MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. Revista Eletrônica Direito e Política, Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica da UNIVALI, Itajaí, v.15, n.3, 3º quadrimestre de 2020. Disponível em: www.univali.br/direitoepolitica - ISSN 1980-7791

PRINCÍPIO DA PRIVACIDADE POR *DESIGN*: FUNDAMENTOS E EFETIVIDADE REGULATÓRIA NA GARANTIA DO DIREITO À PROTEÇÃO DE DADOS[1]

PRIVACY BY DESIGN PRINCIPLE: FOUNDATIONS AND REGULATORY EFFECTIVENESS IN GUARANTEEING THE RIGHT TO DATA PROTECTION

Marco Aurélio Marrafon[2]

Luiza Leite Cabral Loureiro Coutinho[3]

RESUMO

O presente artigo aborda os fundamentos e as diretrizes regulatórias na implementação do princípio *privacy by design* na fase de concepção de uma nova tecnologia, de modo a assegurar a efetividade do direito à proteção de dados e à privacidade. Nesse sentido, trabalha-se o conceito, a origem, o alcance, os princípios derivados, o estado da arte, os meios de implementação e os riscos que envolvem a *privacy by design*. Objetiva-se, com isso, identificar os desafios associados à privacidade e à segurança de dados, além de definir padrões normativos que possam assegurar a privacidade em todas as etapas do ciclo de desenvolvimento do sistema. Utilizou-se o método dedutivo e a pesquisa bibliográfica documental, legislativa e acadêmica, bem como a análise comparativa do tema. Em suma, entende-se que o princípio *privacy by design* é importante garantia à concretização prática do direito à proteção de dados, bem como do direito fundamental à privacidade.

PALAVRAS-CHAVE: Privacidade por design; Inteligência artificial e novas tecnologias; Proteção de dados; Direito fundamental à privacidade e à intimidade.

---

[1] Artigo produzido no âmbito do Grupo de Pesquisas Institucional "Novas Tecnologias, Inteligência Artificial, Direito e Democracia", vinculado ao Programa de Pós-graduação em Direito da Universidade do Estado do Rio de Janeiro – UERJ, sob Coordenação do Prof. Dr. Marco Aurélio Marrafon

[2] Professor da disciplina de Direito e Pensamento Político na graduação, mestrado e doutorado em Direito da Universidade do Estado do Rio de Janeiro – UERJ. Doutor (2008) e Mestre (2005) em Direito do Estado pela Universidade Federal do Paraná – UFPR, com estudos doutorais (sanduíche) na *Università degli Studi di ROMA TRE* – Itália. Coordenador do Laboratório de Direito e Inteligência Artificial – LabDIA da Faculdade de Direito da UERJ. Professor e membro da Academia Brasileira de Direito Constitucional – ABDConst. Advogado. ORCID: https://orcid.org/0000-0002-6891-6221. E-mail: marco_marrafon@yahoo.com.br.

[3] Mestranda em Direito pela Universidade do Estado do Rio de Janeiro (UERJ), na linha de pesquisa em Direito Civil. Pós-graduada *lato sensu* pela Escola da Magistratura do Estado do Rio de Janeiro (EMERJ). Advogada. Bacharel em Direito pela UNIFLU/FDC. ORCID: https://orcid.org/0000-0003-3118-2049. E- mail: luizalcloureiro@gmail.com

ABSTRACT

The present article discusses the foundations and the regulatory guidelines in the implementation of the principle privacy by design at the design stage of a new technology, in order to ensure the effectiveness of the right to data protection and privacy. In this sense, the definition, the origin, the reach, the derived principles, the state of art, the implementations ways and the risks which involve the privacy by design are worked here. This study aims to identify the challenges associated with the privacy and the data security and also define normative standards that can ensure the privacy in all stages of the system development cycle. The deductive method and the literature and legal search were used, as well as the comparative theme analysis. Therefore, we understand that the principle privacy by design is an important assurance to the data protection right achievement and the fundamental right to privacy.

KEYWORDS: Privacy by design; Artificial intelligence and new technologies; Data protection; Fundamental right to privacy and intimacy.

INTRODUÇÃO

Diferente da perspectiva clássica da Grécia antiga, onde a privacidade e a intimidade envolvia a ideia de privação e a vida para satisfação de necessidades, não alcançando, portanto, a liberdade política própria do espaço público[4], a ascensão do individualismo moderno reforçou a noção de privacidade a partir da feição do "direito a ser deixado só", sem sofrer intervenção de terceiros em suas escolhas existenciais, cujo paradigma era a ausência de comunicação, o "zero-relationship"[5].

Essa concepção original passou a ser mitigada pela crescente consciência de que a privacidade é um aspecto fundamental da realização pessoal e do

[4] ROBL FILHO, Ilton Norberto. **Direito, intimidade e vida privada: paradoxos jurídicos e sociais na sociedade pós-moralista e hipermoderna.** Curitiba: Juruá, 2010. p. 57 e ss.

[5] Nas últimas décadas, a privacidade reuniu uma série de interesses ao redor de si, substancialmente alterando o seu perfil. Chega-se ao ponto de verificar, de acordo com a lição de Stefano Rodotá, que o direito à privacidade não mais se estrutura em torno do eixo "pessoa-informação-segredo", no paradigma "zero relationship", mas sim no eixo "pessoa-informação-circulação-controle". Segundo brilhante autor, "A proteção de dados está sob ataque todos os dias. Existe espaço para uma reinvenção afirmativa, ou uma abordagem defensiva é a única opção possível? Os dois objetivos não devem ser separados." (RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 81).

desenvolvimento da personalidade, além de adotar-se a ideia de direito à privacidade como autodeterminação informada.

Assim, a privacidade passou a ser compreendida como um direito fundamental reconhecido pelos artigos 7º e 8º da Convenção Europeia de Direitos Humanos, que prevê direito à vida privada e familiar, o respeito à casa, à correspondência e aos dados pessoais. Em um escopo mais amplo, o artigo 12 da Declaração Universal de Direitos Humanos protege o indivíduo de interferências arbitrárias em sua privacidade, família, casa ou correspondência e ataques a sua honra e reputação. No ordenamento jurídico brasileiro, a privacidade e a intimidade são invioláveis, compreendidos enquanto direitos fundamentais contemplados no inciso X do art. 5º da Constituição da República de 1988.

Nessa linha, a proteção da privacidade e da intimidade não deve ser considerada apenas um valor individual, mas também um elemento essencial das sociedades democráticas regidas pelo Império da Lei e pelos ditames do Estado de Direito.

Na era digital, tais direitos fundamentais merecem especial atenção. Isso porque dados sobre os cidadãos são captados a todo tempo e é visível o desequilíbrio de poder entre os entes controladores do processamento de dados, que determinam o quê, o como e o porquê os dados pessoais são processados, e os indivíduos cujos dados estão em jogo.

Com efeito, exige-se, mais e mais, o funcionamento confiável das tecnologias de informação e comunicação (ICT, em inglês). Afinal, menos privacidade não significa, necessariamente, mais segurança. Contudo, certamente implica em menos liberdade[6]. Daí a importância de construções normativas e regulatórias para fins de garantir o direito à proteção de dados pessoais, assegurando, via de consequência, o direito constitucional à privacidade, à intimidade e, mesmo, à liberdade, em suas multifacetadas manifestações existenciais.

[6] O excesso de vigilância pode repercutir negativamente sobre os direitos fundamentais, restringindo-os. De acordo com Michel Foucault, em sua obra *Vigiar e Punir*, é necessária a "suavização dos crimes antes da suavização das leis. Ora, essa transformação não pode ser separada de vários processos que lhe armam uma base; e (...) de uma modificação no jogo das pressões econômicas, de uma elevação geral do nível de vida, de um forte crescimento demográfico, de uma multiplicação das riquezas e das propriedades e da necessidade de segurança que é uma consequência disso". (FOUCAULT, Michel. **Vigiar e punir.** Tradução de Raquel Ramalhete. 20ª ed. Petrópolis: Ed. Vozes, 1999).

Nessa perspectiva, entende-se que a *privacy by design* deve ser compreendida um princípio fundante que norteia e vincula a elaboração da regulação jurídica de modo a assegurar a eficácia concreta do direito à proteção de dados. Ou seja, esse princípio deve atuar como uma premissa a partir da qual se desdobra um conjunto de diretrizes normativas, bem como uma lógica e uma metodologia de trabalho na estruturação e funcionamento das novas tecnologias.

Com o reconhecimento jurisprudencial da proteção de dados como direito fundamental, é possível vislumbrar, inclusive, o princípio *privacy by design* como uma norma implícita à concretização desse direito fundamental, dotada de caráter vinculante[7].

Estabelecido o ponto de partida, o presente artigo visa contribuir para que a *privacy by design* seja conduzida de forma concreta e eficaz na proteção desses direitos. Trata-se de abordagem do direito à privacidade aplicada à Inteligência Artificial na implementação de um padrão no estágio de design: a proteção de dados desde a fase de concepção da tecnologia a ser criada. Objetiva também identificar desafios associados à privacidade e à segurança de dados e definir modos de construir e assegurar a privacidade em todas as etapas do ciclo de desenvolvimento do sistema.

Para tanto, serão elucidados conceito, origem, alcance, princípios derivados, estado da arte, meios de implementação e riscos que envolvem a *privacy by design*.

A metodologia utilizada foi dedutiva, via pesquisa documental e comparativa com outros ordenamentos jurídicos, bem como ampla análise legislativa e de artigos científicos.

[7] Sobre normas jurídicas no sistema constitucional e a possibilidade de princípios constitucionais implícitos, conferir: MARRAFON, Marco Aurélio. **Hermenêutica, sistema constitucional e aplicação do direito.** 2 ed. Florianópolis: Emais Editora, 2018.

1. PRINCÍPIO *PRIVACY BY DESIGN*: ORIGEM, DESENVOLVIMENTO E PRINCIPIOLOGIA DERIVADA

O termo *privacy*, como conceito jurídico moderno, originou-se na sociedade burguesa estadunidense através da obra de dois juristas, no final do século XIX, Samuel Warren e Louis Brandeis, que, atentos aos avanços tecnológicos, teriam sido os pioneiros a tratar do tema[8] em famoso artigo intitulado *The Right to Privacy*, publicado em 1890 pela *Harvard Law Review*[9].

Após a Segunda Guerra Mundial, a privacidade passou a ser garantida em vários tratados internacionais. Sua menção pioneira veio em 1948, na Declaração Americana dos Direitos e Deveres do Homem, estando, no mesmo ano, prevista na Declaração Universal de Direitos do Homem, aprovada pela Assembleia Geral da ONU; além da Convenção Europeia de Direitos do Homem (1950) e da Convenção Americana de Direitos Humanos, conhecida como "Pacto de São José da Costa Rica" (1969) e, mais recentemente, na Carta de Direitos Fundamentais da União Europeia (2000). No Brasil, o inciso X do art. 5 da Magna Carta expressamente garante a inviolabilidade da privacidade e da intimidade (1988).

Privacy by design e *privacy by default*[10]*,* são princípios que possibilitam uma adequada governança sobre dados. As primeiras ideias de *privacy by design* (PbD) originaram-se na década de 1970 e foram incorporadas nos anos 1990 na Diretiva Europeia de Proteção de Dados: a RL 95/46/EC. Consoante o Considerando nº. 46 da diretiva mencionada, as medidas técnicas e

[8] WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy.** Harvard Law Review, v.4, n.5, 1890, p. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warrenbrandeis.pdf. Acesso em: 06 set. 2020.

[9] CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais.** Coimbra: Almedina, 2005, p. 17.

[10] A *privacy by default* determina que, quando um produto ou serviço é lançado, as configurações mais seguras de privacidade devem ser adotadas como padrão, sem a necessidade de qualquer entrada manual pelo usuário final. Assim, os dados pessoais fornecidos pelo usuário para permitir o uso ideal do produto ou serviço serão mantidos somente pelo tempo indispensável para fornecê-lo. Se outras informações, além daquelas estritamente necessárias, forem requeridas, mantidas por mais tempo que o preciso ou forem divulgadas, a privacidade do usuário terá sido violada. Na prática, em um website que usa cookies, por exemplo, eles só podem ser habilitados quando o usuário consentir e ativar a coleta de dados. Caso não ativados os cookies de forma voluntária, não pode haver a coleta de seus dados pessoais. A Lei Geral de Proteção de Dados exige que todas as sociedades empresárias que façam uso de cookies os deixem desativados como configuração-padrão, cabendo ao usuário decidir quais deseja compartilhar.

organizacionais devem ser tomadas no momento do planeamento de um sistema de tratamento de dados para proteger sua segurança.

Na origem, a *privacy by design* se revela no postulado que impulsiona a ideologia de que a privacidade deve integrar as prioridades de organização, desenvolvimento e planejamento das instituições democráticas e ser parte dos deveres e obrigações de todas as operações de sociedades empresárias que utilizam Inteligência Artificial (IA). Exige-se que as organizações adotem padrões especiais e medidas técnicas que assegurem que apenas os dados pessoais necessários sejam processados para cada propósito específico.

Trata-se de requisito do *European Union's General Data Protection Regulation* (GDPR), em vigor desde 25 de maio de 2018. Ao inclui-la como elemento essencial, a União Europeia (UE) demonstra que a proteção de dados é prioridade para o avanço tecnológico.

A legislação norteamericana, por outro lado, não impõe que requisitos de privacidade sejam implementados em design, ou nas demais etapas de desenvolvimento da tecnologia, embora a FTC[11] incentive as empresas a fazê-lo voluntariamente.

A legislação europeia deixa completamente em aberto quais exatas medidas de proteção deveriam ser tomadas. Basta a "pseudonimização" do nome para a garantia da privacidade? A autenticação do usuário e a introdução técnica do direito de oposição devem ser consideradas.

Ademais, deve-se garantir que o estado da arte e os custos de implementação razoáveis sejam incluídos. Nesse diapasão, o Considerando nº. 78 do GDPR não

[11] A *Federal Trade Commission* é uma agência governamental norteamericana responsável por fiscalizar a segurança e a privacidade de dados nos Estados Unidos da América. Os EUA contam com uma abordagem setorial, que consiste em uma miscelânea de leis federais específicas do setor, muitas vezes aplicadas por diferentes agências e fornecendo diversos padrões. As federais são complementadas por leis estaduais de privacidade, diretrizes autorregulatórias e legislações gerais de proteção do consumidor. A abordagem setorial criou uma colcha de retalhos de leis que se sobrepõem, se encaixam e se contradizem.

fornece muitos pormenores, em que pese faça menção à criptografia e à anonimização de dados como possíveis medidas de proteção[12].

Além de conceder direitos amplos aos titulares dos dados, o GDPR apresenta um padrão elevado de consentimento do titular como justificativa para o tratamento de seus dados pessoais[13].

As sociedades empresárias precisam ter embasamento legal ou razão específica, legítima e explícita para processar dados pessoais de terceiros. Para confiar no consentimento, elas têm que demonstrar que ele foi gratuito, específico, informado e inequívoco. Ou seja, a UE emprega a abordagem *opt-in*[14] quanto ao consentimento do titular no tratamento de seus dados pessoais, em contraste com a abordagem *opt-out* adotada pelos EUA. De modo a abordar o efeito de "caixa preta"[15] que o uso de dados por IA pode gerar, surgiram outras abordagens, incluindo a "auditoria algorítmica".

Embora a privacidade exija que as informações de identificação pessoal sobre os indivíduos sejam protegidas contra o acesso não autorizado, para o qual fortes medidas de segurança são essenciais, faz-se mister reconhecer que a

[12] LGPD, "Art. 5º. Para os fins desta Lei, considera-se: (...); XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; [...]." LGPD, "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...); IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; [...]."

[13] O princípio do consentimento consiste na manifestação livre, inequívoca e informada, mediante a qual o usuário concorda com o tratamento de seus dados pessoais para uma determinada finalidade. É a partir do consentimento que se analisa a legitimidade da coleta, do tratamento e do armazenamento dos dados.

[14] O uso distintivo de dados pessoais já era legítimo por força da Lei do Cadastro Positivo (Lei nº 12.414/2011), que autorizava o *credit scoring* para fins de concessão de crédito mediante coleta de dados pessoais. Com o advento da Lei Complementar nº. 116/2019 alterou-se o sistema de consentimento do cadastro positivo: anteriormente vigorava o modelo "opt-in" (a abertura do cadastro positivo requeria autorização prévia do titular) e passou a adotar o modelo "opt-out" (o cadastro é aberto automaticamente e se encerra quando o consumidor solicita expressamente). O formato inicial detinha baixa adesão, por isso os gestores de bancos de dados impulsionaram tal mudança legislativa.

[15] Uma caixa preta, em geral, é um sistema impenetrável cujas entradas e operações não são visíveis para o usuário ou outra parte interessada. O viés de opacidade da IA pode ser introduzido nos algoritmos como reflexo de preconceitos conscientes ou inconscientes por parte dos desenvolvedores do design, ou podem se infiltrar por erros não detectados, e seus resultados são tendenciosos e distorcidos. Para evitar danos, os designers necessitam dar transparência aos algoritmos e as organizações se responsabilizarem por eventuais efeitos prejudiciais. (PASQUALE, Frank. **The black box society: the secret algorithms that control money and information.** Boston: Harvard University Press, 2016).

privacidade envolve muito mais que garantir acesso seguro aos dados. Privacidade pressupõe controle, permitindo que os titulares mantenham controle individual sobre as informações de identificação pessoal em relação à coleta, análise, armazenamento, uso, manipulação e divulgação.

Apesar dos desafios crescentes trazidos pela convergência de computação social, móvel e em nuvem, a privacidade não é apenas uma tarefa realizável, é ainda altamente desejável para todas as organizações na manutenção da confiança de seus clientes.

Alcançar o resultado desejado de privacidade não requer desistir das muitas vantagens e dos benefícios advindos da tecnologia. Ao invés de tentar (e fracassar) viver "fora da rede" como uma forma de protesto ou ficta proteção contra as violações à privacidade na era da pulverização da informação, é necessária uma mudança de postura quanto à origem do problema: o projeto tecnológico, a concepção da IA, o design.

A privacidade desde o *design* não é um conceito novo em proteção de dados. É a filosofia proposta academicamente por Ann Cavoukian[16], a Comissária de Informação e Privacidade, nos anos 1990 no Canadá. Cavoukian é mundialmente reconhecida como a principal criadora do conceito de *privacy by design* (PbD), tal como é estudado atualmente.

Diante de sistêmicos e crescentes desafios tecnológicos, a PbD fornece uma visão holística e uma perspectiva preventiva da proteção de dados. Sua aplicação atravessa toda a estrutura do negócio, de ponta a ponta, incluindo informações, práticas e processos de negócios, design físico e em rede, e sua infraestrutura, com o objetivo de atingir uma soma positiva na interação, mutuamente benéfica, entre privacidade (como padrão de negócio) e tecnologia.

Já há algum tempo, tem-se consolidado entre os estudiosos da temática que o princípio nuclear *privacy by design* está embasado em sete pilares, que podem ser considerados princípios dele derivados, conforme bem expõe Cavoukian, são

[16] CAVOUKIAN, Ann, CHANLIAU, Marc. **Privacy and Security by Design: A Convergence of Paradigms**. Disponível em: http://www.ipc.on.ca/images/Resources/pbd-convergenceofparadigms.pdf. Acesso em: 16 ago. 2020.

eles: 1) um projeto proativo, não reativo, não repressivo e sim preventivo, que antecipe e evite a invasão à privacidade antes que aconteça, não esperando que os riscos à privacidade de dados se materializem, com o constante monitoramento de riscos e com a entrega de funcionalidades novas que excluam os riscos identificados[17]; 2) a privacidade de dados como configuração-padrão, instituindo medidas de privacidade diretamente em qualquer sistema de tecnologia da informação e comunicação (TIC), já como um paradigma para práticas negociais, além de implementar políticas padronizadas de segurança de dados, incluindo um privilégio mínimo às empresas de tecnologia e uma confiança legítima no controle obrigatório de acesso e na separação de funções; 3) a privacidade incorporada ao projeto, o que significa que estará embutida desde a sua arquitetura, e não adicionada após o fato – o usuário terá o controle para alterar as configurações-padrão e optar por fornecer ou não seus dados –, resultando que a privacidade se torne um componente essencial da funcionalidade central a ser entregue; 4) a funcionalidade completa como uma soma positiva (e não uma soma-zero, sem haver neutralidade, nem opacidade[18]) – ao incorporar a privacidade de dados a determinada tecnologia, processo ou sistema, isso deve ser feito de forma que a funcionalidade total não seja prejudicada e, na medida do possível, que seja otimizada (o produto ou serviço deve ser plenamente utilizável caso o usuário não aceite afrouxar as configurações de privacidade, ou seja, não deve haver funcionalidade adicional

[17] A LGPD, secundando o GDPR, introduziu mudança profunda em termos de responsabilização lato sensu, no que diz respeito à imposição de deveres voltados a prevenir danos. Trata-se do conceito de —prestação de contas‖. Esse novo sistema de — "responsabilização proativa" encontra-se indicado no inciso X do artigo 6º da LGPD. Não descumprir a lei não é mais suficiente; é preciso ativamente prevenir a ocorrência de danos à privacidade no tratamento de dados pessoais de terceiros.

[18] Uma das principais desvantagens das técnicas de aprendizado das máquinas (machine learning) é a opacidade. Como os algoritmos não são mais apenas criados diretamente por seres humanos, o real processo de raciocínio usado pelas máquinas pode ser desconhecido e incognoscível. Mesmo se alguém pudesse consultar a máquina e perguntar quais algoritmos e fatores foram utilizados para chegar a um determinado resultado, a máquina poderia não saber responder. Equivale a perguntar à tartaruga porque sua espécie decidiu se adaptar e desenvolveu um casco. A eficácia dos sistemas autônomos é limitada pela incapacidade atual da máquina de explicar suas decisões, associações e ações para os usuários humanos. Leva-se em conta que preceitos legais, a noção de intencionalidade e de culpa e o devido processo legal são incompatíveis com a IA. O problema aumenta à medida que damos à IA mais e mais tarefas e, portanto, mais poder, o que pode, em última análise, levar à criação de leis por robôs. (MANHEIN, Karl M.; KAPLAN, Lyric. **Artificial Intelligence: Risks to Privacy and Democracy** (October 25, 2018). 21 Yale Journal of Law and Technology 106 (2019), Loyola Law School, Los Angeles Legal Studies Research Paper Nº. 2018-37. Disponível em: https://papers.ssrn.com/sol3/papers. cfm?abstract_id=3273016. Acesso em: 30 jul. 2020).

ou qualquer vantagem ao usuário para flexibilizar o controle da privacidade de seus dados); 5) segurança de ponta a ponta e proteção total do ciclo de desenvolvimento tecnológico, isso porque estritas medidas de segurança, do início ao fim e por todo o domínio, são essenciais para salvaguardar continuamente a privacidade durante todo o ciclo de vida dos dados, não havendo lacunas na proteção e no controle, nem na responsabilização (o tratamento de dados deve ser seguro, desde a coleta até a sua eliminação, não se limitando à etapa de configuração do produto ou serviço); 6) a garantia de escolha, controle, visibilidade e transparência[19] como ferramentas essenciais à confiança na análise e proteção de dados, além de fundamental à ideia de *accountability*, ou seja, as sociedades empresárias devem permitir que seja verificado se cumprem, ou não, o que prometem sobre os dados de seus usuários, seja o controle direto ou por meio de auditorias independentes; 7) as normas regulatórias devem centralizar-se em assegurar a confidencialidade, integridade, disponibilidade e segurança dos dados em benefício de seus titulares, no sentido de que a *privacy by design* é projetada para o gerenciamento de dados pessoais por seus próprios titulares, cabendo aos tech designers oferecerem melhores padrões de privacidade, notificação apropriada e opções amigáveis de configurações aos usuários[20].

Essas e outras questões envolvendo a privacidade de dados desencadearam o "Movimento IA Responsável", encabeçado por Bill Gates e Stephen Hawkins, após a Conferência de Asilomar[21], em 2007, sobre os benefícios e riscos da IA.

[19] Há quatro etapas a serem observadas por todos os desenvolvedores de tecnologia: (i) oferecer ao usuário escolhas informadas sobre sua privacidade; (ii) disponibilizar mecanismos de controle de privacidade robustos e eficazes para assegurar privacidade por todo o ciclo de vida dos dados, desde a coleta até o descarte; (iii) auxiliar os usuários a tomarem as melhores decisões sobre a privacidade de seus dados, esclarecendo quais dados foram ou serão coletados e usados para personalizar experiências e servir de publicidade; (iv) investimentos compatíveis ao armazenamento acessível de dados por seu titular, e de forma segura, para que não sejam acessados por terceiros não autorizados.

[20] CAVOUKIAN, Ann. **Privacy by design: the 7 foundational principles. Implementation and mapping of fair information practices.** Disponível em : https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf Acesso em: 16 ago. 2020.

[21] A Conferência de Asilomar sobre Inteligência Artificial foi organizada pelo *Future of Life Institute* e realizada de 5 a 8 de janeiro de 2017, no *Asilomar Conference Grounds*, no Estado da Califórnia – EUA.

Os valores aos quais os desenvolvedores de IA devem aderir precisam incluir: liberdade, privacidade, responsabilidade, transparência e dignidade humana. Outro valor de vital importância é: o poder conferido pelo controle de sistemas altamente avançados de IA deve respeitar, ao invés de subverter, processos sociais e cívicos dos quais dependa a sociedade. Os princípios de Asilomar emprestaram autoridade moral a tais apelos frente a governos e empresas negligentes. Tanto que, no final de 2018, o Estado da Califórnia positivou os Princípios de Asilomar. Espera-se ser o início de uma tendência a nível internacional.

No Brasil, a Lei Geral de Proteção de Dados (LGPD), cuja vigência teve início em 18 de setembro de 2020, adota, de modo muito tímido e superficial, a perspectiva preventiva de proteção à privacidade de dados *by design*, no artigo 6º ("VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais") e no artigo 46 ("§2º. As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução").

2. RISCOS À PRIVACIDADE E À SEGURANÇA DE DADOS PESSOAIS

A Inteligência Artificial (IA) é a tecnologia mais disruptiva da era moderna, uma ferramenta poderosa para resolver problemas e criar outros novos[22]. Eventos recentes ilustram como a IA pode ser transformada em uma arma para corromper eleições (como ocorreu no escandaloso caso da empresa de análise de dados *Cambrigde Analytica* nos EUA)[23] e envenenar a confiança das pessoas nas instituições democráticas e em seus valores fundamentais, agravando a atual

[22] MANHEIN, Karl M.; KAPLAN, Lyric. **Artificial Intelligence: Risks to Privacy and Democracy** (October 25, 2018). 21 Yale Journal of Law and Technology 106 (2019), Loyola Law School, Los Angeles Legal Studies Research Paper nº. 2018-37. Disponível em: https://papers.ssrn.com/sol3/papers. cfm?abstract_id=3273016. Acesso em: 30 jul. 2020.

[23] **THE GREAT HACK (PRIVACIDADE HACKEADA)**. Direção: Karim Amer e Jehane Noujaim. Produção: Karim Amer, Jehane Noujaim, Pedro Kos, Geralyn Dreyfous e Judy Korin. Netflix. Data de lançamento mundial: 26 jan. 2019. Disponível em: https://www.netflix.com/br/title/80117542. Acesso em: 8 ago. 2020.

crise de legitimidade[24]. Assim como em outras tendências disruptivas, o direito demora a acompanhar os avanços da tecnologia.

Por trás da nomenclatura, a Inteligência Artificial emula a cognição humana por meio de programas de computação. A IA trabalha na dimensão algorítmica, com grande capacidade de processamento de dados e estabelecimento de conexões, mas seu nível de linguagem não alcança a consciência hermenêutica, restringindo-se à dimensão lógico-formal das manifestações linguísticas[25].

Ainda assim, ela tem sido considerada uma forma de "computação inteligente" que, por um conjunto de orientações previamente programadas (os algoritmos) define comandos de ação e reação, num sistema de "*if* (...) *then* (...)".[26]

Já a "Internet das Coisas"[27] (IoT) representa um ecossistema de sensores eletrônicos encontrados em nossos corpos, escritórios, casas, veículos e lugares públicos. Produto da "Internet das Coisas" tem sido a ascensão do *Big Data*[28] e da análise de dados.

Tais ferramentas permitem mudanças sofisticadas e quase imperceptíveis do comportamento dos consumidores, espectadores e eleitores, acarretando perda da privacidade[29] e da autonomia na tomada de decisões.

---

[24] CHEVALIER, Jacques. **O Estado pós-moderno**. Tradução de Marçal Justen Filho. Belo Horizonte: Fórum, 2009, p. 183-284.

[25] Sobre o tema, conferir: MARRAFON, Marco Aurelio. **Filosofia da Linguagem e limites da IA na Interpretação Jurídica.** Revista Consultor Jurídico, 2019. Disponível em: https://www.conjur.com.br/2019-jul-22/constituicao-poder-filosofia-linguagem-limites-ia-interpretacao-juridica. Acesso em: 16 ago. 2019.

[26] **EXPLAINED (EXPLICANDO)**. 2ª Temporada. 8º episódio: Código de Programação. Direção: Ezra Klein e Joe Posner. Produtores executivos: Ezra Klein, Kara Rozansky, Chad Mumm, Lisa Nishimura, Joe Posner, Jason Spingarn-Koff e Kate Townsend. Netflix. Data de lançamento mundial: 23 maio 2018. Disponível em: https://www.netflix.com/br/title/80216752. Acesso em: 22 ago. 2020.

[27] "Coisas" seria qualquer objeto natural ou feito pelo homem ao qual é atribuído um endereço de internet e que transfere dados por uma rede sem interação de pessoa para pessoa ou de pessoa para computador.

[28] As tecnologias de *Big Data* são definidas como aquelas com capacidade para processar, com bastante velocidade, um grande volume de dados dos formatos mais variados. Volume, variedade e velocidade no processamento de dados são conhecidos como os três Vs do *Big Data*.

[29] Estabelece o Código Civil Brasileiro em seu artigo 21 que: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Tecnologias refinadas de manipulação progrediram ao ponto em que os indivíduos entendem que as decisões tomadas por IA podem parecer próprias, mas são, na verdade, frequentemente "guiadas" por algoritmos. Um exemplo robusto é o "grande empurrão", uma forma de "computação persuasiva" que permite governar as massas de forma eficiente, sem envolver os cidadãos em processos democráticos.

Por isso, é possível antever o cenário de IA emergente como um novo modelo de totalitarismo digital, marcado pelo domínio algorítmico e ausência de liberdade, no qual os direitos dos usuários definidos por algoritmos[30].

Mais preocupantes são os riscos *sui generis* decorrentes da IA, que incluem a capacidade de a IA gerar perfis comportamentais abrangentes de diversos conjuntos de dados e reidentificar dados anônimos. Isso expõe detalhes dos dados pessoais mais íntimos para anunciantes, governos e até estranhos. Os maiores perigos estão nas redes sociais, que contam com IA para alimentar seus modelos de incremento de receita.

Muitos sistemas diferentes estão sob o abrangente guarda-chuva da Inteligência Artificial. Incluem os *Expert Systems*, que são algoritmos detalhados passo a passo, que contêm uma série de regras programadas por humanos para a resolução de problemas.

Mais adiante, desenvolve-se o *Machine Learning* (ML), forma avançada de IA que depende menos da programação humana e mais da capacidade dos algoritmos de usarem métodos estatísticos e aprenderem com os dados conforme progridem. ML pode ser supervisionado e treinado por humanos, ou não, significando, neste último caso, que seria autodidata e poderia não haver interferência humana em seus *inputs*.

[30] O filme norte-americano "O show de Truman: o show da vida" retrata, num cenário de ficção, um ambiente no qual cada pessoa vivencia apenas a sua realidade individual do mundo. Tal contexto poderia ser transportado para a realidade atual da era digital no que tange ao que nos é, diariamente, recomendado por algoritmos que analisam, armazenam e manipulam nossos comportamentos como usuários da rede mundial de computadores. Em tocante cena do filme, o "programador da vida" do protagonista Truman assim afirma: "We accept the reality of the world with which we are presented, it's as simple as that".

Forma mais intensa de ML é o *Deep Learning* (DL), que usa algoritmos de aprendizado, chamados "redes neurais artificiais", vagamente inspiradas nas estruturas do cérebro humano[31], e que se conectam umas às outras em diversas camadas que se reconectam e se editam instantaneamente por *loops* de *feedback*, denominados "retropropagação".

Enquanto a IA não superar a inteligência humana, continuaremos na era do *Artificial Narrow Intelligence* (ANI), ou IA fraca, na qual, programas de computador com fins especiais superam humanos em tarefas específicas, como jogos de xadrez e análise textual. Já a próxima geração de IA será a *Artificial General Intelligence* (AGI) quando a capacidade da IA ultrapassará a solução de um predefinido conjunto de questões para ser aplicada a qualquer problema. E num futuro ainda distópico, a IA superará de forma autônoma os mais inteligentes seres humanos, alcançando a *Artificial Super Intelligence* (ASI).

Os perigos presentes e previstos que a IA representa aos princípios fundamentais de privacidade, autonomia, igualdade, devido processo legal e ao Estado de Direito são anteriores ao advento da IA, como a manipulação secreta de preferências do consumidor e do eleitor, mas são ainda mais eficazes com o vasto poder do processamento de dados. Felizmente, há tempo para planejar. Infelizmente, falta o senso apropriado de urgência.

Inseridos estamos na Sociedade da Exposição[32] e há diversificadas concepções de privacidade sendo vilipendiadas, senão vejamos: a) *informational privacy* é o direito de autocontrolar o fluxo de dados pessoais e aplica-se tanto às informações privadas quanto àquelas que compartilhamos com outros em confiança; b) *decisional privacy* é o direito de fazer escolhas e tomar decisões sem intromissão ou inspeção de terceiro(s); c) *behavioral privacy* inclui ser capaz de agir como quiser, livre de observação indesejada ou de interferência; d)

[31] TEGMARK, Max. **Life 3.0: Being Human in the Age of Artificial Intelligence**. New York: Alfred A. Knopf, 2017, p. 33-106.

[32] Na sociedade pós-moderna, o hiperindividualismo ganha força e adota múltiplas formas: a) o princípio da identidade pessoal, o movimento de rejeição aos determinismos sociais e às identificações estáveis, a ilusão de uma "ilimitada propriedade do eu" e a criação da "sociedade líquida" (BAUMANN, 2001); b) a "absolutização do eu" e o desenvolvimento de uma "cultura do narcisismo" acentuada pela busca por realização pessoal autocentrada; c) a modificação da relação com o coletivo, corrompendo as noções de espaços sociais comuns e exaltando as diferenças, a intolerância, a polarização e a singularidade.

physical privacy que abrange direitos ao esquecimento e à proteção contra mandados ilegais de busca e apreensão[33].

Os dados são, portanto, a força vital da Inteligência Artificial. Os produtos que os gigantes da tecnologia (*Facebook*, *Apple*, *Google*, etc.) ofertam, com gratuidade aparente, são veículos para coletar grandes quantidades de dados, sendo remunerados, pois, indiretamente.

Os dados pessoais são hoje a mercadoria mais valiosa da era digital, negociada em larga escala pelas mais poderosas sociedades empresárias do mundo. É a mercancia dos traços mais íntimos da nossa personalidade que impulsiona seus modelos de negócios e sua receita. Paga-se muito caro por serviços supostamente gratuitos ou de baixo custo com o livre acesso aos nossos dados. Fomenta-se o "capitalismo de vigilância", conforme bem diagnosticado por Zuboff[34].

Diante desse contexto, a humanidade parece ter adentrado na "era do niilismo da privacidade" e da "pós-verdade", em um novo modelo de desinformação pró-lucro quanto a nossos próprios dados e de como, quando e porque são coletados e manipulados pelos gigantes da tecnologia e por *third-parties*.

Algoritmos não possuem *proxi* do que é verdade que lhe permita distingui-la de *fake news*. Quando o paradigma algorítmico é definido em segundos, por cliques virtuais impulsivos, não há verossimilhança com a consciência moral que possibilita à máquina evitar a fragmentação dos fatos, a polarização de opiniões e o retrocesso social[35].

Nesse perspectiva, a IA pode comprometer a privacidade pessoal e o livre arbítrio dos cidadãos. Enquanto isolados, os conjuntos de dados individuais

[33] CASTELLITTO, Anita L. Allen. **Understanding privacy: the basics**. Disponível em: https://www.law.upenn.edu/cf/faculty/aallen/workingpapers/pli2007.pdf. Acesso em: 16 ago. 2020.

[34] ZUBOFF, Shoshana. **The age of surveillance capitalism:** the fight for a human future at the new frontier of power. New York: Publicaffairs, 2019. Nesse contexto, parece que a humanidade chegou no futuro sombrio previsto por Orwell, in: ORWELL, George. **1984**. Tradução de Heloísa Jahn e Alexandre Hubner. Rio de Janeiro: Companhia das Letras, 2009.

[35] Para maior compreensão: BALDI, Vania. **A construção viral da realidade: ciberpopulismo e polarização dos públicos em rede.** Observatório Special Issue**,** (2018), 004-020 Disponível em: http://obs.obercom.pt/index.php/obs/article/view/1420/pdf. Acesso em 03 ago. 2019.

dispersos na rede em milhares de servidores podem fornecer *insights* limitados de informações, mas tal limitação pode ser resolvida por um processo de "fusão de dados"[36], que mescla, analisa, organiza e correlaciona esses dados, permitindo a criação de "perfis psicográficos".

A partir desse momento, terceiros criam perfis sofisticados dos usuários, que oferecem verdadeiro tesouro de inteligência útil para quem deseja influenciar escolhas. Por isso, a agregação e a coordenação de bancos de dados distintos têm o potencial de beneficiar ou prejudicar a sociedade. Por exemplo, dados de saúde podem ser usados com o propósito de curar doenças, ou para desqualificar candidatos a prêmios de seguro.

Embora os usuários possam invocar a configuração "não rastrear" (Do Not Track – DNT)[37] em seus navegadores, não há exigência de que os *sites* honrem as solicitações de DNT, assim, a maioria as ignora. Isso porque o modelo de negócios para mídia social e outros serviços *online* "gratuitos" dependem da monetização de dados e do conteúdo.

Nesse cenário, muitos usuários fazem uso de pseudônimos[38] nas redes sociais. O anonimato consiste no processo de retirar informações de identificação pessoal de dados coletados para a fonte original não ser identificada. Porém, dispõe o artigo 5º, inciso IV, da Constituição da República Federativa do Brasil de 1988

[36] O *Facebook´s Photo Review* – o *Deep Face* – é um sistema de reconhecimento facial pautado em *deep learning* que identifica os componentes principais de uma imagem e a compara com outras da sua imensa base de dados, sendo considerado, hoje, mais preciso que o sistema atual do FBI. (MANHEIN, Karl M.; KAPLAN, Lyric. **Artificial Intelligence: Risks to Privacy and Democracy** (October 25, 2018). 21 Yale Journal of Law and Technology 106 (2019), Loyola Law School, Los Angeles Legal Studies Research Paper Nº. 2018-37. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273016 . Acesso em: 30 jul. 2020).

[37] "Quem controla o passado, controla o futuro. Quem controla o presente, controla o passado." A frase, ainda oportuna atualmente, era o *slogan* da figura usada por George Orwell (o pseudônimo de Eric Arthur Blair) para representar o Estado totalitário no universo distópico da obra "1984", publicada originalmente em 1949. O futuro, simbolizado pelo ano de 1984 – antes distante –, previa uma sociedade autômata, onde não haveria livre arbítrio nem liberdade: os indivíduos eram monitorados e controlados de modo absoluto e integral. O Grande Irmão, um messias para aquela desventurada sociedade, ditava as regras do jogo e observava todos, assim diziam os cartazes espalhados por cada canto da cidade. Nesse universo literário, a privacidade tinha se tornado termo obsoleto, abolido do dicionário e da memória das pessoas. (CENTODUCATTE, Rafael Avellar. **De 1984 a Westworld: a era dos dados e da vigilância**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/de-1984-a-westworld-a-era-dos-dados-e-da-vigilancia-01052020. Acesso em: 02 maio 2020).

[38] O processo de "pseudonimização" substitui elementos identificadores dos dados com outros artificiais ou pseudônimos, envolvendo técnicas como mascaramento de dados e criptografia, que podem ser usadas para proteger a identidade de cidadãos comuns, mas também de criminosos.

que: "É livre a manifestação do pensamento, sendo vedado o anonimato". Revelar a identidade é obrigatório para que os indivíduos sejam responsabilizados por seus atos caso ajam em desacordo com a lei.

A maioria das organizações que publica dados anônimos utiliza a abordagem posterior de privacidade. A abordagem de privacidade anterior (*privacy by design)* é bastante popular na comunidade acadêmica de ciência da computação, porém raramente é usada em lançamentos de dados reais. O anonimato é um desafio importante, pois essa tensão entre privacidade, liberdade e utilidade estará no centro do desenvolvimento de *Big Data*.

A indústria da publicidade é especialista em influenciar os hábitos das pessoas e suas decisões. A publicidade comportamental *online* utiliza-se de *machine learning* e algoritmos para desenvolver referências que possam antecipar padrões comportamentais do usuário.

Empresas de tecnologia especializadas em *third-party advertising* usam IA para personalizar anúncios, a fim de direcioná-los a usuários específicos para contextos específicos. Os terceiros (*third-parties*) situam-se entre o site ou aplicativo de postagem da publicidade e o anunciante que adquire o espaço publicitário em determinado site.

Na medida em que as informações sobre cada pessoa se tornam de granulares a completas, a publicidade comportamental cria um "querer" disfarçado de escolha cognitiva. O único mecanismo de defesa do usuário é apenas recusar a publicidade sob a crença errônea de que tal postura impedirá a coleta de dados[39].

[39] A *IBM* conduziu uma pesquisa segundo a qual 78% dos consumidores nos EUA acreditam que a capacidade de uma empresa de tecnologia de proteger seus dados pessoais é "extremamente importante". Todavia, apenas 20% dos consumidores "confiam totalmente" nas empresas para proteger seus dados. Em outra pesquisa conduzida pela *Blue Fountain Media*, 90% dos participantes estavam muito preocupados com a privacidade na internet, mas, ao mesmo tempo, 60% deles estavam felizes ao baixar aplicativos gratuitos sem ler os Termos de Uso. Essas pesquisas mostram que os consumidores se preocupam com a privacidade, mas não se sentem capacitados para assumir o controle de seus dados ou pensam que não têm direito de forçar a proteção de sua privacidade. (MANHEIN, Karl M.; KAPLAN, Lyric**. Artificial Intelligence: Risks to Privacy and Democracy** (October 25, 2018). 21 Yale Journal of Law and Technology 106 (2019), Loyola Law School, Los Angeles Legal Studies Research Paper Nº. 2018-37. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273016. Acesso em: 30 jul. 2020).

Há uma continuidade de influência: da persuasão à manipulação, podendo até tornar-se coerção. A tecnologia persuasiva funciona como um "reforço intermitente positivo" (termo este originário da psicologia) e implanta no usuário um hábito, de forma inconsciente, como uma forma – quase imperceptível – de reprogramação neurolinguística do humano pela máquina.

3. A EFETIVIDADE REGULATÓRIA DO PRINCÍPIO *PRIVACY BY DESIGN* ENQUANTO GARANTIA FUNDAMENTAL DO DIREITO À PROTEÇÃO DE DADOS

Com o crescimento da internet, a confiança está se tornando um fator cada vez mais importante no ecossistema digital. A desmedida coleta, análise e processamento de informações pessoais deu origem a sérias preocupações com privacidade, especialmente em relação à vigilância eletrônica em larga escala, à criação de perfis psicográficos e à divulgação de dados privados.

A privacidade tornou-se um fator crítico de confiança e de restrição das liberdades básicas na atual sociedade da informação. É amplamente reconhecido que, a menos que um sistema seja desenvolvido desde a base com proteção de seu núcleo axiológico essencial, falhas surgirão devido a deficiências inesperadas e não superadas. Com efeito, incorporar privacidade associada à segurança diretamente no *design* do sistema, produto ou serviço é uma etapa crucial para a proteção de dados.

Mesmo que seja preciso ter cautela com o conceito de regulação, sendo difícil defini-lo com precisão, entende-se, para os fins deste estudo, a regulação como o uso intencional de autoridade para afetar o comportamento de uma parte diferente de acordo com padrões previamente estabelecidos, envolvendo instrumentos de coleta de dados e de modificação do comportamento.

Quando se trata da tutela de direitos que exigem ação pública e/ou estatal, a regulação se realiza por meio de normas jurídicas *(lato sensu)* válidas e aptas a promover a adequação das condutas aos fins almejados. No que tange à eficácia regulatória, ela se perfaz quando a intervenção regulatória cumpre seus objetivos declarados.

O princípio *privacy by design* se manifesta enquanto diretriz regulatória que promove, entre outros aspectos, o emprego da *tecnorregulação* como instrumento para atingir os objetivos das leis de regência da matéria, como a LGPD no Brasil e o GDPR na União Europeia. Certas características intrínsecas ao projeto são fruto de escolhas técnicas e normativas de seus desenvolvedores, sem se ignorar a regulação tecnológica como fator de eficácia do *design*, conforme o teste de coerência e a aplicação de critérios recomendáveis. Privilegia-se a obrigação de meio, de estabelecer o *design* no caminho correto da proteção de dados.

O Artigo 25 do GDPR[40] é notoriamente vago, mas seu rigor ainda é importante tanto para proteção contra ameaças quanto contra multas do GDPR. Independentemente de se tratar de um *website*, aplicativo (*app*) ou produto que envolva Inteligência Artificial, a privacidade deve ser resguardada desde a fase de *design* e ao longo do ciclo de vida, ou seja, durante o engajamento ponta-a-ponta e após, ainda que já esteja desativado.

O GDPR exige algumas medidas técnicas e organizacionais, como criptografia e pseudonimização, mas isso não é o início e o fim da privacidade projetada. Infelizmente, o próprio GDPR não fornece uma lista de verificações exigidas e de critérios a ser observados.

O princípio *privacy by design* requer sistemas instalados, razão pela que necessita ser delineado um *checklist* para os sistemas: a) ter um compromisso organizacional documentado com os padrões mínimos de proteção de dados,

[40] GDPR, "Artigo 25 – Proteção de dados por design e por padrão – 1. Considerando o estado da técnica, o custo de implementação e a natureza, escopo, contexto e finalidades do processamento, bem como os riscos de probabilidade e severidade variadas para os direitos e liberdades das pessoas físicas decorrentes do processamento, o controlador deve, tanto no momento da determinação dos meios de processamento como no momento do próprio processamento, implementar medidas técnicas e organizacionais adequadas, tais como pseudonimização, que são concebidas para implementar princípios de proteção de dados, como a minimização de dados, de forma eficaz forma e para integrar as salvaguardas necessárias no tratamento, a fim de cumprir os requisitos do presente regulamento e proteger os direitos das pessoas em causa. 2. O responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que, por defeito, apenas sejam tratados os dados pessoais necessários para cada finalidade específica do tratamento. Essa obrigação se aplica à quantidade de dados pessoais coletados, à extensão do seu processamento, ao período de armazenamento e à acessibilidade. Em particular, tais medidas devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados sem a intervenção do indivíduo a um número indefinido de pessoas singulares. 3. Um mecanismo de certificação aprovado de acordo com o Artigo 42 do GDPR pode ser usado como um elemento para demonstrar a conformidade com os requisitos estabelecidos nos parágrafos 1 e 2 deste artigo."

incluindo cultura corporativa, práticas comerciais e serviços comerciais; b) nomear um diretor de proteção de dados (DPO), se aplicável, ou contratar um consultor de proteção de dados; c) estabelecer uma estrutura de proteção de dados, com criptografia e pseudonimização; d) criar e documentar um sistema de manutenção de registros para atividades de processamento de dados; e) formular um sistema de gerenciamento de riscos, incluindo o gerenciamento de *compliance*[41]; f) atualizar o treinamento de controle de privacidade para os funcionários que lidam com dados pessoais de clientes e outros funcionários; g) utilizar mecanismos de autoavaliação e autorregulação para melhor auditar e monitorar a implementação dos sistemas supramencionados; h) estabelecer medidas de segurança que visem minorar e evitar incidentes e violações do direito à privacidade de dados.

Malgrado inicialmente deva atentar-se ao *checklist* acima para os seus sistemas, o maior foco de trabalho das gigantes da tecnologia e demais empresas que utilizem Inteligência Artificial em seus produtos ou serviços, na garantia da

[41] LGPD, "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. §1º. Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. §2º. Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei. §3º. As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional. Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais."

privacidade como padrão principiológico desde o *design* para todo o ciclo de vida do tratamento de dados, em conformidade com o GDPR e com a LGPD, deve ser o *checklist* de seus processos, da seguinte forma: a) alocar responsabilidade[42] para o controle da *privacy by design* e *privacy by default*, aos setores técnico de informática, jurídico, de compras e vendas, etc.[43]; b) identificar riscos à privacidade em todos os processos; c) documentar seu processamento de dados, usando o sistema de manutenção de registros projetado na Lista de verificação de sistemas; d) fazer as avaliações de conformidade antes de coletar dados para uso ou armazenamento; e) criar uma "Central de Privacidade do Cliente", que permita aos titulares de dados coletados acessá-los; f) descrever a finalidade do processamento de dados (a base legal) e identificar medidas que evitem que os dados sejam processados para outros fins; g) monitorar as medidas de minimização de coleta de dados, implementar controles apropriados e corrigir os inadequados; h) descrever os controles de acesso aos dados; i) criar "Contratos de Processamento de Dados" e revê-los amiúde; j) monitorar eventuais falhas nas práticas de segurança implantadas; k) identificar as fontes de informações e notificar os usuários sobre o processamento de dados; l) descrever o processo seguido em caso de violação da segurança de dados, seguindo as regras de notificação do GDPR e da LGPD; m) efetivar as medidas da lista de verificação de sistemas, expostas no parágrafo anterior.

O problema que a PbD busca resolver é a maneira pela qual os fenômenos que são prejudiciais à privacidade e proteção de dados são tratados. Parte do desafio é que a proteção da privacidade tende a ser reativa por natureza e, mais

[42] Para as autoras Gisela Sampaio da Cruz Guedes e Rose Venceslau Meireles, a LGPD, nos artigos 42 a 45, adotou a teoria subjetiva da responsabilidade civil, devendo haver prova da culpa do agente pelo dano causado no tratamento inadequado de dados pessoais de determinado titular, seja na hipótese de omissão na adoção de medidas de segurança para o tratamento apropriado dos dados pessoais de terceiros ("quando não fornecer a segurança que o titular dele pode esperar"), seja no descumprimento das obrigações impostas na lei ("em violação à legislação de proteção de dados pessoais" ou "quando deixar de observar a legislação").

[43] Com efeito, serão obrigados a reparar o dano específico por violação da privacidade os protagonistas da LGPD: os controladores e os operadores, que respondem solidariamente. Já no que se refere às vítimas, segundo o *caput* do artigo 42 da LGPD, tais figuras não se resumem aos titulares dos dados violados, podendo tratar-se de qualquer pessoa que sofra um dano resultante de burla às normas protetivas de dados na internet, até a pessoa jurídica que considere ilegal o processamento de dados de seus funcionários ou feito por um concorrente que venha a lhe causar danos efetivos. (MORAES, Maria Celina Bodin de. **LGPD: um novo regime de responsabilização civil dito proativo**. Disponível em: http://civilistica. com/lgpd-um-novo-regime-de-responsabilizacao-civil-dito-proativo/. Acesso em: 03 out. 2020).

importante, as normas reagem e se adaptam lentamente e de forma corretiva quando o dano já está ocorreu, não observando, portanto, um dos preceitos fundamentais da PbD: a necessidade de um *design* proativo, não reativo/repressivo e verdadeiramente preventivo.

Outro agravante é que os dados pessoais se tornaram um ativo importante e valioso, tanto para os negócios (com a monetização de dados em troca de serviços digitais ou *insights*) quanto para as instituições públicas (com foco em vigilância, segurança nacional e outras iniciativas de *Big Data*). A falta de conscientização e conhecimento técnico dos usuários da internet, o fato de que o processamento de dados pessoais é transversal a inúmeros aspectos da vida cotidiana e o quão rápido a tecnologia se desenvolve são fatores que aumentam os riscos.

Tem-se afirmado que tal cenário rendeu estruturas jurídicas globais inadequadas e ineficazes em seus próprios termos. O motivo? A tecnologia é adaptada para mitigar os problemas após virem à tona, quando o dano concreto já está sedimentado, numa visão reativa e meramente corretiva, nada preventiva. Isso porque muitas tecnologias invasoras de privacidade (PITs, em inglês) são desenvolvidas e aplicadas em ritmo tão frenético que os regulamentos não conseguem acompanhar.

Essas razões explicam a importância de considerar privacidade e proteção de dados com antecedência, para que esses problemas e riscos sejam evitados já na fonte causadora. Eis a linha de raciocínio proposta pelo princípio PbD!

Quando aqueles visados pela regulamentação adotam a forma de processamento de dados compatível com as normas protetivas, o seu *design* de tecnologia deverá criar um benefício a seu favor – um selo de *compliance* que reconheça suas boas práticas no processamento de dados –, fomentando a confiança do consumidor em seus produtos e/ou serviços e uma maior credibilidade social na gestão legítima de seus negócios.

Alguns fatores devem ser salientados como motivadores para o cumprimento da perspectiva preventiva do princípio *privacy by design*, partindo-se de um consenso quanto aos seguintes benefícios: (a) vantagem competitiva no mercado

contra outros projetos que não ofereçam respeito à privacidade dos dados pessoais do consumidor ou cliente; (b) maior confiança e lealdade do consumidor; (c) garantias de eficiência do processo e mitigação dos riscos como resultado do processamento de dados pessoais estritamente necessários aos fins comerciais previamente expostos; (d) minimização de riscos e, por conseguinte, dos custos derivados de violações à privacidade e segurança de dados; (e) a assunção de postura proativa na implementação e no desenvolvimento de produtos ou serviços em conformidade com os valores fundamentais da privacidade, autonomia, igualdade e devido processo legal; e, por fim, (f) os consumidores tratarão a privacidade de seus dados pessoais como questão de negócio, e não um problema de *compliance*.

O princípio PbD incentiva o foco na abordagem holística da privacidade, como um recurso de *design* das atividades e dos processos de uma organização por inteiro, a fim de obter um alto padrão de privacidade e proteção de dados, compatível com o argumento da internalização da regulação.

Nessa perspectiva, ele se torna fundamental na garantia de efetividade do direito à proteção de dados, devendo ser percebido como verdadeira norma implícita à concretização desse direito fundamental.

CONSIDERAÇÕES FINAIS

Conforme evidenciado ao longo deste artigo, na era digital marcada pelo domínio de novas tecnologias "inteligentes", são graves os riscos e as possibilidades de violação do direito à proteção de dados enquanto direito fundamental para a garantia da privacidade, da intimidade e, mesmo, da liberdade constitucionalmente protegida.

Em especial, o poder por trás da Inteligência Artificial está no acesso de uma máquina aos nossos dados pessoais. É essencialmente o que a IA faz: processa dados. Quanto mais dados coletados, armazenados e analisados, maior será a qualidade do algoritmo de aprendizado criado, para o bem ou para o mal. Quanto mais variáveis ou recursos, mais complexo e potencialmente preciso o modelo será. As empresas de tecnologia bem-sucedidas serão aquelas com o acesso a

dados precisos. Quanto mais dados coletados, mais eficazes, rápidos e precisos serão os algoritmos.

Assim, a Inteligência Artificial pode ser usada tanto para aumentar a eficácia quanto para mascarar os propósitos e métodos de manipulação. Se o fim é minar a autonomia e a participação democrática, a IA se torna uma arma indispensável. Uma nação consegue, hoje, abalar outra sem precisar invadir suas fronteiras físicas, mas o faz influenciando o comportamento dos seus cidadãos. Afinal, se todo poder emana do povo, as mídias sociais[44] permitem comandar a voz que elege os membros do corpo estatal.

A idéia básica que fundamenta o princípio do *privacy by design* é incorporar salvaguardas de privacidade em todas as etapas dos projetos desenvolvidos, desde a concepção. Não seria permitido desenvolver qualquer sistema, produto ou serviço, sem que a proteção da privacidade esteja no centro desse desenvolvimento. Inspira-se que as sociedades empresárias incorporem a privacidade em seus valores corporativos e empreguem o discurso também pragmaticamente, como um diferencial capaz de reforçar seu compromisso com a ética e a transparência.

No Brasil, ainda não se adotam expressamente os termos *privacy by design e privacy by default.* Contudo, a LGPD faz uso de conceitos similares, estabelecendo o dever de serem utilizadas medidas técnicas aptas a proteger os dados dos usuários contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação e/ou difusão. Ainda, estabelece que as organizações contem com meios de prevenir danos aos dados tratados e comprovem que atendem esses requisitos.

Partindo dessas premissas, conclui-se que o princípio da *privacy by design* deve ser concebido como um princípio fundante a partir do qual se deve construir todo o arcabouçou regulatório com vistas à garantia do direito fundamental à proteção

[44] Os gastos com mídia social secreta em campanhas de influência não são relatados e muitas vezes não são rastreáveis, de modo que interferências estrangeiras e ilegais não são regulamentadas, nem detectadas. Sociedades empresas de mídia social impõem restrições sobre quem pode acessar os dados do usuário, no entanto, ativamente compartilham dados entre si, geralmente sem consentimento expresso. Nessa toada, usuários se tornam "ratos de laboratório", submetidos a experimentos que afetam até as eleições.

de dados. Segundo seus postulados, a proteção de dados deve ocorrer durante o processamento destes de forma simultânea e integrada ao processo tecnológico, tanto na criação para o primeiro, quanto no aperfeiçoamento para o segundo.

Para tanto, compete ao agente responsável pelo tratamento o emprego de medidas técnicas e organizacionais adequadas à proteção dos dados, sem privar seu titular, contudo, do acesso a produto ou serviço a ser disponibilizado.

A primeira etapa rumo à superação desse aparente desafio para a *privacy by design* consiste na capacidade do agente de tratamento de dados atuar de forma preventiva e transparente no processo de concepção do novo produto ou serviço[45], incorporando a privacidade e a proteção de dados em todo seu ciclo de vida.

A inclusão do princípio PbD à ordem jurídica brasileira e à agenda de *compliance* para o desenvolvimento de novas tecnologias da informação e das comunicações (TIC), com foco no *technological enforcement*, deve conduzir a proteção proativa de dados a um patamar autoexecutável, em perspectiva preventiva, em que pese os desafios de ordens técnica, informacional, regulatória e mercadológica, que devem ser superados a partir de uma tutela promocional dos direitos da personalidade e das garantias fundamentais.

Sob essa perspectiva, em síntese, o presente estudo propõe a) que a proteção de dados deve ser compreendida como direito fundamental conectado aos direitos fundamentais à privacidade, à intimidade e à liberdade; e b) o princípio *privacy by design* deve funcionar como fonte irradiadora das diretrizes normativas regulatórias para a proteção dos direitos fundamentais acima citados, uma vez que concretiza a exigência de privacidade desde o projeto e o incentivo

[45] "A tutela da pessoa nem mesmo pode se esgotar no tradicional perfil do ressarcimento do dano. Assume consistência a oportunidade de uma tutela preventiva: o ordenamento deve fazer de tudo para que o dano não se verifique e seja possível a realização efetiva das situações existenciais." (PERLINGIERI, Pietro. **O direito civil na legalidade constitucional**. Tradução de Maria Cristina de Cicco. Rio de Janeiro: Renovar, 2008. p. 768). Também é pertinente o que, hoje, ensina Rose Meireles: "não basta a tutela abstencionista em face da personalidade. É a atuação concreta da liberdade que atribui valor preliminar, existencial e substancial ao problema da personalidade, a exemplo da liberdade de circulação, liberdade de instrução, liberdade de informação, liberdade de pensamento, liberdade de expressão." (MEIRELES, Rose Melo Vencelau. **Autonomia privada e dignidade humana**. Rio de Janeiro: Renovar, 2009. p. 59-60).

a empresas de tecnologia a serem mais conscientes quanto à privacidade dos titulares de dados.

Consideradas essas premissas, algumas medidas práticas e funcionais otimizam a concretização do princípio *privacy by design* e a proteção de dados: a) adotar modelos *opt-in* (ao invés dos ineficazes modelos *opt-out*) para o consentimento e a autorização do uso de dados pessoais, como a União Europeia faz à luz do GDPR; b) apoiar o desenvolvimento de novos mecanismos de incentivo a serviços favoráveis à promoção da privacidade; c) fomentar maior investimento em engenharia de privacidade, especialmente numa abordagem multidisciplinar por agências de fomento à pesquisa; d) promover os resultados dessas pesquisas por meio de formuladores de políticas públicas, pela mídia e por empresas de tecnologia; e) incluir componentes de suporte à privacidade em projetos de infraestrutura tecnológica; f) exigir transparência sobre os usos posteriores de dados do usuário; g) reforçar os mecanismos de responsabilização (civil, administrativa e criminal) por coleta, uso, manipulação e tráfico de dados sem a anuência do titular[46]; e f) reforçar o reconhecimento da propriedade, controle e autonomia sobre os dados pessoais por seus titulares.

Muitas dessas medidas podem ser realizadas adotando-se regulamentos semelhantes ao europeu e ao californiano. Todavia, o uso crescente de IA em um ecossistema de dados traz inúmeros desafios a serem superados pelos legisladores, tais como a) a necessidade de regras próprias que estabeleçam processos de privacidade articuláveis, padrões de segurança cibernética e procedimentos de desidentificação do anonimato[47]; b) a regulamentação da

[46] Preconiza o *Civil Liability Regime for Artificial Intelligence – European Added Value Assessment,* documento oficial emitido pelo Parlamento Europeu acerca das normas jurídicas positivados pelos países-membros sobre responsabilidade civil aplicável ao uso de Inteligência Artificial, que os danos pelos quais um causador pode ser civilmente responsabilizado incluem danos materiais emergentes, lucros cessantes e danos extrapatrimoniais decorrentes da violação da privacidade como direito da personalidade.

[47] LGPD, "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. §1º. A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. §2º. Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. §3º. A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais."

supervisão da agregação, fusão e análise de dados pessoais, bem como a utilização de *blockchain* e tecnologias em cadeia de título semelhante para permitir aos usuários se apropriarem de seus dados pessoais e monetizarem o seu uso; c) a promoção de maior regulamentação sobre auditoria de terceiros; e d) a exigência de supervisão e de responsabilidade pelo uso de algoritmos e qualquer informação relacionada à IA ou que tenha potencial de relacionar-se com uma pessoa, incluindo o dever de justificativa transparente para a tomada de decisões.

Conquanto tais proposições não resolvam os riscos da IA, fornecerão, ao menos, uma discussão mais aprofundada.

Ao final, vale trazer à baila a sábia advertência de Stefano Rodotá[48]: "ao lado da percepção, cada vez maior, dos riscos do progresso tecnológico, está a consciência da impossibilidade de deter tal progresso, mesmo este não se apresenta mais com prognósticos somente positivos. (...) cresce a distância entre o velocíssimo mundo da inovação tecnológica e aquele lentíssimo do planejamento socioinstitucional".

Daí a importância de uma regulação constitucionalmente adequada, que estabeleça um ambiente regulatório forte, comprometido com os direitos fundamentais da privacidade, da intimidade e da liberdade e que possa coibir que as novas tecnologias sejam utilizadas para fins escusos ou exclusivamente econômicos, de modo a afetar os ditames da democracia no Estado de Direito.

REFERÊNCIAS DAS FONTES CITADAS

BALDI, Vania. **A construção viral da realidade: ciberpopulismo e polarização dos públicos em rede.** Observatório Special Issue, (2018), 004-020 Disponível em: http://obs.obercom.pt/index.php/obs/article/view/1420/pdf. Acesso em 03 ago. 2019.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Zahar, 2001. CASTELLITTO, Anita L. Allen. **Understanding privacy: the basics**. Disponível

[48] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 41-42.

em: https://www.law.upenn.edu/cf/faculty/aallen/workingpapers/pli2007.pdf. Acesso em: 16 ago. 2020.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

CAVOUKIAN, Ann. **Privacy by design: the 7 foundational principles. Implementation and mapping of fair information practices.** Disponível em : https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf Acesso em: 16 ago. 2020.

CAVOUKIAN, Ann, CHANLIAU, Marc. **Privacy and Security by Design: A Convergence of Paradigms**. Disponível em: http://www.ipc.on.ca/images/Resources/pbd-convergenceofparadigms.pdf. Acesso em: 16 ago. 2020.

CENTODUCATTE, Rafael Avellar. **De 1984 a Westworld: a era dos dados e da vigilância**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/de-1984-a-westworld-a-era-dos-dados-e-da-vigilancia-01052020. Acesso em: 02 maio 2020.

CHEVALIER, Jacques. **O Estado pós-moderno**. Tradução de Marçal Justen Filho. Belo Horizonte: Fórum, 2009, p. 183-284.

COLLINS, Harry M. **Science studies and machine intelligence**. In: JANASOFF, Sheila; MARKLE, Gerald E.; PETERSEN, James C.; PINCH, Trevor. Handbook of science and technology studies. Londres: Sage Pub, 1995, p. 286-301.

EXPLAINED (EXPLICANDO). 2ª Temporada. 8º episódio: Código de Programação. Direção: Ezra Klein e Joe Posner. Produtores executivos: Ezra Klein, Kara Rozansky, Chad Mumm, Lisa Nishimura, Joe Posner, Jason Spingarn-Koff e Kate Townsend. Netflix. Data de lançamento mundial: 23 maio 2018. Disponível em: https://www.netflix.com/br/title/80216752. Acesso em: 22 ago. 2020.

FOUCAULT, Michel. **Vigiar e punir**. Tradução de Raquel Ramalhete. 20ª ed. Petrópolis: Ed. Vozes, 1999.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose. **Término do tratamento de dados**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: RT, 2019, p. 231-244.

LEITE, Luiza; DANTAS, Vitória. **Surgimento do contencioso de dados em 3, 2, 1...** Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/surgimento-do-contencioso-de-dados-em-3-2-1-13062020. Acesso em: 23 ago. 2020.

LEVITSKY, Steven; ZIBLATT, Daniel. **Como as democracias morrem**. Tradução de Renato Aguiar. 1ª ed. Rio da Janeiro: Zahar, 2018, p. 169-193.

MANHEIN, Karl M.; KAPLAN, Lyric. **Artificial Intelligence: Risks to Privacy and Democracy** (October 25, 2018). 21 Yale Journal of Law and Technology 106 (2019), Loyola Law School, Los Angeles Legal Studies Research Paper Nº. 2018-37. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273016. Acesso em: 30 jul. 2020.

MARRAFON, Marco Aurélio. **Hermenêutica, sistema constitucional e aplicação do direito.** 2 ed. Florianópolis: Emais, 2018.

_____. **Filosofia da Linguagem e limites da IA na Interpretação Jurídica.** Revista Consultor Jurídico, 2019. Disponível em: https://www.conjur.com.br/2019-jul-22/constituicao-poder-filosofia-linguagem-limites-ia-interpretacao-juridica. Acesso em 16 ago. 2019.

MEIRELES, Rose Melo Vencelau. **Autonomia privada e dignidade humana**. Rio de Janeiro: Renovar, 2009. p. 59-60.

MORAES, Maria Celina Bodin de. **LGPD: um novo regime de responsabilização civil dito proativo**. Disponível em: http://civilistica.com/lgpd-um-novo-regime-de-responsabilizacao-civil-dito-proativo/. Acesso em: 03 out. 2020.

ORWELL, George. **1984**. Tradução de Heloísa Jahn e Alexandre Hubner. Rio de Janeiro: Companhia das Letras, 2009.

PASQUALE, Frank. ***The black box society: the secret algorithms that control money and information***. Boston: Harvard University Press, 2016.

PERLINGIERI, Pietro. **O direito civil na legalidade constitucional**. Tradução de Maria Cristina de Cicco. Rio de Janeiro: Renovar, 2008. p. 768.

REGIS, Erick da Silva. **Linhas gerais sobre a Lei 13.709/2018 (a LGPD): objetivos, fundamentos e axiologia da Lei Geral de Proteção de Dados brasileira e a tutela de personalidade/privacidade**. Disponível em: https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/revistas-especializadas/rdpriv-103-janmar.pdf. Acesso em: 16 set. 2020.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROBL FILHO, Ilton Norberto. **Direito, intimidade e vida privada: paradoxos jurídicos e sociais na sociedade pós-moralista e hipermoderna.** Curitiba: Juruá, 2010.

SARMENTO, Daniel. **Aplicativos, criptografia e direitos fundamentais em tempos de erosão democrática**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica-14052020. Acesso em: 14 maio 2020.

SILVA, WELLINGTON CLAY PORCINO. **Tecnologia a serviço da segurança pública**. Disponível em: https://www.jota.info/coberturas-especiais/inova-e-acao/tecnologia-a-servico-da-seguranca-publica-17042020. Acesso em: 16 ago. 2020.

SHAW, Jonathan. **Artificial Intelligence and Ethics: Ethics and the dawn of decision-making machines**. Harvard Magazine. Disponível em: https://www.harvardmagazine.com/2019/01/artificial-intelligence-limitations. Acesso em: 19 ago. 2020.

TEGMARK, Max. **Life 3.0: Being Human in the Age of Artificial Intelligence**. New York: Alfred A. Knopf, 2017, p. 33-106.

THE GREAT HACK (PRIVACIDADE HACKEADA). Direção: Karim Amer e Jehane Noujaim. Produção: Karim Amer, Jehane Noujaim, Pedro Kos, Geralyn Dreyfous e Judy Korin. Netflix. Data de lançamento mundial: 26 jan. 2019. Disponível em: https://www.netflix.com/br/title/80117542. Acesso em: 8 ago. 2020.

THE SOCIAL DILEMMA (O DILEMA DAS REDES). Direção: Jeff Orlowski. Roteiro: Davis Coombe, Vickie Curtis e Jeff Orlowski. Netflix. Data de lançamento mundial: 09 set. 2020. Disponível em: https://www.netflix.com/br/title/81254224. Acesso em: 12 set. 2020.

UNIÃO EUROPEIA. **Prioridade: preparar a Europa para a era digital – capacitar as pessoas graças a uma nova geração de tecnologias**. Bruxelas. Disponível em: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-. Acesso em: 8 ago. 2020.

VED, Anamika. **Privacy and Security by design is a crucial step for privacy protection**. Disponível em: https://leastauthority.com/blog/privacy-and-security-by-design-is-a-crucial-step-for-privacy-protection/. Acesso em: 19 set. 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**. Harvard Law Review, v.4, n.5, 1890, p. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 06 set. 2020.

ZUBOFF, Shoshana. **The age of surveillance capitalism:** the fight for a human future at the new frontier of power. New York: Publicaffairs, 2019.