessária nova criação humana. Esse processo faz parte de uma rotina embutida no próprio algoritmo, a qual se repete continuamente. Em resumo, dessa forma teremos algoritmos que foram formados automaticamente a partir de outros algoritmos.⁵⁸

No contexto da proteção de dados pessoais, considerando que a coleta, armazenamento e tratamento desse dados é feita, em sua maioria, por algoritmos, alguns desafios merecem nossa atenção, para fins de entendimento de como relacionam-se.

5.1.1.1 Necessidade de ligação à uma base de dados

Algoritmos e suas utilidades trazem consigo uma gama de benefícios, tanto para indivíduos quanto em nível de empresas e sociedade no geral. Entretanto, quando não utilizados de uma maneira ética, apresentam riscos extremamente relevantes, principalmente no que tange à privacidade e à proteção de dados

⁵⁸ DOMINGOS, 2015.

peçoais. Isso ocorre porque, para cumprirem sua valoraçãõ positiva, é necessário que estejam ligados à uma base de dados.

A utilidade dos algoritmos aumentou e adquiriu um caráter muito mais importante quando a esses foi possível a conexão à uma base de dados. Isso ocorre porque os algoritmos, por si só, não possuem sentido próprio, a não ser que sejam conectados de alguma maneira à uma base de dados, a partir da qual poderão atuar. Assim, conclui-se que quando não ligados à uma base de dados, são inertes.⁵⁹

A partir da necessidade de ligação à uma base de dados para a construção de sentido do uso de algoritmos para essa finalidade, o que hoje ainda não fica claro é sobre quais dados esses algoritmos atuarão.

Há que se reconhecer, ainda, que por muitas vezes a base de dados é composta por uma gama de dados peçoais ou sensíveis, sem que as peçoas às quais os dados são relacionados saibam sobre quais são levados em consideração para a produção de resultados.

Por um lado é importante que a peçoia à qual os dados são relacionado tenha acesso a quais deles são considerados e produzem determinados resultados. Por outro lado, tal abertura pode apresentar uma ameaça a outros pontos importantes, tais quais sigilo comercial, propriedade intelectual, concorrência, dentre outros, uma vez que a referida abertura implicaria na transparência de processos internos empresariais.

É certo, ainda, que na formação desses bancos de dados, por muitas vezes se tem o consentimento geral do usuário, ponto que gera controvérsias na discussão sobre o tema. Entretanto, a necessidade de consentimento integral do uso de dados é dada pelo usuário, na maioria das vezes, como mera formalidade para que o mesmo possa utilizar um determinado serviço e, não raro, o usuário não possui o entendimento do que significam os termos de consentimento.

Fica evidente, portanto, que o consentimento deve ser uma ferramenta válida para a utilização do banco de dados, mas, ao mesmo tempo, os termos de

⁵⁹ GILLESPIE, T. **The Relevance of Algorithms**. Cambridge: MIT Press, 2014.

consentimento devem ser temperados com princípios básicos de ordem pública, a fim de equilibrar a relação entre usuários e detentores dos bancos de dados.

Analogia pode ser feita ao processo de criação do Código de Defesa do Consumidor, que teve como premissa o reconhecimento da vulnerabilidade da figura do consumidor frente às empresas das quais consumia produtos. As regras de tal Código acabaram servindo, portanto, como balizadoras da relação consumeirista, com foco em instrumentos que possibilitassem o equilíbrio entre as partes, a partir do reconhecimento de disparidade de forças.

5.1.1.2 Opacidade

Surge, então, um dos principais desafios relacionados aos algoritmos: sua opacidade, que está diretamente ligada à dificuldade de descrever ou ter acesso a todos os passos dados pelos algoritmos até chegar a uma decisão. Isso quer dizer que tal dificuldade impede a decodificação integral da maneira com que se chegou a determinados resultados, os quais muitas vezes causam impactos concretos na vida em sociedade, conforme já demonstrado.

Frank Pasquale entende existir *algoritmos secretos* que são capazes de controlar a economia e processos econômicos a partir do acesso às informações. Ademais, tais informações poderiam ser manipuladas ao longo do tempo, de maneira a alterar comportamentos humanos, por exemplo. Para tanto, o termo *black box* que consta já no título do livro e é referido por diversas vezes ao longo do estudo, teria um duplo sentido. O primeiro diz respeito à analogia com as caixas-pretas de aviões, as quais armazenam, através de um sistema próprio, todas as informações de voz e dados existentes nos aviões, de modo que o entendimento aqui é que estamos vivendo numa sociedade de supervigilância, a partir de uma análise mais sociológica do resultado do uso massivo de dados e algoritmos. O segundo sentido representa a opacidade dos algoritmos, sendo em sentido

figurado algoritmos fechados, que conseqüentemente não podemos ver ou fazer o devido rastreamento.⁶⁰

A característica da opacidade causa efeitos, ainda, no que tange o desconhecimento de quais dados do banco de dados interligado que foram utilizados para a tomada de decisão pelo algoritmo. Isso quer dizer, portanto, que se terá decisões tomadas por algoritmos em que a busca pela explicação ou pelo tipo de dados utilizado não será possível, nem para a pessoa à qual os dados de referem. Em resumo, existirão resultados com projeções diretas em um indivíduo, produzidos com base em seus dados pessoais, em que o indivíduo que produziu tais dados e, portanto, é detentor dos mesmos, não terá acesso ao racional pelo qual se chegou a uma determinada decisão.

Depreende-se, portanto, que além de um desafio técnico em sentido estrito causado pela opacidade dos algoritmos, tem-se um desafio jurídico de entendimento e responsabilização.

A partir do momento em que a decodificação da forma com que se chegou a determinado resultado não pode ser feita, de que maneira seria possível o entendimento do embasamento que deu origem a cada resultado? Trata-se de uma pergunta com resposta retórica, uma vez que quando não inviabiliza completamente tal entendimento, a opacidade dificulta qualquer análise minuciosa, impossibilitando, para tanto, o entendimento integral.

Tem-se, ainda, que diante da impossibilidade citada acima, o desafio jurídico adquire uma nova conotação, a qual gira em torno da responsabilidade sobre os resultados. A partir da existência da opacidade, a dificuldade de identificação da cadeia é consequência natural. Uma vez que não é passível de entendimento os passos que levaram a um determinado resultado, no caso de esse resultado ser discriminatório, por exemplo, quem deveria ser responsabilizado juridicamente?

As possibilidades de responsabilização são muitas, a exemplo e sem se limitar, ao programador que deu origem ao algoritmo-base ou da empresa que

⁶⁰ PASQUALE, F. A. **The Black Box Society**: The Secret Algorithms that Control Money and Information. Cambridge: Harvard University Press, 2016.

iniciou esse processo. Nesse caso, poderíamos pensar no sentido de que se está diante da aplicação do risco-proveito.

Entretanto, não é justo que um procedimento que sofre tantas interferências ao longo do tempo, inclusive decorrentes da aprendizagem automática dos algoritmos que acabam por gerar outros algoritmos, tenha apenas a pessoa ou empresa que iniciou o processo, a qual sequer tem capacidade de mensurar os resultados, tenha a responsabilidade exclusiva e integral por eventuais danos causados. Por outro lado, a não responsabilização de nenhuma das partes envolvidas no processo também não parece ser uma opção viável.

5.1.1.3 A (falta de) neutralidade

Apesar da visão inicial geral relacionada a algoritmos nos indiquem que eles são, conforme já mencionado no presente trabalho, matemáticos e objetivos e, portanto, neutros, isso não condiz com a realidade.

Nos ensinamentos de Silveira⁶¹:

Nem softwares, nem os algoritmos nele contidos são neutros. Eles geram efeitos e foram criados e desenvolvidos para determinadas finalidades. Apesar de serem imateriais e invisíveis, os algoritmos têm um ponto de partida e uma finalidade original que pode ter sido alterada pelos seus usuários ou pelo próprio algoritmo [...] algoritmos são invenções e, como toda invenção, guarda as intenções dos seus criadores.

Para tanto, é necessário levar em consideração não só o ponto de partida de cada algoritmo, mas também a finalidade inicialmente pretendida com o mesmo. Algumas perguntas básicas para reflexão sobre o tema poderiam ser *Quem programou?*, *Para quem programou?* e *Quando programou?*.

Com isso, o desenvolvimento tecnológico torna-se um desafio ainda maior dentro dos órgãos públicos. Ao mesmo tempo que o setor privado tem muito a contribuir nesse aspecto, uma vez que as tecnologias utilizadas por esses, de

⁶¹ SILVEIRA, S. A. **Governo dos Algoritmos**. Revista de Políticas Públicas, São Luiz, v. 21, n. 1, p. 267-281, jan./jun. 2017. p. 271-272. Disponível em: <<http://www.periodicoseletronicos.ufma.br/index.php/rppublica/article/view/6123>>. Acesso em: 12 dez. 2017.

maneira geral, estão muito à frente daquelas utilizadas pelos setores públicos, a falta de neutralidade dos algoritmos surge como uma ameaça ao uso das mesmas.

Há que se considerar, para tanto, a incapacidade do setor público no Brasil suportar em larga escala a utilização de novas tecnologias, tanto pela falta de recursos financeiros, quanto por falta de interesse dos seus integrantes. Se considerado o apoio do setor privado como uma opção viável para avanços tecnológicos, dever-se-á considerar qual o interesse envolvido nesse apoio, cuja finalidade por muitas vezes ficará comprometida pela falta de neutralidade.

Ademais, os próprios mecanismos de autocorreção dos algoritmos podem interferir nessa neutralidade, alterando a relevância dos dados e possuindo influência direta na construção de padrões e tendências.

Existe, ainda, a necessidade de neutralidade da rede como um todo e não apenas dos algoritmos que a compõem. Quando se fala em neutralidade da rede, se quer dizer que todas as informações constantes na rede (a exemplo da *internet* mas não se limitando à mesma) devem receber o mesmo tratamento, a fim de não influenciar o acesso dos indivíduos a determinados conteúdos, por exemplo, ferindo a sua autonomia ou causando discriminação. Salieta-se, ainda, que quando se refere ao tratamento, é de uma maneira integral, englobando, portanto, velocidade, livre acesso a diferentes conteúdos, dentre outros.

Nesse sentido, o próprio Marco Civil da Internet no Brasil⁶² refere a preservação e garantia da neutralidade na rede como um princípio básico do uso da internet no país. Entretanto, há que se reconhecer que muitos desafios estão e continuarão sendo enfrentados até que a neutralidade exista de uma maneira integral.

⁶² BRASIL, 2014, art. 3, IV.

5.2 A NECESSIDADE DA GOVERNANÇA DOS ALGORITMOS

No subcapítulo anterior, viu-se os principais desafios em torno do uso dos algoritmos e sua conseqüente relação com os dados pessoais, tanto de um ponto de vista mais técnico, quanto no que tange as suas principais implicações do ponto de vista jurídico.

Entretanto, mesmo diante dos desafios apresentados e dos possíveis impactos negativos, a presença e o nível de penetração dos algoritmos computacionais na sociedade da informação impedem que se volte ao status anterior, no qual a presença de tais algoritmos ainda não era disseminada – e, conseqüentemente, o uso de dados pessoais não se dava de uma maneira tão eficiente quanto a partir de algoritmos.

Assim, fica clara uma mudança de paradigma social acerca da matéria⁶³:

[...] percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social [...] Tanto o Estado como seus entes privados utilizavam intensamente o fluxo de informações pessoais para o seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito frequentemente na exclusão de algum aspecto da vida social.

Nesse contexto, o intenso uso de softwares, aplicativos de celular e demais sistemas implicam, obrigatoriamente, na ampla disseminação e uso dos algoritmos, bem como dos dados – muitas vezes pessoais - em torno deles⁶⁴. Como exemplos de meios de disseminação e utilização de algoritmos pode-se citar celulares, televisões conectadas, semáforos inteligentes⁶⁵, sistemas de *score* de crédito⁶⁶, dentre outros.

⁶³ BRASIL, 2010, p. 42

⁶⁴ MANOVICH, Lev. **Software takes command**. New York: A&C Black, 2013.

⁶⁵ Como exemplo de semáforo inteligente no Brasil podemos utilizar aqueles que foram implementados na cidade de Curitiba, no estado do Paraná, nos quais idosos e pessoas com deficiência e mobilidade reduzida podem passar o cartão de isento do ônibus, ou seja, cartão que comprova tais condições, a fim de aumentar o tempo de travessia dos semáforos. (CURITIBA. Agência de Notícias da Prefeitura de Curitiba. **Idosos podem usar cartão de isento para aumentar tempo de travessia**. Curitiba, 6 mar. 2017. Disponível em: <<http://www.curitiba.pr.gov.br/noticias/idosos-podem-usar-cartao-de-isento-para-aumentar-tempo-de-travessia/41404>>. Acesso em: 15 dez. 2017.)

⁶⁶ Sistemas de *score* de crédito são sistemas construídos para dar pontuações aos consumidores, a quais tem por base seu perfil, gerando a pontuação a partir de dados anteriores coletados e

Os dados podem ser, portanto, oriundos tanto de sistemas informatizados quanto de sensores que cada vez mais fazem parte do dia a dia, o que só é possível através do que hoje é conhecido como internet das coisas⁶⁷.

Observa-se, ainda, que no exemplo da utilização de semáforos inteligentes que aumentam o tempo de travessia de idosos, uma informação inicialmente objetiva como a informação de que uma pessoa idosa está atravessando a rua, pode se tornar uma informação com alto valor de mercado, dependendo da finalidade com que utilizada.

armazenados, classificando, assim, o maior ou menor risco de inadimplência. A legalidade de tais sistemas foi objeto de julgamento enquanto recurso repetitivo no Superior Tribunal de Justiça, REsp 1419697/RS, na qual reconheceu-se a legalidade da prática, desde que presente critérios específicos, conforme ementa:

“RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA "CREDIT SCORING". COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL. I - TESES: 1) O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). 2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). 3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011. 4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas. 5) O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados. II - CASO CONCRETO: 1) Não conhecimento do agravo regimental e dos embargos declaratórios interpostos no curso do processamento do presente recurso representativo de controvérsia; 2) Inocorrência de violação ao art. 535, II, do CPC. 3) Não reconhecimento de ofensa ao art. 267, VI, e ao art. 333, II, do CPC. 4) Acolhimento da alegação de inocorrência de dano moral "in re ipsa". 5) Não reconhecimento pelas instâncias ordinárias da comprovação de recusa efetiva do crédito ao consumidor recorrido, não sendo possível afirmar a ocorrência de dano moral na espécie. 6) Demanda indenizatória improcedente. III - NÃO CONHECIMENTO DO AGRAVO REGIMENTAL E DOS EMBARGOS DECLARATÓRIOS, E RECURSO ESPECIAL PARCIALMENTE PROVIDO.” (BRASIL. Superior Tribunal De Justiça. Terceira Turma. **Recurso Especial Representativo de Controvérsia nº 1419697**. Recorrente: Boa Vista Serviços S/A. Recorrido: Anderson Guilherme Prado Soares. Relator: Ministro Paulo de Tarso Sanseverino. Brasília, 12 de novembro de 2014. Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/152068666/recurso-especial-esp-1419697-rs-2013-0386285-0>>. Acesso em: 13 dez. 2017.)

⁶⁷ “A internet das coisas (do inglês, *Internet of Things, IoT*), é uma rede de objetos físicos, veículos, prédios e outros que possuem tecnologia embarcada, sensores e conexão com rede capaz de coletar e transmitir dados.” (INTERNET das coisas. In: **Wikipédia**, a enciclopédia livre, 2017. Disponível em: <https://pt.wikipedia.org/wiki/Internet_das_coisas>. Acesso em: 13 dez. 2017.)

Por exemplo, partindo da tendência de que idosos tem um gasto maior com medicamentos do que pessoas mais jovens, a informação de qual região da cidade possui maior circulação de pessoas idosas pode ser valiosa para empresários que queiram abrir uma farmácia, focando no ganho de capital com essa informação – a qual, de maneira isolada e individual pode não ter um valor elevado, mas a partir do momento que analisada a partir do ganho escala, com os principais pontos de circulação de idosos em uma cidade, torna-se uma informação com valor de mercado.

Para tanto, é fundamental que o critério da finalidade para a qual os dados foram coletados esteja sempre em foco, para que não se faça um uso inadequado dos dados, que em geral seria de maneira mais extensa daquela pelo qual o dado foi coletado.

Além da possibilidade de extensão de uso de dados pessoais para além daqueles inicialmente indicados como finalidade, tem-se um aspecto interessante relacionado às possibilidades econômicas não decorrentes, necessariamente, de uso inadequado de dados relacionado às suas finalidades. Nesse sentido, Silveira⁶⁸ esclarece:

Na fase atual da economia pós-industrial, a informação sobre consumo da mercadoria retorna ao capitalista como elemento crucial do processo de reprodução do capital. Os dados sobre como o produto foi consumido, o horário exato da compra e os metadados da transação chegam antes ou junto com o dinheiro resultante do processo de circulação. Assim, o crescimento das transações de compra e venda realizadas pelas redes digitais gera cada vez mais dados sobre o perfil do consumidor que adquiriu uma mercadoria.

Tais dados podem dar origem, ainda, a um processo especulativo, na combinação de tendências de mercado com a estratégia de marketing das empresas com o aparecimento de notícias específicas com foco na alteração de comportamento dos consumidores.

Há que se falar, ainda, na possibilidade de cruzamento de dados, que podem propiciar informações ainda mais valiosas tendo como base dados que inicialmente parecem ser sem valor.

⁶⁸ SILVEIRA, S. A. da. **Tudo sobre Tod@s**: Redes Digitais, Privacidade e Venda de Dados Pessoais. São Paulo: Edições Sesc São Paulo, 2017. p. 22.

Considerando que (i) é impossível que não sejam mais utilizados algoritmos nem dados pessoais, já que se está na sociedade da informação; (ii) existem diversos malefícios quando a utilização de dados ultrapassa os limites para os quais foram concedidos, inclusive com ameaça de violação a direitos e garantias fundamentais; (iii) muitas informações são tanto do interesse público quanto de entes privados, podendo trazer, ao mesmo tempo, benefícios à sociedade em geral e aos indivíduos detentores de tais informações; e (iv) a utilização e manipulação de dados por algoritmos propiciam a inovação, fica evidente que o maior desafio relacionado à utilização de algoritmos e coleta, armazenamento e tratamento de dados pessoais gira em torno do equilíbrio entre esses quatro pontos, que por vezes são concorrentes entre si.

Nesse aspecto, a existência de um procedimento de governança algorítmica que propicie esse equilíbrio aparece como uma solução viável, desde que os diferentes pontos de vista e interesses sejam considerados para tal governança. O ideal é que exista um caráter interdisciplinar, envolvendo aspectos jurídicos, regulatórios, técnicos e comportamentais. A priorização dos mais variados aspectos envolvidos deveria considerar a transparência, as garantias técnicas relacionadas tanto aos algoritmos propriamente ditos quanto às formas de coleta, armazenamento e tratamento de dados e, por fim, a responsabilidade no caso de ilegalidades cometidas com base em decisões de algoritmos, com base em critérios objetivos.⁶⁹

Ademais, considerando que o uso de algoritmos como ferramentas pressupõe a criação de perfis (*profiles*) por meio de tendências encontradas, a qual poderia ser feita de maneira automatizada ou não, bem como a questão referente à ordem de operações a serem realizadas, a governança algorítmica deverá levar em consideração as diferentes posições sociais ocupadas pelos indivíduos. Do contrário, vieses serão automaticamente criados e, como consequência, haverá uma reprodução em maior escala das discriminações sociais.

⁶⁹ EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 4/2015**. Towards a new digital ethics: Data, Dignity and Technology. Brussels, 11 Sept. 2015. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf>. Acesso em: 15 dez. 2017.

Por um lado, é necessário o fortalecimento de cada cidadão no sentido de que ele tenha o conhecimento necessário para entender e decidir sobre a utilização de seus próprios dados⁷⁰, a fim de capacitá-lo para dar o consentimento inequívoco sobre o uso de seus dados pessoais, ao contrário do mero consentimento formal existente hoje. Deve ser levado em conta, ainda, que tal consentimento diz respeito diretamente às pessoas e não às coisas, elevando, portanto, o caráter de relevância do mesmo. Dessa forma, seria propiciado o controle sobre os dados pessoais para os indivíduos.

Por outro lado, a governança de algoritmos também aparece como estratégia fundamental, atuando como uma forma de agência sobre algoritmos, plataformas digitais e sobre o conjunto de dados utilizados como base pelos algoritmos. A abordagem da governança é, em suma, a utilização de processos claros, que tenham como foco a minimização dos riscos envolvendo o uso de algoritmos, com respeito às garantias fundamentais, tendo, ao mesmo tempo, a extração do maior benefício possível, considerando o equilíbrio de interesses entre todas as partes envolvidas.

Em suma, o que teríamos é a proteção do cidadão com a proteção aos seus dados pessoais, ao mesmo tempo em que seria propiciado às empresas que manipulam dados uma segurança jurídica não existente hoje no Brasil, uma vez que carente de legislação específica, com decisões baseadas em diferentes interpretações e analogias dos dispositivos vigentes.

Por fim, a estratégia de governança algorítmica na proteção de dados pessoais é apolítica, com foco no interesse da sociedade em geral e todos os entes que a compõem, considerando, ainda, as tecnologias digitais como catalisadoras do desenvolvimento econômico e social de um país e elementos fundamentais para competitividade e inovação.

⁷⁰ MANCINI, P.; VIS, F. **How do digital platforms shape our lives?** In: World Economic Forum, Oct 2015. Disponível em: <https://www.weforum.org/agenda/2015/10/how-do-digital-platforms-shape-our-lives/?utm_content=buffer09d73&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer>. Acesso em: 15 dez. 2017.

6 DA NECESSIDADE DE LEGISLAÇÃO ESPECÍFICA DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

De acordo com o contexto apresentado por meio do presente trabalho, fica evidente a necessidade de legislação específica acerca de proteção de dados no Brasil, de maneira a contribuir no aspecto regulatório com a governança algorítmica.

É imenso o tamanho do desafio para a viabilização de uma governança algorítmica eficiente, que considere todos os pontos relevantes que tangem a questão, sobretudo sem a existência de um conflito de interesse. Por um lado, poderíamos ter soluções mais orientadas ao mercado que, ao visarem lucro, adotariam procedimentos de governança de algoritmos que não considerasse tão profundamente os aspectos de real consentimento – e não apenas formal. Por outro, também não é praticável a governança de algoritmos que, em um sentido estritamente protecionista, inviabilize o uso de algoritmos como um todo, importando, portanto, em barreiras às inovações tecnológicas.

Uma legislação acerca da proteção de dados pessoais, cujos termos fossem temperados com as variáveis apresentadas no presente trabalho e envolvidas no processo de governança algorítmica, aparece como uma solução viável no meio termo entre uso indiscriminado de dados pessoais e uma barreira total a processos de inovação tecnológica, importando, portanto, no uso da tecnologia de uma maneira benéfica em geral a partir de algoritmos.

Em que pese a legislação vigente tangencie a questão em alguma medida, ela não é suficiente para direcionar decisões e cobrir integralmente lacunas deixadas acerca do tema.

Conforme Doneda⁷¹, no ordenamento brasileiro,

[...] o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

⁷¹ DONEDA, 2014, p. 65.

Assim, passa-se para a análise do contexto jurídico brasileiro.

6.1 DOS DISPOSITIVOS JÁ EXISTENTES

Ora, pois, que se a Constituição Federal do Brasil traz, em seu artigo 5º, X⁷², a garantia de inviolabilidade da vida privada e da intimidade, ainda que de uma maneira indireta, temos a privacidade como um direito fundamental expresso constitucionalmente e, como consequência, a proteção de dados pessoais.

Ademais, outro instrumento nesse sentido é o *Habeas Data*, remédio constitucional que tem como objetivo proteger os cidadãos em sua esfera íntima contra: (i) conservação de dados não verdadeiros ou com finalidades diferentes daquelas autorizadas em lei; (ii) utilização de bancos de dados coletados por meios ilegais, fraudulentos ou ilícitos; e (iii) armazenamento referente a dados sensíveis, tais quais opiniões políticas, orientação sexual, religião, dentre outros⁷³. O *Habeas Data* será concedido:

- a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou bancos de dados de entidade governamentais ou de caráter público;
- b) para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.⁷⁴

Salienta-se, entretanto, que na prática o desafio de impetrar *Habeas Data* resume-se em saber exatamente quem detém os dados pessoais e com quais finalidades. Além disso, sobre quais dados são utilizados, de que forma e para qual motivação. Por consequência, a partir do momento em que não é possível a identificação exata acerca de quem detém tais dados, sequer será possível a impetração do remédio constitucional supracitado, tornando-o, portanto, ineficiente na proteção de dados pessoais.

Um avanço na questão de proteção de dados pessoais no ordenamento brasileiro é o constante no Código de Defesa do Consumidor, que institui em seu

⁷² BRASIL, 1988, art. 5º, X.

⁷³ SILVA, J. A. **Curso de Direito Constitucional Positivo**. 31. ed., rev. e atualizada até Emenda Constitucional nº 56, de 20 de dezembro de 2007. São Paulo: Malheiros, 2008. p. 453.

⁷⁴ BRASIL, 1988, art. 5º, LXXII.

artigo 43 limites à coleta, armazenamento e tratamento de dados pessoais nas relações consumeiristas⁷⁵, a fim de combater a potencial abusividade do fornecedor frente ao consumidor, dado o desequilíbrio de forças entre as partes.

Por fim, o princípio de proteção da privacidade e dos dados pessoais, constante no Marco Civil da Internet⁷⁶, o qual regulamenta o uso da internet no Brasil, também corrobora com o direito à privacidade como direito fundamental. Entretanto, na falta de maiores detalhes da execução de tais princípios, novamente se está diante de um desafio prático de aplicação, a exemplo do que ocorre com o *Habeas Data*.

6.2 DOS PROJETOS DE LEI EM TRAMITAÇÃO

Ainda que a existência de uma legislação específica já aprovada acerca da proteção de dados pessoais não seja realidade hoje no Brasil, existem dois projetos de lei em tramitação no Congresso Nacional que merecem uma atenção especial no presente trabalho, para fins de entendimento de onde o Brasil se encontra hoje na evolução de legislações sobre o tema, apesar da sua análise minuciosa não ser objeto do presente: o PL 4060/12 e o PL 5276/16.

No que tange ao PL 4060/12, a crítica primordial – e, portanto, com efeitos no projeto de lei como um todo - que se tece é sobre a definição de dado pessoal. O projeto de lei entende como dado pessoal, em seu artigo 7º, I, “qualquer informação que permita a identificação exata e precisa de uma pessoa determinada”⁷⁷.

Entretanto, tal definição deixa margem para contornos da legislação que inicialmente tem como finalidade a proteção de dados pessoais, uma vez que em um

⁷⁵ BRASIL. **Lei nº 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set.1990. Edição extra. art. 43. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 17 dez. 2017.

⁷⁶ BRASIL, 2014.

⁷⁷ BRASIL. Congresso Nacional. Câmara dos Deputados. **Projeto de Lei nº 4067**, de 2012. Acrescenta parágrafo ao art. 32 da Lei nº 9.394, de 20 de dezembro de 1996, de diretrizes e bases da educação nacional, dispondo sobre a idade da criança para ingresso no primeiro ano do ensino fundamental. Autor: Romero Rodrigues. Apresentação: 14 jun. 2012. art. 7º. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012>. Acesso em: 17 dez. 2017.

contexto em que dados pessoais identificados, de maneira precisa e exata, poderiam ser manipulados para se tornarem apenas identificáveis e não recebendo, portanto, nenhum tipo de proteção, uma vez que não considerado como dado pessoal por definição.

Dentre outras críticas que podem ser feitas a tal projeto, o qual demonstra ter um menor grau de aderência a princípios gerais de proteção de dados pessoais, que são amplamente utilizados no contexto internacional, merecem destaque: (i) a ausência de menção a consentimento e graus de consentimento, limitando-se a dizer que os dados pessoais serão tratados com lealdade e boa-fé, com foco no legítimo interesse das partes; e (ii) a permissão de compartilhamento de dados pessoais com terceiros, desde que esses participem de alguma forma do tratamento de dados, o que acaba por permitir, ainda que indiretamente, a ampla circulação de dados pessoais.⁷⁸

De toda forma, o PL 4060/12 mostra-se muito mais focado no tratamento dos dados e na forma com que poderá ser realizado, do que na proteção dos dados pessoais propriamente dita, deixando, ainda, importantes lacunas para a referida proteção, tendo como consequência o mantimento da vulnerabilidade do cidadão, ainda que diante de uma legislação específica.

Por outro lado, o PL 5276/16 mostra-se muito mais adequado no sentido da proteção dos dados pessoais, sem inviabilizar o uso da tecnologia e suas inovações. Não poderia ser diferente, uma vez que a criação de tal projeto é fruto de grandes debates da sociedade⁷⁹ como um todo, em caráter interdisciplinar, como o tema em questão exige.

⁷⁸ ARTIGO 19 BRASIL. **Proteção de dados pessoais no Brasil** - Análise dos projetos de lei em tramitação no Congresso Nacional. São Paulo, nov. 2016. p. 42. Disponível em:

<<http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>>. Acesso em: 19 dez. 2017.

⁷⁹ Por iniciativa do Ministério da Justiça e Cidadania, foram realizadas duas consultas públicas com o texto do então anteprojeto de lei, uma no ano de 2011, através da plataforma online disponível em <<http://culturadigital.br/dadospessoais/>> e outra no ano de 2015, através da plataforma online disponível em <<http://pensando.mj.gov.br/dadospessoais/>>. As contribuições se deram tanto pelo setor empresarial, quanto pelo setor acadêmico e por instituições da sociedade civil, além dos próprios cidadãos. Ademais, após a versão ser final ser enviada para aprovação, diversos coletivos relacionados à proteção de dados pessoais demonstraram apoio à aprovação do PL 5276/16, a exemplo do Intervezes, por meio da Carta Aberta disponível em <<http://intervezes.org.br/wp-content/uploads/2016/06/Carta-Aberta.-PL-Dados-Pessoais.02.06.2016.pdf>>, e do Coalizão

O primeiro de destaque, que possui reflexos em toda questão de proteção de dados pessoais, é da definição de dado pessoal como “dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa”⁸⁰. Ademais, as divisões de tipos de dados vão além de dados pessoais, havendo a menção e definição de dados sensíveis e dados anonimizados.

Pode-se citar, ainda, enquanto pontos positivos, em contraponto aos negativos constantes no PL 4060/12: (i) a presença de graus de consentimento, informando que o processo poderá ser realizado apenas mediante consentimento livre, inequívoco e informado e detalhando, ainda, informações necessárias para os detentores de dados no que tange o tratamento; e (ii) a necessidade de consentimento expresso do titular para o compartilhamento de dados pessoais com terceiros, impedindo, nos termos da lei e exceções previstas por meio de políticas públicas, a ampla possibilidade de compartilhamento de dados pessoais.⁸¹

De forma inovadora na embrionária legislação brasileira de proteção de dados pessoais, o PL 5276 prevê, ainda, a designação (e não criação) de um órgão regulatório, com a finalidade de fiscalizar e zelar pela implementação da lei⁸².

Ainda que não se trate de um órgão completamente independente, se for feito da maneira como adicionado pelo texto do projeto de lei, a especialização de um órgão com funções primordiais relacionadas à fiscalização e zelo da lei de proteção de dados pessoais aparece como um avanço importante. Deve-se considerar que um dos desafios de hoje, além das lacunas causadas pela ausência de legislação específica, é a falta de especialidade e até mesmo de conhecimento do assunto dos órgãos públicos, tanto fiscalizatórios quanto do próprio judiciário, a fim fazer valer

Direitos na Rede, considerando fundamental a aprovação do projeto, disponível em <https://direitosnarede.org.br/seus_dados_s%C3%A3o_voc%C3%AA/2017/01/27/por-que-a-aprovacao-do-pl5276-16-e-fundamental-para-o-brasil.html>.

⁸⁰ BRASIL. Congresso Nacional. Câmara dos Deputados. Projeto de Lei nº 5276, de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Autor: Poder Executivo. Apresentação: 13 maio 2016. art. 5º, I. Disponível em:

<http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016>. Acesso em: 16 dez. 2017.

⁸¹ ARTIGO 19 BRASIL, 2016, p. 27-28.

⁸² ARTIGO 19 BRASIL, 2016, p. 29.

garantias fundamentais como a privacidade e, por consequência, a proteção de dados pessoais.

Embora críticas do ponto de vista da proteção de dados pessoais possam ser tecidas tanto ao PL 4060/12 quanto ao PL 5276/16, tem-se que o que chega mais próximo da garantia de proteção em equilíbrio com o desenvolvimento tecnológico, assegurando igualmente a inovação, é o segundo, estando, inclusive mais próximo das legislações presentes no contexto internacional.

6.3 BREVE CONTEXTO INTERNACIONAL

O Brasil é um dos poucos países do mundo que ainda não possui legislação específica de proteção de dados pessoais. Considerando que se está diante da sociedade da informação, em que a economia baseada em dados é iminente, o país acaba por, além da violação ao direito fundamental de privacidade, perder competitividade no cenário internacional.

Há que se considerar, ainda, que no que tange a proteção de dados pessoais, é necessário que o poder estatal possua uma conduta positiva, no sentido de prevenção de violações, a partir do seu dever de tutela de segurança dos cidadãos.

Além disso, imperioso reconhecer que com o advento da tecnologia as barreiras físicas entre países adquirem uma nova conotação, de maneira que para o compartilhamento de dados ou informações são praticamente irrelevantes do ponto de vista técnico.

Nesse contexto, a título de exemplificação, importante citar o *General Data Protection Regulation*⁸³, sistema de regulação de dados na União Europeia, com aplicação integral a todos países que compõem o bloco econômico, além da previsão de que países que se relacionam economicamente, isso quer dizer, fazem negócios com algum componente da União Europeia também devem seguir as mesmas regras.

⁸³ INTERSOFT CONSULTING SERVICES AG. **General Data Protection Regulation**. Hamburg, 27 abr. 2016. Disponível em: <<https://gdpr-info.eu/>>. Acesso em: 22 dez. 2017.

Além disso, o *General Data Protection Regulation* foi recentemente atualizado depois de uma série de debates, trazendo alterações que passarão a valer a partir de maio de 2018, tais quais a inclusão do direito ao acesso e a incorporação de *Privacy by Design*⁸⁴ como um requerimento legal de adequação às normas.⁸⁵

Ainda que exista essa regulação geral para todos os países da União Europeia, não raro se vê legislação nacional à respeito da proteção de dados pessoais, as quais, por sua vez, também devem obedecer a regulação geral.

Cita-se o exemplo da Alemanha, com o *German Data Protection Act*⁸⁶ que foi igualmente atualizado a partir das novidades trazidas pelo *General Data Protection*. Nesse sentido, a legislação específica alemã traz, dentre outros dispositivos, o propósito de proteção à privacidade dos indivíduos, com aplicação tanto a entes públicos quanto a entes privados.

Em um exemplo com a realidade econômica e social um pouco mais próxima da do Brasil, podemos citar o Chile, com a *Ley de Proteccion de Datos de Caracter Persona*⁸⁷, válida no país desde o ano de 1999.

Os exemplos trazidos no presente não têm o objetivo de esgotar todas as legislações específicas sobre a proteção de dados pessoais existente no mundo, mas apenas demonstrar que diferentes países vêm discutindo sobre a tutela de dados pessoais há muito tempo, inclusive já atualizando seus dispositivos, ao passo que no Brasil sequer se tem projetos de lei aprovados.

⁸⁴ *Privacy by Design* é uma abordagem de sistema de engenharia que considera a privacidade de maneira integral no processo. Além disso, trata-se de uma cultura que parte do princípio da privacidade. (PRIVACY by design. In: Wikipédia, a enciclopédia livre, 2017. Disponível em: <https://en.wikipedia.org/wiki/Privacy_by_design>. Acesso em: 22 dez. 2017.)

⁸⁵ AN OVERVIEW of the main changes under GDPR and how they differ from the previous directive. In: **EU GDPR Portal**. GDPR Key Changes. [2016?]. Disponível em: <<https://www.eugdpr.org/key-changes.html>>. Acesso em: 22 dez. 2017.

⁸⁶ GERMANY. German Bundestag. **Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs-und-Umsetzungsgesetz-EU-DSAnpUG-EU)**, Vom 30. Juli 2017. In: Bundesanzeiger Verlag, Bonn, n. 44, p. 2097-2132, 5. Juli 2017. Disponível em: <https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1514295967197>. Acesso em: 23 dez. 2017.

⁸⁷ CHILE. Congreso Nacional. Biblioteca del Congreso Nacional de Chile. **Ley nº 19.628**, de 28 agosto de 1999. Proteccion de Datos de Caracter Personal. Santiago, 6 agosto 1999. Disponível em: <<https://www.leychile.cl/Navegar?idNorma=141599&idVersion=1999-08-28>>. Acesso em: 23 dez. 2017.

6.4 CONSIDERAÇÕES ACERCA DA LEGISLAÇÃO DE PROTEÇÃO DE DADOS PESSOAIS VIÁVEL PARA O BRASIL

Ainda que presente o contexto internacional e que os primeiros passos com foco em uma legislação específica de proteção de dados no Brasil venham sendo dados, há que se reconhecer (i) que a experiência internacional, ainda que muito válida a título de aprendizado, não seria eficaz se simplesmente transposta para o Brasil, dadas as suas peculiaridades; e (ii) que o projeto de lei 5276/16 apresenta-se como uma boa alternativa para início de uma regulação para a proteção de dados pessoais, entretanto, pontos importantes não são priorizados no texto do projeto de lei.

Ademais, acerca da importância das informações e seu risco potencial:

A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo desse registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei.⁸⁸

Nesse sentido, parte-se para uma reflexão: o que seria uma boa legislação de proteção de dados para o Brasil, com foco na proteção de dados, mas sem barrar a inovação tecnológica e as maravilhas advindas dela?

No contexto de algoritmos como uma das principais formas de ameaça à proteção de dados pessoais, o foco deve ser, portanto, a criação de uma lei de proteção de dados que, considerando a ampla utilização de algoritmos e seus inúmeros benefícios, possa, ao mesmo tempo em que propicia tal uso e a inovação tecnológica como um todo, contornar ou prevenir os potenciais problemas criados a partir do uso de algoritmos. Nesse caso, teríamos uma espécie de direcionamento

⁸⁸ UNITED STATES. U.S. Department of Health and Human Services. **Records, Computers and the Rights of Citizens**. Washington, D.C., 7 jan. 1973. Disponível em: <<https://aspe.hhs.gov/report/records-computers-and-rights-citizens>>. Acesso em: 18 dez. 2017.

geral à governança algorítmica, que seria suficientemente amplo a ponto de não deixar lacunas que se tornem possibilidades de contorno da legislação, sem ser, ao mesmo tempo, extremamente fechada, a ponto de impossibilitar de alguma forma a utilização de algoritmos como um todo.

Em suma, o que se quer é a criação de uma legislação de proteção de dados pessoais que contorne ou previna os problemas causados pelos algoritmos. Fica fácil perceber, portanto, que tal regulação se trata, na verdade, de um instrumento de política pública, e não de mera regulação.

Passa-se a traçar, então, elementos essenciais que deveriam ser levados em consideração quando da proposição de qualquer texto de lei envolvendo a proteção de dados pessoais no contexto brasileiro, com as diferentes variáveis envolvidas, incluindo os algoritmos. Salienta-se que não se trata de um rol exaustivo de proteção de dados pessoais, mas sim de priorizações para a criação de uma legislação.

6.4.1 Abrangência integral de setores

Com o objetivo de que os cidadãos tenham uma proteção integral e harmônica, é primordial que a abrangência de validade de eventual legislação de proteção de dados englobe todos os setores, sejam eles privados, públicos ou em parcerias entre os dois. Não é possível se falar parcialmente em proteção de dados, uma vez que, nesse caso, estaríamos omitindo o dever de tutela integral do Estado de uma garantia fundamental.

6.4.2 Conceito de dado pessoal

Ao contrário do que estabelece o PL 4060/12, a definição de dado pessoal constante na legislação deve ser abrangente e não restrita, no mesmo sentido da que já consta no PL 5276/16, ou seja, dado pessoal como aquele referente a uma pessoa identificada ou identificável. Essa definição visa evitar contornos sobre a legislação de proteção aos dados pessoais, diante da eventual possibilidade de que

seja transformado um dado pessoal identificado em apenas identificável – causando, portanto, o mesmo resultado pelo uso, apenas para que não exista o amparo legal de proteção.

Ademais, outras categorias de dados para proteção também devem ser consideradas, a exemplo de dados sensíveis e anonimizados.

6.4.3 Relação com outros sistemas de proteção

A legislação deve considerar, ainda, a existência de outros sistemas de proteção de dados pessoais ao redor do mundo. A existência de tais sistemas não deve servir como barreiras à criação da legislação própria, entretanto, considerando as relações econômicas e negociais que o Brasil estabelece com outros países, a legislação local não pode servir como impeditivo de tais relações, sob o risco de limitar consideravelmente a economia local.

O que se quer dizer, em suma, é que é necessário que a legislação brasileira de dados pessoais converse com outros sistemas de proteção de dados pessoais, a fim de não impedir relações internacionais pelo tráfego de informações e a sua consequente proteção.

6.4.4 Mecanismo de proteção voltado exclusivamente à pessoa natural

Uma discussão recorrente no que tange à proteção de dados pessoais é se dados pessoais deveriam englobar apenas pessoas naturais ou se diriam respeito tanto a pessoas naturais quanto a pessoas jurídicas. A defesa que se faz é que a proteção decorrente dessa legislação de proteção de dados pessoais é decorrente do direito fundamental de privacidade, devendo ser aplicável, portanto, apenas a pessoas naturais.

Outrossim, há que se considerar que para a proteção de pessoas jurídicas em um contexto similar ao da proteção de dados pessoais, já existem outros meios, tais

quais a Lei de Propriedade Industrial⁸⁹ e a proteção ao sigilo comercial, industrial e financeiro⁹⁰.

6.4.5 Consentimento

O consentimento dado para o uso de dados pessoais deve ser expresso, inequívoco, livre e informado. Para tal, é necessário um investimento, inicialmente, na capacitação dos indivíduos para entendimento do que será feito com seus dados, a fim de evitar um mero consentimento formal. Isso requer, ainda, transparência por parte de quem vai fazer a coleta, armazenamento e tratamento dos dados pessoais, com relação ao ciclo de vida do dado de uma maneira integral.

Defende-se, ainda, a existência de graus de consentimento – que não apenas a concordância integral com os termos propostos ao usuário. Os benefícios poderiam variar de acordo com o grau de consentimento fornecida, mas isso evitaria o aceite integral por mera necessidade de acesso à determinada plataforma.

6.4.6 Legítimo interesse

Para a possibilidade de acesso aos dados pessoais, é necessário a existência de legítimo interesse para tal. Isto é, não será permitida a ampla circulação de dados pessoais, a menos que exista o legítimo interesse da parte envolvida ou autorização expressa de lei para tal. Entretanto, ressalta-se que o entendimento de legítimo interesse não se trata de uma norma aberta, a fim de evitar eventuais contornos e o próprio esvaziamento da norma.

⁸⁹ BRASIL. **Lei nº 9.279**, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Diário Oficial da União, Brasília, DF, 15 maio 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9279.htm>. Acesso em: 18 dez. 2017.

⁹⁰ *In verbis*: “É assegurado o sigilo comercial, industrial, financeiro ou qualquer outro sigilo protegido por lei, bem como o relativo às comunicações internas dos órgãos e entidades governamentais” (BRASIL. **Lei nº 10.650**, de 16 de abril de 2003. Dispõe sobre o acesso público aos dados e informações existentes nos órgãos e entidades integrantes do Sisnama. Diário Oficial da União, Brasília, DF, 17 abr. 2003. art. 2º, VIII, § 2º. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.650.htm>. Acesso em: 24 dez. 2017.)

Legítimo interesse deve ser relacionado a uma finalidade específica, previamente entendida e consentida pelo detentor dos dados, tendo como base, ainda, a ponderação. A título de exemplificação, cita-se que questões de *marketing* não devem servir de justificativa para o acesso de dados por meio do legítimo interesse, a menos que consentido, nos termos do subcapítulo anterior, pelo detentor dos direitos.

6.4.7 Autoridade de fiscalização do cumprimento da legislação

Entende-se, por fim, que a legislação de proteção de dados deve servir como conduta ativa do Estado com foco de evitar violações de dados pessoais, mas é importante que a mesma tenha a previsão de criação de uma autoridade com autonomia administrativa, normativa e financeira, com foco na fiscalização do cumprimento da legislação, bem como pelo zelo aos seus direcionamentos.

Nesse sentido, tal órgão deveria ter, ainda, a possibilidade – e por possibilidade entende-se, ainda, a viabilidade técnica e financeira, além da previsão legal de autorização para atuação – de auditabilidade de algoritmos nas diferentes instituições.

Isto posto, seria possível a conexão direta entre a legislação de proteção de dados pessoais à uma atuação centrada na governança algorítmica, com foco não só na proteção de dados pessoais, mas também favorável à inovação tecnológica, sem deixar de lado os benefícios decorrentes de se viver na sociedade da informação.

7 CONCLUSÃO

O desenvolvimento tecnológico, sobretudo no que diz respeito à utilização de algoritmos como parte essencial de novos processos econômicos e sociais, possibilitou a captação, armazenamento e manipulação de dados pessoais a um baixo custo e em velocidade e eficiência muito além do que é possível por padrões humanos.

Os cidadãos, a partir da democratização da tecnologia, especialmente com o amplo acesso à internet, por um lado, obtiveram uma infinidade de novas possibilidades e, por outro, encontram-se em estado de ameaça à tutela de direitos e garantias fundamentais, a exemplo do direito à privacidade, desdobrado em direito à proteção de dados pessoais.

Sendo os algoritmos os principais responsáveis pelas possibilidades de uso de dados pessoais, os resultados de sua ampla utilização culminam no desafio de propiciar o desenvolvimento tecnológico e as maravilhas advindas dele, ao mesmo tempo em que se confere proteção aos dados pessoais.

A governança algorítmica aparece, então, como alternativa viável na finalidade de equilíbrio de interesses no uso de algoritmos com foco na proteção de dados pessoais, a partir da consideração de pontos interdisciplinares para a governança geral sobre o uso de algoritmos, tais quais jurídicos, técnicos e regulatórios. É necessário considerar, portanto, que eventuais conflitos de interesses na esfera da governança algorítmica, sejam na sua criação ou na sua aplicação prática, devem ser analisados sob uma perspectiva geral, inclusive tendo como base princípios gerais e viabilidade técnica.

Como se percebeu neste trabalho, diante da inexistência de legislação específica para proteção de dados pessoais no Brasil e a partir do estudo do contexto internacional de regulação sobre o tema, a necessidade de criação dessa legislação é emergente, tanto como forma de tutela a garantias fundamentais quanto como elemento de competitividade no mercado internacional, a partir de delimitações claras acerca do seu uso. A proteção de dados pessoais apresenta-se

como necessária não apenas como mera regulação, mas sim como ferramenta de política pública.

A partir da atual legislação acerca do tema, em dispositivos dispersos e com aplicação de analogias, não conferindo, portanto, a tutela necessária para a efetiva proteção de dados pessoais enquanto direito fundamental, buscou-se a priorização de itens que deveriam ser levados em consideração quando da criação da legislação de proteção de dados pessoais no Brasil. Tal legislação servirá, ainda, como um direcionamento geral para a criação e aplicação da governança algorítmica, evitando que a eficiência do método de governança algorítmica seja comprometida por eventuais conflitos de interesse sem subsídio legal específico de orientação.

Diante da realidade brasileira, do contexto legal internacional, dos dispositivos já existentes e dos projetos de lei em tramitação no país, devem ser priorizados quando da elaboração de uma lei sobre proteção de dados pessoais: (i) a necessidade de abrangência integral de setores; (ii) o conceito de dado pessoal amplo; (iii) a relação com outros sistemas de proteção, a fim de possibilitar que ambos os sistemas se comuniquem; (iv) que seja mecanismo de proteção aplicável exclusivamente à pessoa natural; (v) a necessidade de real consentimento, e não apenas como mera formalidade; (vi) a necessidade de legítimo interesse, a fim de evitar contornos da legislação baseado no interesse das partes; e, por fim, (vii) a criação de uma autoridade independente de fiscalização do cumprimento da legislação, com a possibilidade de auditoria sobre os dados e seus mecanismos de captação, armazenamento e manipulação.

REFERÊNCIAS BIBLIOGRÁFICAS

AN OVERVIEW of the main changes under GDPR and how they differ from the previous directive. In: **EU GDPR Portal**. GDPR Key Changes. [2016?]. Disponível em: <<https://www.eugdpr.org/key-changes.html>>. Acesso em: 22 dez. 2017.

ARTIGO 19 BRASIL. **Proteção de dados pessoais no Brasil** - Análise dos projetos de lei em tramitação no Congresso Nacional. São Paulo, nov. 2016. Disponível em: <<http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>>. Acesso em: 19 dez. 2017.

BAUMAN, Z. **Danos Colaterais**: desigualdades sociais numa era global. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BAUMAN, Z.; DONSKIS, L. **Cegueira moral**: a perda da sensibilidade na modernidade líquida. Tradução de Carlos Alberto Medeiros. 1. ed. Rio de Janeiro: Zahar, 2014.

BAUMAN, Z. **Modernidade líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

BEVILAQUA, C. **Theoria geral do direito civil**. 4. ed. atualizada por Achilles Bevilaqua. Rio de Janeiro: Francisco Alves, 1949.

BRASIL. Congresso Nacional. Câmara dos Deputados. **Projeto de Lei nº 4067**, de 2012. Acrescenta parágrafo ao art. 32 da Lei nº 9.394, de 20 de dezembro de 1996, de diretrizes e bases da educação nacional, dispondo sobre a idade da criança para ingresso no primeiro ano do ensino fundamental. Autor: Romero Rodrigues. Apresentação: 14 jun. 2012. art. 7º. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012>. Acesso em: 17 dez. 2017.

BRASIL. Congresso Nacional. Câmara dos Deputados. Projeto de Lei nº 5276, de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Autor: Poder Executivo. Apresentação: 13 maio 2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016>. Acesso em: 16 dez. 2017.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 nov. 2017

BRASIL. **Decreto nº 8.771**, de 11 de maio de 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Diário Oficial da União, Brasília, DF, 11 maio 2016. Edição extra. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm>. Acesso em: 2 dez. 2017.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Caderno de Investigações Científicas. Brasília: Secretaria de Direito Econômico/Departamento de Defesa e Proteção do Consumidor, v. 2, cap. 1. 2010. Disponível em: <<http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>>. Acesso em: 2 dez. 2017.

BRASIL. **Lei nº 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Edição extra. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 17 dez. 2017.

BRASIL. **Lei nº 9.279**, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Diário Oficial da União, Brasília, DF, 15 maio 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9279.htm>. Acesso em: 18 dez. 2017.

BRASIL. **Lei nº 10.650**, de 16 de abril de 2003. Dispõe sobre o acesso público aos dados e informações existentes nos órgãos e entidades integrantes do Sisnama. Diário Oficial da União, Brasília, DF, 17 abr. 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.650.htm>. Acesso em: 24 dez. 2017.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 21 nov. 2017.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Poder Executivo, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 9 dez. 2017.

BRASIL. Ministério das Relações Exteriores. **Brasil e Alemanha apresentam à ONU projeto de resolução sobre o direito à privacidade na era digital**. Brasília, 2013. Disponível em: <<http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/3424-brasil-e-alemanha-apresentam-a-onu-projeto-de-resolucao-sobre-o-direito-a-privacidade-na-era-digital>>. Acesso em: 6 dez. 2017.

BRASIL. Superior Tribunal De Justiça. Terceira Turma. **Recurso Especial Representativo de Controvérsia nº 1419697**. Recorrente: Boa Vista Serviços S/A. Recorrido: Anderson Guilherme Prado Soares. Relator: Ministro Paulo de Tarso Sanseverino. Brasília, 12 de novembro de 2014. Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/152068666/recurso-especial-resp-1419697-rs-2013-0386285-0>>. Acesso em: 13 dez. 2017.

BUTTERFIELD, A.; NGONDI, G. E. **A Dictionary of Computer Science**. 7. ed. New York: Oxford University Press, 2016.

CATALA, Pierre. Ebauche d'une théorie juridique de l'information. **Informatica e Diritto**, [Paris], ano IX, n. 1, p. 15-31, jan. 1983. p. 20. Disponível em: <http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf>. Acesso em: 3 dez. 2017.

CHILE. Congreso Nacional. Biblioteca del Congreso Nacional de Chile. **Ley nº 19.628**, de 28 agosto de 1999. Protección de Datos de Caracter Personal. Santiago, 6 agosto 1999. Disponível em: <<https://www.leychile.cl/Navegar?idNorma=141599&idVersion=1999-08-28>>. Acesso em: 23 dez. 2017.

CUEVA, R. V. B. **A insuficiente proteção de dados pessoais no Brasil**. Justiça & cidadania, Rio de Janeiro, v. 18, n. 195, p. 8-13, nov. 2016.

CURITIBA. Agência de Notícias da Prefeitura de Curitiba. **Idosos podem usar cartão de isento para aumentar tempo de travessia**. Curitiba, 6 mar. 2017. Disponível em: <<http://www.curitiba.pr.gov.br/noticias/idosos-podem-usar-cartao-de-isento-para-aumentar-tempo-de-travessia/41404>>. Acesso em: 15 dez. 2017.

D'ACQUISTO, G. et al. **Privacy by design in big data**: An overview of privacy enhancing technologies in the era of big data analytics. [S. l.]: European Union Agency for Network and Information Security, Dec. 2015. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport>. Acesso em: 7 dez. 2017.

DATA SCIENCE BRIGADE. **Operação Serenata de Amor**. [S. l.]: [2016?]. Disponível em: <<https://serenatadeamor.org/>>. Acesso em: 26 nov. 2017.

DOMINGOS, P. **The Master Algorithm**: How the Quest for the Ultimate Learning Will Remake Our World. Journal of Computer Science and Technology, New York, 2015, v. 15, p.157-158.

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

DONEDA, D. O Direito Fundamental à Proteção de Dados Pessoais. In: MARTINS, G. M. (Coord.) et al. **Direito Privado & Internet**. São Paulo: Atlas, 2014. cap. 3.

DRUCKER, P. F. **Inovação e Espírito Empreendedor: Práticas e Princípios**. 1ª ed. São Paulo: Pioneira Thomson, 2002.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 4/2015**. Towards a new digital ethics: Data, Dignity and Technology. Brussels, 11 Sept. 2015. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf>. Acesso em: 15 dez. 2017.

GERMAN. German Bundestag. **Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs-und-Umsetzungsgesetz-EU-DSAnpUG-EU)**, Vom 30. Juli 2017. In: Bundesanzeiger Verlag, Bonn, n. 44, p. 2097-2132, 5. Juli 2017. Disponível em: <https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1514295967197>. Acesso em: 23 dez. 2017.

GILLESPIE, T. **The Relevance of Algorithms**. Cambridge: MIT Press, 2014.

GOULART, G. D. **O impacto das novas tecnologias nos direitos humanos e fundamentais: o acesso à internet e a liberdade de expressão**. Revista Direitos Emergentes na Sociedade Global, vinculada ao Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria, [Santa Maria], v. 1, n. 1, p. 145-168. jan./jun. 2012. ISSN 2316-3054. Disponível em: <<https://periodicos.ufsm.br/REDESG/article/view/5955#.WVIKR-vyvio>>. Acesso em: 12 dez. 2017.

GOULART, G. D. **Por uma visão renovada dos arquivos de consumo**. Revista de Direito do Consumidor, [S. l.], v. 107/2016, p. 447-482, set./out. 2016.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. Acesso à Internet e à Televisão e Posse de Telefone Móvel Celular para Uso Pessoal. In: _____. **Pesquisa Nacional por Amostra de Domicílios**. [Rio de Janeiro]: IBGE, 2008, 2011, 2013, 2014, 2015. Suplementos. Disponível em: <http://www.ibge.gov.br/home/xml/suplemento_pnad.shtm>. Acesso em: 8 dez. 2017.

INTERNET das coisas. In: **Wikipédia**, a enciclopédia livre, 2017. Disponível em: <https://pt.wikipedia.org/wiki/Internet_das_coisas>. Acesso em: 13 dez. 2017.

INTERSOFT CONSULTING SERVICES AG. **General Data Protection Regulation**. Hamburg, 27 abr. 2016. Disponível em: <<https://gdpr-info.eu/>>. Acesso em: 22 dez. 2017.

LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. p.29.

LIMBERGER, T. **Cibertransparência**: informação pública em rede: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016.

LIMBERGER, T. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

MANCINI, P.; VIS, F. **How do digital platforms shape our lives?** In: World Economic Forum, Oct 2015. Disponível em: <https://www.weforum.org/agenda/2015/10/how-do-digital-platforms-shape-our-lives/?utm_content=buffer09d73&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer>. Acesso em: 15 dez. 2017.

MANOVICH, Lev. **Software takes command**. New York: A&C Black, 2013.

MANYIKA, J. et al. **Big data**: The next frontier for innovation, competition, and productivity. The McKinsey Global Institute, May 2011. Disponível em: <<https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation>>. Acesso em: 7 dez. 2017.

MIOZZO, J. **Após rumores de que teria aumentado preço da camisa da Chapecoense, Netshoes se pronuncia**. In: InfoMoney, 29 nov. 2016. Disponível em: <<http://www.infomoney.com.br/negocios/grandes-empresas/noticia/5878682/apos-rumores-que-teria-aumentado-preco-camisa-chapecoense-netshoes-pronuncia>>. Acesso em: 7 dez. 2017.

NAÇÕES UNIDAS NO BRASIL. **Sob liderança de Brasil e Alemanha, ONU cria mandato de relator sobre privacidade na era digital**. [S.I.]: 2015. Disponível em: <<https://nacoesunidas.org/sob-lideranca-de-brasil-e-alemanha-onu-cria-mandato-de-relator-sobre-privacidade-na-era-digital/>>. Acesso em: 6 dez. 2017.

NAÇÕES UNIDAS. Centro de Informação das Nações Unidas. **Declaração Universal dos Direitos Humanos**. Rio de Janeiro: 2009. Disponível em: <<http://www.onu.org.br/img/2014/09/DUDH.pdf>>. Acesso em: 27 nov. 2017.

O GLOBO, **O escândalo da espionagem dos EUA**. [S.I.]: 2013. Disponível em: <<https://oglobo.globo.com/mundo/o-escandalo-da-espionagem-dos-eua-10191175>>. Acesso em: 3 dez. 2017

O'NEIL, C. **Weapons of Math Destruction**: How Big Data Increases Inequality and Threatens Democracy. Denver: Crown, 2016.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho**, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias, n. L 281, p. 31-39, 23 nov. 1995. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em: 6 dez. 2017.

PASQUALE, F. A. **The Black Box Society: The Secret Algorithms that Control Money and Information**. Cambridge: Harvard University Press, 2016.

PERASSO, V. O que é a 4ª revolução industrial - e como ela deve afetar nossas vidas. In: **Bbc Brasil**, 2016. Disponível em: <<http://www.bbc.com/portuguese/geral-37658309>>. Acesso em: 22 nov. 2017.

PRIVACY by design. In: Wikipédia, a enciclopédia livre, 2017. Disponível em: <https://en.wikipedia.org/wiki/Privacy_by_design>. Acesso em: 22 dez. 2017.

RAMOS, A. de C. **Curso de Direitos Humanos**. 1. ed. São Paulo: Saraiva, 2014.

RIFKIN, Jeremy. **A Terceira Revolução Industrial: Como o poder lateral está transformando a energia, a economia e o mundo**. São Paulo: M. Books do Brasil, 2012.

RODOTÀ, S. **Tecnologie e Diritti**. Bologna: il Mulino, 1995.

SETZER, V. W. **Dado, Informação, Conhecimento e Competência**. DataGramaZero - Revista de Ciência da Informação, [S. l.], n. zero, dez. 1999. Disponível em: <<https://www.ime.usp.br/~vwsetzer/datagrama.html>>. Acesso em: 30 nov. 2017.

SILVA, J. A. **Curso de Direito Constitucional Positivo**. 31. ed., rev. e atualizada até Emenda Constitucional nº 56, de 20 de dezembro de 2007. São Paulo: Malheiros, 2008.

SILVEIRA, S. A. da. **Tudo sobre Tod@s: Redes Digitais, Privacidade e Venda de Dados Pessoais**. São Paulo: Edições Sesc São Paulo, 2017.

SILVEIRA, S. A. **Governo dos Algoritmos**. Revista de Políticas Públicas, São Luiz, v. 21, n. 1, p. 267-281, jan./jun. 2017. p. 271-272. Disponível em: <<http://www.periodicoeletronicos.ufma.br/index.php/rppublica/article/view/6123>>. Acesso em: 12 dez. 2017.

SOLIS, B. **What's the future of Business? Changing the way businesses create experiences**. Hoboken: John Wiley & Sons, Inc., 2013.

SOLOVE, D. J. **The digital person**: technology and privacy in the information age. New York: New York University Press books, 2004. Disponível em: <<http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text.htm>>. Acesso em: 1º dez. 2017.

UNITED NATIONS. Human Rights Council. **Resolution A/HRC/32/L.20**. The promotion, protection and enjoyment of human rights on the Internet. [Geneva], 27 June 2016. Disponível em: <<https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf>>. Acesso em: 9 dez. 2017.

UNITED STATES. U.S. Department of Health and Human Services. **Records, Computers and the Rights of Citizens**. Washington, D.C., 7 jan. 1973. Disponível em: <<https://aspe.hhs.gov/report/records-computers-and-rights-citizens>>. Acesso em: 18 dez. 2017.

WARREN, S. D.; BRANDEIS, L. D. **Das Recht auf Privatheit – The Right to Privacy**. Harvard Law Review, v. IV. n. 5. Dec. 1890.

WIENER, N. **God, Golem, Inc.:** A comment on Certain Points Where Cybernetics Impinges on Religion. Cambridge: MIT The Press, 1966.

WORLD ECONOMIC FORUM. Global Agenda Council on the Future of Software & Society. **Deep Shift Technology Tipping Points and Societal Impact**. Survey Report, Sept. 2015. Disponível em: <http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf>. Acesso em: 27 nov. 2017.

ZUBOFF, S. **Big Other**: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology, [S. l.], v. 30, issue 1, p. 75-89, Apr. 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754>. Acesso em: 12 dez. 2017.