



Por que voltar a antigas categorias do constitucionalismo democrático na proteção de dados pessoais?

Why go back to ancient categories of democratic constitutionalism in protection of personal data?

Maria Clara Mendonça Perim^{1*}

REFERÊNCIA

PERIM, Maria Clara Mendonça. Por que voltar a antigas categorias do constitucionalismo democrático na proteção de dados pessoais?. *Revista da Faculdade de Direito da UFRGS*, Porto Alegre, n. 58, p. 325-346, ago. 2025. DOI: <https://doi.org/10.22456/0104-6594.144010>.

RESUMO

Este artigo tem por objetivo discutir as qualidades do Direito em frente ao desafio da proteção de dados pessoais, a partir da transformação disruptiva da inteligência artificial (IA). Para tanto, sintetiza os atributos da IA e o fato de que máquinas têm recebido o poder de tomar decisões públicas sem transparência, controle ou responsabilidade. A seguir, discute se o Direito está apto a oferecer respostas adequadas a esse problema, pontuando as seguintes dificuldades: a) a velocidade da virada tecnológica dificulta que o sistema jurídico apresente respostas tempestivas, pois a produção do Direito requer amadurecimento; b) o desconhecimento do que se pretende regular torna difícil a escolha pública normativa e suas justificações racionais; c) a indefinição sobre os campos da gestão de dados pessoais, se pertencem à esfera pública ou à vida privada, gera embaraços para sua regulação pelo Direito, já que este ainda adota a lógica dessa dicotomia tipológica; d) as noções de territorialidade, jurisdição, soberania e o paradigma da produção do Direito a partir das ideias de Estado e de Constituição dificultam a solução de problemas transnacionais; e) os múltiplos formatos de esferas públicas em redes complicam a adaptação da metodologia da deliberação pública legislativa aos seus mecanismos comunicativos. Em que pese tais limites, as concepções de Estado de Direito, Democracia e Justiça permanecem úteis à proteção de dados pessoais, pois representam um aprendizado histórico antitético ao arbítrio e eficaz na proteção dos valores de segurança, igualdade e liberdade.

PALAVRAS-CHAVE

Direito; dados pessoais; constitucionalismo democrático.

ABSTRACT

This article aims to discuss the qualities of the Law in light of the challenges of protecting personal data, specially against the disruptive transformation of artificial intelligence (A.I.). In order to do so, we synthesize the attributes of A.I and the fact that machines have been given the power to make public decisions without transparency, control or responsibility. In sequence, we discuss if the Law is fit to offer adequate responses for this problem, pointing out the following difficulties: a) the speed of technological changes makes it difficult for the legal system to present timely responses, since the production of Law requires maturation; b) the lack of knowledge of the regulated object complicates public normative choices and its rational justifications; c) the undefinition if personal data belongs to Private or Public Law creates obstacles for legal regulation, since this dichotomous logic is still used in legal study; d) the notions of territoriality, jurisdiction, sovereignty, and paradigms of Law production in the current context of State and Constitution hinder the finding of solutions for transnational problems; e) the multiple formats of the public sphere in networks complicate the adaptation of

^{1*} Doutora em direito público pela Universidade Estadual do Rio de Janeiro (UERJ). Linha de pesquisa: direito constitucional contemporâneo, processo constitucional, democracia, orçamento público, governança e instituições. Mestre em Saúde Coletiva - Políticas Públicas pelo Programa de Pós-Graduação em Saúde Coletiva da Universidade Federal do Espírito Santo. Promotora de Justiça no Ministério Público do Estado do Espírito Santo, com atuação na defesa do patrimônio público. Coordenadora do Fórum de Integridade e Participação Social dos Poderes Legislativos Municipais no Espírito Santo. Integra o Grupo de Trabalho sobre Corrupção e Governo Aberto da Rede Brasileira de Estudos e Práticas Anticorrupção da Transparência Internacional.





the methodology of public legislative deliberation to methods of communication. In spite of such limitations, the concepts of State of Law, Democracy and Justice remain useful for the protection of personal data, since they represent a historical learning against arbitrary decisions and are effective in protecting values related to safety, equality and freedom.

KEYWORDS

Law; personal data; democratic constitutionalism.

SUMÁRIO

1. Introdução. 2. Será possível proteger dados pessoais a partir dos mesmos paradigmas do Direito? 3. Como o Direito e as antigas categorias do constitucionalismo democrático podem ajudar? 4. Conclusões. Referências. Dados da publicação.

1 INTRODUÇÃO

A verdade é que tudo mudou. A vida não é mais como era antes e talvez nunca mais volte a ser. Trata-se de uma nova perspectiva de realidade tecnológica avassaladora que carrega consigo novas formas de agir, tumultua sentimentos e altera visões de mundo.

Os dados pessoais estão no centro disso e passaram a ser um bem valiosíssimo. Chirita (2018) argumenta que se trata da nova moeda. É a partir dessa propriedade que se produzem consumo, política e afetividades. O fenômeno tem ganhado maior escala a partir da revolução tecnológica da inteligência artificial (IA).

A IA é um campo da ciência que produz máquinas capazes de simular o raciocínio e o aprendizado humanos, inclusive para analisar dados em uma escala superior à capacidade de pessoas. As finalidades do uso da IA são diversas: produzir estatísticas, fazer projeções, categorizar objetos etc. Para variadas funções, a IA se alimenta dos dados pessoais e retroalimenta sensações humanas.

Neste novo tempo, todos são absorvidos por um processo de sociabilidade com o qual ainda não se sabe lidar. Nem se sabe aonde vai chegar. Há alertas sobre riscos. Em 2009, Rodotà mencionou a realidade perturbadora do fim da privacidade. De certa forma, há uma redução na autonomia das pessoas, quando submetidas aos estímulos da IA.

Diante desse cenário, evidencia-se a vulnerabilidade dos consumidores, que consiste na condição de desigualdade em que eles se encontram em relação ao fornecedor, seja por assimetria de informações, de conhecimentos técnicos, de poderio econômico, seja por qualquer outro motivo que torne desproporcional a relação de consumo. É o que acontece, por exemplo, diante do manejo da IA para estimular aquisição de bens e serviços a partir de um conhecimento prévio produzido na análise de preferências dos consumidores.





Para além da vulnerabilidade do consumidor, face a face aos gigantes da tecnologia, parece evidente que a IA traz danos à democracia – ao menos na dimensão de eleições livres, justas e iguais – e a direitos fundamentais.

A danosidade da gestão temerária de referências pessoais evidenciou-se após o vazamento de dados do *Facebook*, ligado ao uso dessas informações pela *Cambridge Analytica* para a campanha de Trump à presidência dos EUA (Valente, 2018). Porém, esse é apenas um dos casos de repercussão internacional relacionados com o acesso indevido de informações².

Visando a compreender esse fenômeno, Manheim e Kaplan (2019) realizaram uma análise conceitual da IA para qualificá-la como uma tecnologia disruptiva capaz de *extrair inteligência* (detecção, processamento e resposta da informação) de *dados não estruturados*, em velocidades e escalas mais altas do que o raciocínio humano.

Segundo os autores, a IA gera *perfis comportamentais*, a partir de conjuntos de dados, os quais são captados e compartilhados em fontes dispersas (plataformas de mensagens, métodos de vigilância e Internet das Coisas³). Depois, esses dados são mesclados, organizados e correlacionados para revelar tudo sobre as pessoas de forma granular: hábitos, religião, preferências políticas, comportamentos etc. Esse conjunto permite:

- a) amplificar a captação de grandes quantidades de dados pessoais (força vital da IA – extração de dados é o negócio principal da rede), o que corrói a privacidade;
- b) tornar possível reidentificar dados anônimos, o que expõe detalhes íntimos de pessoas e governos e suprime o anonimato;
- c) antecipar as tomadas de decisão e prever suscetibilidade a gostos e assuntos a partir dos perfis comportamentais, o que viabiliza manipular a vontade de indivíduos a ponto de terem como suas decisões que, na verdade, são guiadas pelos algoritmos;
- d) produzir resultados baseados em raciocínios incognoscíveis, o que gera opacidade, já que existe um “aprendizado da máquina” que depende cada vez menos da programação humana e sim da capacidade de um algoritmo usar métodos estatísticos para “aprender” com os dados conforme eles progridem⁴.

² Há outros escândalos envolvendo a exposição das contas dos correntistas digitais do Banco Inter (Conecta Já, 2020) ou o descomunal vazamento de dados na rede hoteleira Marriott, que resultou no acesso indevido a informações pessoais de cerca de 500 milhões de hóspedes no mundo todo, inclusive a seus dados sobre *cartões* de crédito e passaportes (Gallas, 2019).

³ Coleta de dados brutos de pessoas em ações físicas e comunicações.

⁴ A máquina encontra padrões nos dados não estruturados a partir dos quais ela modela o conhecimento.





Por isso, o direito à autodeterminação informativa tem sido considerado como um direito fundamental autônomo que merece proteção transconstitucional. Isso é refletido em muitos documentos, como a Carta dos Direitos Fundamentais da União Europeia (União Europeia, 2000).

Contudo, os perigos ainda estão incontroláveis. Em que pese todo o leque de entendimentos transnacionais em torno da proteção de dados, os caminhos para sua efetividade continuam pouco explorados. Máquinas têm recebido o poder de tomar decisões públicas e fazem isso sem transparência, controle ou responsabilidade (Manheim; Kaplan, 2019).

Nesse quadro, mesmo diante da evolução regulatória dessa matéria em nível mundial, há algum consenso de que os atuais paradigmas jurídicos – ou ao menos a forma como se efetivam – são insuficientes para lidar com o problema da proteção de dados.

O Regulamento Geral de Proteção de dados (GDPR) tem sido o modelo regulatório mais importante dessa geração para a política de proteção de dados (Hoofnagle; Sloat; Borgesius, 2019). No Brasil, a Lei Geral de Proteção de Dados é uma conquista, mas sobrevivem a ela vácuos importantes, seja no campo da sua própria concretização, seja em relação ao déficit de normas em outras áreas, como o tratamento de dados em investigações de ilícitos e as *fake news*.

Será que o Direito é capaz de dar conta das complicações derivadas da IA? Será que está apto a oferecer respostas adequadas aos embargos que a difusão de dados pessoais pode causar? Se sim, será que esse é um Direito de uma nova dimensão – um pensar para o futuro – ou a resposta para a proteção de dados ainda está nas antigas conquistas do constitucionalismo democrático?

Essas são interrogações de difícil resposta, mas o dilema pode não ser tão inequívoco. Talvez haja um espaço muito útil entre a limitação do Direito e a sua potestade em mudar a realidade. As respostas estão em algum lugar entre o sim e o não.

2 SERÁ POSSÍVEL PROTEGER DADOS PESSOAIS A PARTIR DOS MESMOS PARADIGMAS DO DIREITO?

Por certo, o tratamento de dados é um assunto multidisciplinar, porque se conecta a dinâmicas sociais, políticas e normativas. Verdade seja dita, o manejo de dados pessoais parece afetar diversas estruturas que funcionam sob lógicas diferenciadas. Para fins deste





artigo, considera-se dado pessoal qualquer informação relacionada com a pessoa natural identificada ou identificável, conforme delimitado pela Lei n.º 13.709/2018.

O estudo de Chirita (2018) se baseou nas três principais empresas digitais – Google, Facebook e Microsoft – para demonstrar que o *big data* favorece a discriminação de preços. Mas não apenas isso, porque também revelou que há propósitos inter-relacionados na coleta e processamento de categorias de dados pessoais. As conclusões reforçam a preocupação de que a manipulação de dados de usuários tenha se tornado, agora, uma *norma social*.

Sobre o conceito de *norma social*, o sentido aqui empregado para compreender o fenômeno da manipulação de dados é *descritivo*, ou seja, aquele que considera uma norma social como tradição que é amplamente seguida pela sociedade e praticada pelos seus membros.

Não desconhecemos que a concepção de *norma social* como hábito foi adequadamente contestada pela teoria do Direito. Nesse sentido, Hart (2009) já compreendia as *normas sociais* como preceitos que impõem obrigações de conduta e são tratadas no discurso de uma sociedade como um elemento do sistema moral de grupos que exercem pressão para sua observância. Logo, norma social é mais do que um mero hábito.

Apesar da relevância de distinções conceituais, para fins da discussão da conexão da normatividade *vs.* dados pessoais, a noção descritiva de *norma social* é suficiente para demonstrar que o manejo de dados se tornou uma realidade esperada, mesmo que não haja propriamente uma pressão moral para que as pessoas realizem essas atividades.

A transmutação de uma *norma social* implica alterações na lógica estrutural de sistemas de convivência humana. Logo, é uma fantasia pensar que o Direito pode resolver todas as suas questões, já que ele não domina totalmente as essencialidades do mundo da vida.

Apesar dessa insuficiência, o Direito é um sistema que normatiza fatos relevantes para a sociedade. É intrínseco ao Direito conferir previsibilidade às ocorrências sociais e às consequências derivadas de condutas humanas. É por isso que, embora não domine tudo, o Direito transita em todas as formas de relações sociais e as modula, performa e orienta.

A origem da regulamentação da proteção de dados remonta à década 1960, com a proposta de criação do *National Data Center* pelo governo dos Estados Unidos. O projeto consistia em um gigantesco banco de dados concentrando as informações pulverizadas em sistemas da administração pública sobre os cidadãos. Após acirradas discussões sobre a ameaça às liberdades, o governo norte-americano abortou a ideia (Doneda, 2011).





No final da década de 1970, inicia-se um novo momento da proteção de dados baseado na autodeterminação informacional. Zanatta (2018) o caracteriza pela posituação de direitos individuais de liberdade, com ênfase na contratualização do consentimento, nas garantias de informação, lealdade e fidedignidade. Ou seja, um rol de garantias que gira em torno do domínio do indivíduo sobre seus dados pessoais e a liberdade de deles dispor.

Atualmente, a pretensão regulatória encontra empecilhos. A crítica central aos limites do modelo da autodeterminação está na vulnerabilidade da pessoa em frente aos gigantes da tecnologia e na consequente deficiência do consentimento como freio efetivo à difusão desregrada de informações pessoais. Na prática, o usuário é levado a aceitar as políticas por adesão, sem que haja verdadeiramente possibilidade de reflexão sobre elas (Chirita, 2018).

Assim, têm surgido novas alternativas com vistas a aumentar a proteção de dados, como é o caso da risificação. Essa metodologia pretende ultrapassar a perspectiva da autonomia como estratégia central para mitigar ameaças a liberdades a partir da gestão de riscos.

Alguns autores defendem o processo da risificação regulatória porque ele supera a tradicional concepção bilateral entre o sujeito de direito e o controlador e traz perspectivas mais coletivas no tratamento dos dados. São diversas as suas vantagens, inclusive sob a ótica da precaução e, inequivocamente, a gestão de riscos agrega proteções (Quelle, 2016).

A despeito disso, isoladamente, a risificação é insuficiente para excluir a regulação do Direito na proteção contra a ameaça ou dano a direito individual por violação de dados pessoais. Precipita-se quem defende a abolição (e não a adaptação) da metodologia da proporcionalidade na proteção de dados.

Sobre o tema, estão com a razão Manheim e Kaplan (2019) quando incluem, na lista de propostas para uma regulação eficiente da proteção de dados, diretrizes que conjugam perspectivas diversificadas e não se limitam a focar apenas uma única via de proteção.

Para eles, a proteção contra os riscos da IA inclui os seguintes princípios: privacidade, responsabilidade (*design*, processo e transferências ilícitas de dados), redução de riscos, transparência, controle e segurança, consentimento (*opt-in*) e justificativas, limites de compartilhamento, definição de finalidade, restrição de decisões automatizadas em direitos humanos, inclusão da privacidade no *design* e política de antitruste (Manheim; Kaplan, 2019).





É preciso reconhecer que há avanços nas legislações de proteção de dados ao redor do mundo e, particularmente, o GPDR tem sido considerado o mais exemplar. Hoofnagle, Bart Van Der e Borgesiusc (2019) elencam oito características essenciais do GPDR:

- a) incentivo à governança de dados pelas empresas;
- b) equiparação da privacidade aos níveis das leis que as empresas “levam a sério” (antitruste e anticorrupção) diante da gravidade de penalidades e dos procedimentos de segurança e notificação de incidentes;
- c) exigência de proteções e compromissos de prestadores de serviços e terceiros em limites contratuais ao uso de dados transmitidos em cadeia;
- d) elevação estrutural dos funcionários de privacidade dentro de empresas, conferindo-lhes atribuições que transcendem a lealdade com a empresa e que implicam o relato do que realmente acontece;
- e) qualificação do consentimento para superar a usual baixa voluntariedade do “pegar ou largar”;
- f) incentivo às ações humanas nos círculos de tomada de decisões;
- g) favorecimento de relacionamentos primários entre titulares de dados e empresas, mitigando a força dos vendedores online indiretos.
- h) previsão de período de experimentação o que, desde sua aplicação em 2018, tem levado a auditorias e exames criteriosos sobre as formas de usos de dados.

Indubitavelmente, o GPDR tem servido de parâmetro para legislações em diversos países. Por outro lado, remanescem vácuos normativos importantes, seja porque ainda não há uniformidade na adoção de suas premissas, seja porque há muitas controvérsias sobre a efetividade desses mecanismos e a força de reação das empresas de tecnologia.

Essas dúvidas controvertem sobre a aptidão do Direito para lidar com o problema. Logo, é importante definir quais são as dificuldades do Direito nesse campo, para além daquelas que são usualmente discutidas em relação aos limites do consentimento e da autodeterminação informacional. Identificamos cinco pontos essenciais da questão.

A *primeira* limitação do Direito diz respeito à condição sempre defasada da legislação em matéria de tecnologia. A velocidade da virada tecnológica dificulta que o sistema jurídico acompanhe em tempo real as demandas desse tema.

De fato, a produção do sistema jurídico funciona na lógica da tradição e da deliberação democrática e, assim, tanto os processos legislativos como também a consolidação do *common law* requerem desenvolvimentos longos. Na formação de maiorias





legislativas e na interpretação permanente do costume pela jurisprudência, produzir Direito leva tempo.

No atual cenário disruptivo, não é simples gerar leis e políticas regulatórias. Ainda que se admita certa dose de celeridade na produção legislativa pelas majorias – o que permitiria resposta tempestiva do sistema jurídico aos problemas tecnológicos –, há dificuldades reais em realizar deliberações efetivamente democráticas e inclusivas.

Ryfe (2005) aponta que os desafios práticos de deliberações envolvem no mínimo três momentos: a organização do encontro, a prática da deliberação e o produto da conversa. Esses desafios são mais agudos na agenda da proteção de dados, porque discussões importantes (Quem participa da deliberação? Qual a metodologia desse debate? A quem se vinculam seus resultados?) são complicadas diante dos novos ambientes das redes sociais. Não é nada fácil definir afetados, mediar diálogos ou legitimar soluções. Nesse novo cenário, apenas planejar a deliberação e entender suas novas dinâmicas já delongam.

Como ainda não existe uma teoria para uma deliberação funcional que envolva as recentes formas de interação comunicativa, vale o modelo clássico das democracias liberais, no qual o fluxo para elaboração de leis pressupõe uma série de procedimentos de tramitação legislativa entre iniciativas diversas, estruturas bicamerais, objeções de minorias e regras de veto. Todo esse pacote faz o Direito ser como um filho a ser gestado com paciência.

Para mais, o puritanismo positivista está superado. Dworkin (2014) está com a razão no ponto em que vê o Direito como uma cadeia entremeada pela tradição e por complexidades que lhe agregam diferentes tons, ou seja, como uma permanente tentativa de garantir certa integridade entre o passado e o futuro, em idas e vindas de proposições jurídicas.

Dessa forma, a interpretação do Direito nada tem de unívoca e a sua fonte não é exclusiva dos legisladores. Trata-se de uma elaboração multifacetada entre poderes e povo que, diga-se de passagem, nem sempre pode ser romanceada, porque é, em regra, conflituosa. Isso a qualifica como um processo bastante imbricado e não imediatista.

Intrinsecamente considerado, o dissenso não é um problema. É da essência do constitucionalismo democrático que desacordos interpretativos são condições normais para o próprio desenvolvimento do Direito. Se cabe ao constitucionalismo democrático reconciliar interesses conflitantes, há espaço para positividades, até no *Backlash* (Post; Siegel, 2007).

Todavia, é preciso reconhecer que a interpretação do Direito é um processo de muitas mãos – de atores da justiça e da sociedade – que ocorre por mecanismos complexos. As reivindicações sobre o significado da Constituição são dinâmicas, históricas e nada





sincrônicas. Logo, o Direito não é uma realidade posta em um momento específico. Ele leva tempo, seja pela via da tradição, seja pelos avanços e retrocessos de conflitos.

Em síntese, a demora é um problema para o Direito na proteção de dados, uma vez que os processos de amadurecimento normativo dos pontos sensíveis desse tema não acompanham a rapidez da evolução tecnológica.

O *segundo* obstáculo para o Direito na proteção de dados – que em parte decorre do primeiro – é a imponderabilidade do que se pretende regular. É difícil conferir previsibilidade ao imprevisível.

É um pressuposto das escolhas públicas normativas que se saiba exatamente de que trata essa regulação: qual o seu objeto? Por que deve ser regulado? Quem são os afetados e quais os seus interesses? Quais são as consequências em deixar as coisas como estão (fora do campo do Direito)? Qual o valor a ser protegido pela norma?

Se essas são perguntas cruciais para desenvolver a norma jurídica, é um problema para a regulação da proteção de dados que seus *feedbacks* não sejam claros. Apesar dos esforços para compreender processos da inteligência artificial, eles não são transparentes sobre como funcionam e quais direitos e valores podem impactar. Na medida em que são nebulosos os fatos e indefinidas suas consequências, a regulação pelo Direito é ineficaz.

Por exemplo, a Internet das Coisas é a evolução de uma rede de *computadores* interligados para uma rede de *objetos* interligados. Não se trata de uma mera extensão da Internet, mas de uma rede complexa de sistemas independentes e interoperáveis que são implementados por diferentes modos de comunicação (Weber, 2009). Trata-se da possibilidade de uma rede de *coisas* controlar remotamente os objetos e apreender informações a partir deles.

As pessoas, em geral, não conhecem o que é e como funciona a Internet das Coisas. Não se sabe ao certo quais são as possíveis consequências de seu desenvolvimento. De mais a mais, os *objetos* interligados pela Internet das Coisas são usados por pessoas e é, no mínimo, uma imprecisão terminológica a denominação objetiva sobre o controle de algo que, ao fim e ao cabo, diz muito sobre *sujeitos*. Afinal, em que terreno estamos pisando?

Outro exemplo é que as opacidades transitam na *Dark* e na *Deep web*. A *Deep Web* é a parte da Internet que não se encontra registrada e é inacessível pelos motores de busca tradicionais. Dentro da *Deep Web*, há websites que só podem ser consultados por softwares específicos (p. ex., o *Tor*), que permitem preservar a identidade dos usuários.





Por sua vez, os espaços de *Dark Web* são frequentemente utilizados para ilícitos, mas funcionam também para garantir privacidade e proteger comunicações pessoais por várias razões que vão desde questões íntimas até resistências políticas. Essas novidades, dentre as quais estão *Iot*, *Deep Web*, algoritmos e *fake news*, é um mundo oculto, ao menos para as “maiorias” que supostamente deveriam deliberar sobre sua regulação jurídica.

A proteção de dados ainda transita no campo do desconhecido. Portanto, a segunda grande dificuldade do Direito em regulamentá-la é precisamente o fato de os cidadãos, e quiçá as autoridades públicas, não conhecerem o funcionamento desse mundo digital. Sabe-se pouco, o conhecimento é desigual e não compartilhado, além de contaminado por imaginários. Essa imprecisão redundava em inviabilizar justificações racionais.

A abordagem aqui é diferente daquela feita por Manheim e Kaplan (2019). Eles apontam que a IA é opaca porque não é possível definir como a máquina pensa, ou seja, qual a sua lógica. De fato, se a IA produz raciocínio por si só, ou seja, a partir dos dados e não da programação, perde-se o controle sobre a tomada de decisão. Desconhecidas as “razões” da máquina, a decisão não é passível de ser debatida.

A advertência sobre essa opacidade é correta, mas não é apenas a lógica da tomada de decisão da máquina que é incógnita. Há muitos mistérios em torno de toda essa questão e poucas esperanças de garantia de previsibilidade em curto espaço de tempo.

Nesse quadro de incertezas, o Direito tem dificuldade em organizar o discurso racional e suas justificações em um bloco de possíveis decisões a serem tomadas e suas respectivas vantagens e desvantagens. Verdadeiramente, o Direito não tem tido facilidade sequer em definir quais seriam exatamente as visões de mundo a serem escolhidas.

Acontece que essa elaboração de fundamentações é necessária para o que Barcellos (2016) denomina *o devido procedimento de elaboração normativa*, composto por um conjunto de “[...] deveres de natureza procedimental que exigem a apresentação pública de uma justificativa contendo razões e informações acerca das proposições normativas”.

A *terceira* dificuldade que o Direito enfrenta na proteção de dados está na indefinição sobre os campos a que pertencem as novidades da gestão de dados pessoais, ou seja, na dúvida sobre se essas atividades são do âmbito da esfera pública ou da vida privada.

Com efeito, a IA interconecta áreas bastante diversificadas. Há uma intersecção importante do tratamento de dados com o mundo empresarial, com as relações consumeristas e até mesmo com a comunicação íntima entre pessoas. Isso tende a qualificar e dimensionar o tratamento de dados pessoais para o âmbito da vida privada.





De fato, a tendência do modelo liberal e procedimentalista do Direito é segregar as esferas públicas e privadas e, como dizia Saldanha (1983), há uma série de componentes decisivos que diferenciam a vida privada da vida pública em diversos planos, entre *praças* e *jardins*.

O problema é que a noção de publicidade é bastante afetada pela disruptiva transmissão de dados pessoais e instalou-se uma confusão sobre os riscos para a permanência dessa antiga dicotomia. É possível que o Direito enfrente dificuldades em lidar com isso.

A evidente correlação da proteção de dados com a privacidade, com a influência dos algoritmos nos processos eleitorais, com a formação de blocos populistas e com outros temas do Poder Público (p. ex., as estratégias antiterroristas e as ações e serviços de Inteligência) caracteriza a matéria como de direito público. Se dados pessoais suscetibilizam justiça, democracia e o funcionamento das instituições, estão no âmbito do Direito Público.

Sempre coube ao Direito distinguir entre *esfera pública* e *esfera privada*. É preciso lembrar que o apagamento dessas balizas e a supressão de esferas privadas marcaram o totalitarismo (Arendt, 2012). À vista disso, é recomendável que essas questões sejam discutidas pelo Direito. No entanto, definir o que é a ordem pública, onde ela termina e onde começa a ordem privada em redes sociais, apresenta nuances ainda inexploradas.

O ponto de definição do tratamento de dados nas categorias do *público* ou do *privado* remete a uma *quarta* dificuldade do Direito, que diz respeito às noções de *territorialidade*, *jurisdição* e *soberania*.

Por mais que as concepções de direitos fundamentais tenham expandido suas proteções a um nível transnacional, remanesce o paradigma da produção jurídica a partir das ideias de Estado e de Constituição. A histórica concepção de Estado de Direito afirmou a igualdade perante a lei e viabilizou as primeiras proteções dos direitos fundamentais.

A transnacionalização⁵ reflete sobre novas bases de afirmação dos direitos fundamentais e, nesse passo, sugere analisar se não apenas a jurisdição, mas também outros paradigmas originários de concepções do estado moderno – como povo e território – estão aptos a garantir direitos nessa quadra da história. Os desafios da paz, da igualdade estrutural entre pessoas e povos e, agora, da proteção de dados, reclamam multifacetadas interconexões.

Quando o que se quer é regular de forma eficiente o tratamento de dados em um ambiente de transferências transnacionais e preponderância de grandes empresas, o apego às raias estatais é um contratempo. Em verdade, já se constatou que as legislações locais podem

⁵ Sobre o tema, vide: Galindo (2006) e Neves (2018).





gerar confusões e inseguranças jurídicas e, ademais, dificilmente produzirão, por si sós, resultados satisfatórios em termos de exequibilidade.

Nesse sentido, a regulação da IA nos Estados Unidos é frágil porque fragmentada, setorial e reduzida à autorregulamentação da indústria (Manheim; Kaplan, 2019). Esses são defeitos perfeitamente transportáveis para as legislações estatais. Não à toa, a União Europeia tem sido mais bem-sucedida. Por isso, é um problema para o Direito, na proteção de dados pessoais, a vinculação de regulações a conceitos muito estanques de Estado, soberania e jurisdição.

O último ponto e a *quinta* dificuldade do Direito em garantir proteção aos dados pessoais (sem dúvida há muitos outros) é a metodologia da deliberação pública legislativa que pressupõe a sua legitimação intrínseca.

Mais do que administrar esse pacote de indefinições tipológicas na regulação do tratamento de dados pessoais, apresenta-se para o Direito a tarefa de lidar com múltiplos formatos de esferas públicas em redes, com suas lógicas, interferências e dinâmicas, pois pertence ao campo do Direito a procedimentalização da democracia deliberativa.

Há muito se discutem procedimentos que viabilizam a formação da vontade das maiorias para legitimar a norma jurídica. A gênese disso é que a teoria contratualista se fundou na ideia de vontade popular como fonte do Direito, ainda que com resguardo da intangibilidade dos direitos fundamentais. Simultaneamente, o Direito deve prever procedimentos para a formulação da deliberação democrática e legitimá-los.

Sem adentrar na discussão entre visões procedimentalistas e substancialistas do Direito, é basilar que a Constituição (e o Direito) tenha um papel mínimo na definição legal sobre a regra do jogo político, ou seja, sobre aqueles procedimentos que garantem a origem democrática para produzir o Direito legítimo, a partir da interação social discursiva (Habermas, 2003).

A erupção da IA subverte a lógica dos canais tradicionais da democracia deliberativa e suscita questões sobre quais seriam os procedimentos requeridos para a legitimação da sua própria regulação. Afinal, como deve ser uma esfera pública apta a obter soluções para o problema da proteção de dados pessoais? Quais seriam os procedimentos e padrões morais mínimos a serem adotados nesse âmbito?

Tudo isso indaga se os antigos paradigmas do sistema jurídico, ou até mesmo a própria ideia de Justiça, são suficientes para responsabilizar-se pela proteção de dados pessoais. Afinal, concepções, como proteção jurisdicional de direitos fundamentais, soberania





estatal popular e democracia deliberativa, retrucam adequadamente os riscos da IA e do indiscriminado tratamento de dados?

3 COMO O DIREITO E AS ANTIGAS CATEGORIAS DO CONSTITUCIONALISMO DEMOCRÁTICO PODEM AJUDAR?

O atual sentimento de impotência do Direito para enfrentar o gigante da proteção de dados é real. Esse medo é uma crise, porque ele produz a sensação generalizada de que as antigas premissas de solução de problemas são atualmente insuficientes para resolvê-los. Como questionado por Rodotà (2009), será que o conceito da proteção de dados abriu uma nova era para a proteção de liberdades realmente voltadas para o futuro?

A humanidade caminha entre opções labirínticas para as quais as antigas categorias do Direito parecem não indicar saídas. Concepções como *Estado de Direito*, *Democracia* e *Justiça* ainda não decifram adequadamente o que se apresenta no plano virtual.

Quando a crise acontece, a tendência humana é buscar algo novo que facilite a solução dos problemas. Esse movimento pode representar a ruptura com aquilo que se considera velho, obsoleto e superado. Ultrapassada a idealização do progresso como algo linear e evolutivo, não se pode mais negar a possibilidade de sepultamento de visões de mundo.

Dizia Kuhn (2013, p. 201) que, assim como as revoluções científicas se iniciam com a percepção de que o paradigma existente deixou de funcionar adequadamente para a solução de problemas da ciência, as revoluções sociais e políticas “[...] iniciam-se com um sentimento crescente, com frequência restrito a um segmento da comunidade política, de que as instituições existentes deixaram de responder adequadamente aos problemas”. Este é um tempo de novidades e anomalias. Talvez até seja um tempo de efetiva crise e, verdadeiramente, como acrescenta o autor, “[...] quando mudam os paradigmas, mudam com eles o mundo” (p. 201).

Mas, pensando bem, há um aprendizado histórico que é simplesmente antitético às idas e vindas de arbítrios para os quais não se deseja voltar. Logo, é preciso não temer o novo, mas ter cautela para não esquecer o que houve, porque “[...] a tentação de escrever a história passada a partir do presente é generalizada e perene” (Kuhn, 2013, p. 234), mas pode ser perigosa.





Portanto, ainda que não se cultive a fantasia de que os clássicos padrões do Direito estão aptos a resolver todas as questões, é necessário não descuidar das lições aprendidas pela humanidade. O caminho é reconhecer os limites do Direito em suas tradicionais modelagens, mas também enxergar em que ele pode ajudar a resolver as batalhas atuais.

Isso requer ver além do Direito Positivo e viabilizar o diálogo do factual com categorias filosóficas, como são os conceitos de Estado de *Direito*, de *Democracia* e de *Justiça*. É urgente compreender como tais concepções interagem com o presente e de que forma elas devem influenciar as contemporâneas soluções para a proteção de dados pessoais.

Não são obsoletas as diretrizes do Direito para resolver os problemas da difusão de dados pessoais. A despeito da obviedade, a tese de que o Direito persiste como um remédio proveitoso contra os riscos dessas inovações significa prescrever o uso das concepções elementares de Estado de *Direito*, *Justiça* e *Democracia* como inafastáveis nesse campo.

Isso não é singelo porque implica dizer que os paradigmas do Direito se mantêm em meio à crise que assolava antigos costumes. Consequentemente, eles devem orientar descobertas em forma e substância e isso equivale afirmar que o que está acontecendo agora não é totalmente novo e voltado para o futuro. A valer, não se trata de substituir a privacidade física pela proteção de dados de um corpo virtual, porque as opressões que podem se apresentar terão contornos mundanos e podem se manter corpóreas.

Sendo assim, o fundamento nuclear para o retorno às clássicas categorias do Direito na proteção de dados pessoais está na constatação de que a difusão de dados pessoais gera perigos que, se vistos abstratamente, são semelhantes àqueles que a humanidade já enfrentou tendo o próprio Direito como aliado. Com remodelados formatos e dinâmicas, a difusão desprotegida de dados pessoais hostiliza *liberdade*, *igualdade* e *segurança*.

O evento do 11 de Setembro abriu espaço para a condenação da privacidade para fins de combate ao terrorismo. Houve três desdobramentos: a) redução de garantias de transferências de dados; b) reduções de salvaguardas à privacidade nos setores de negócios; e c) multiplicação de ferramentas tecnológicas de classificação, seleção, ordenação e controle de indivíduos. Essas consequências implicaram colocar a nau da proteção de dados em uma deriva à qual as autoridades não deram conta de responder (Rodotà, 2009).

Nessa virada de descontrole, a *liberdade* é posta em xeque em face à perda da autonomia na tomada de decisão; a *igualdade* tropeça na formação das bolhas de algoritmos que afastam a diferença da convivência social e impulsionam políticas binomiais; e, finalmente, a *segurança* se desfaz na imprevisibilidade das consequências de tudo isso.





Se relembarmos a história, perceberemos que foram precisamente essas ameaças que levaram à modelagem do constitucionalismo e da democracia. A afluência das ideias de *Estado de Direito*, *Democracia* e *Justiça* surge e circula em momentos disruptivos contra o arbítrio. Nesses eixos, o Direito pode ajudar, e muito.

A conceituação do *Estado de Direito* não é unânime, embora esse seja um dos valores mais bem recebidos em todas as ideologias. Apesar das divergências sobre os elementos do *Estado de Direito* em termos de procedimentalidade e/ou substancialidade, aceita-se que há um núcleo mínimo consensual. É também uma unanimidade no entendimento de que o *Estado de Direito* é um dos primeiros conceitos antitéticos ao arbítrio e à opressão (Tamanaha, 2004).

O núcleo do *Estado de Direito* pressupõe que um sistema jurídico possa conferir previsibilidade sobre as ações de seus cidadãos (segurança jurídica). Melhor dizendo, ele permite que as pessoas possam planejar suas vidas a partir da garantia da confiança recíproca entre os cidadãos e o Estado mediante um igual tratamento estatal para todos.

Para Joseph Raz (1979), a essência nuclear do Estado de Direito está na condição de um sistema jurídico funcionar como guia prático de conduta. Com discordâncias pontuais, Fuller (1964) elenca os princípios que considera imprescindíveis para as leis em um Estado de Direito:

- a) a existência de leis promulgadas, gerais, claras, estáveis, públicas, factíveis de cumprimento, congruentes e prospectivas;
- b) a eficiência de uma máquina que garanta a eficácia da lei para funcionar como guia da conduta, o que pressupõe a definição de limites às autoridades administrativas e um Poder Judiciário livre de pressões externas, acessível, impessoal, com decisões públicas e racionais.

Esses atributos do Estado de Direito se comunicam diretamente com *segurança jurídica*. Na medida em que o descontrole da transmissão de dados pessoais agrava a imprevisibilidade do futuro, aumenta a dificuldade de fixar marcos seguros e estabilizar relações sociais. Além disso, o caráter transnacional do problema atrapalha o sistema jurídico em metas de congruência, conturba a igualdade no tratamento normativo e gera dúvidas sobre a factibilidade de cumprimento das leis sobre esse tema.

Postos os embaraços sobre a mesa, é preciso pensar como o Direito pode superar tais atribulações e ajudar a proteger os dados pessoais.





Ora, em relação à *segurança jurídica* – ponto central do Estado de Direito – o Direito continua sendo um dos sistemas sociais mais aptos a regular condutas e impor obrigações.

A primeira característica que faz do Direito um dispositivo importante nessa tarefa é o seu objetivo de regular validamente condutas mediante a coercitividade legitimada. As provações enfrentadas pelos sistemas jurídicos no tratamento da proteção de dados pessoais não elidem ou suprimem o seu papel nesse desafio. Não é gratuitamente que um dos mais frequentes elogios ao GPDR tem sido a eficácia de suas multas, vultosas o suficiente para erigir a proteção de dados ao *status* de política importante para o mercado.

No que tange à *igualdade*, o *Estado de Direito* também é fundamental. É assim porque, em estruturas em que as relações são radicalmente assimétricas entre os atores, é precisamente a norma jurídica que pode contribuir para equilibrar a balança e evitar dominações. Esse fenômeno acontece na relação gigantes da tecnologia *vs.* usuários.

O Direito possui um grande talento para transitar entre as relações públicas e as privadas e, mais do que isso, para definir o que é do âmbito da esfera pública e o que é privado. Essencialmente, tais definições são pressupostos do *locus* de intangibilidade do indivíduo.

A liberdade jurídica é conformada por normas que aprovam direitos e deveres, e a consciência é liberdade que permite aos indivíduos concretizar seus interesses morais, filosóficos ou religiosos (Rawls, 2016). Em síntese, os direitos à intimidade, à privacidade e à honra/imagem jungem-se à liberdade e estampam a objeção da interferência.

O direito à intimidade é aquele próprio da integridade moral da pessoa. Para Barroso (2015), constituem a intimidade personalíssima do homem seus valores, sentimentos, desejos e frustrações. O conceito de privacidade moderna não é oposto à esfera pública, mas à esfera social e à intrusão da sociedade na região recôndita do homem (Rawls, 2016).

Embora o sistema jurídico seja imprescindível às liberdades, o estímulo atual não deve ser pela via da desregulamentação total do campo de proteção de dados pessoais, o que pode agravar as assustadoras imprevisibilidades e assimetrias de poder. A provocação deve ser de outra natureza, qual seja: como regular esse campo? Qual seria a tipologia de regulação mais adequada? Quem estaria apto a desempenhá-la e efetivar seu cumprimento?

Certamente, todos esses exercícios para pensar novas formas de regulação normativa da proteção de dados não acabarão com o bloqueio de congruência e factibilidade que advém da baliza fincada na figura do Estado como entidade que centraliza a produção do Direito e que se erige em pilares de soberania e de Jurisdição.





Contudo, a limitação estatal em tratar de assuntos transnacionais também é um problema que o próprio Direito pode ajudar a superar. Sem embargo do paradigma do sistema jurídico estatal, a ideia de *Justiça* pode ser bastante proveitosa, quando considerados os desenvolvimentos da proteção transnacional de direitos fundamentais.

A ideia de *Justiça* como distribuição de bens sociais para a finalidade de promover *liberdade e igualdade* é adequada para a regulação da difusão de dados pessoais, porque remete a um *status* básico de universalidade de direitos humanos que pode ser vantajoso como escudo protetivo.

A *Teoria da Justiça* reabilitou a moral para as escolhas sociais (Rawls, 2016). Rawls adota a fundamentação contratualista para embasar compromissos substantivos e propõe arbitrar exigências conflitantes e distribuir recursos por equidade⁶. É nuclear à proteção de dados pessoais o bloco de três ideias centrais de *Justiça* que dizem respeito à prevalência de valores, à redução de desigualdades e à vedação do sacrifício de liberdades fundamentais.

A discussão sobre o tratamento de dados pessoais deve ser abordada em suas dimensões ideal (correção moral) e fática (eficácia social). Por mais trabalhoso que seja o destrinchar de uma jovem realidade virtual, é adequado voltar a uma metodologia orientada pelos “problemas” para direcionar a busca de soluções que sejam morais.

Nesse caminhar, é preciso adotar etapas típicas do projeto rawlseliano: a) interpretar a situação-base (fática e axiológica) do problema; e b) abstrair racionalmente proposições setoriais que reflitam uma adequada concepção de *Justiça* para a solução dos impasses.

Eis que foi o Direito que internalizou os mais sofisticados mecanismos de deliberação democrática com vistas à elaboração de soluções morais a partir de diagnósticos fáticos. Em função disso, ele se mantém essencial no tratamento de dados pessoais.

Esses significados da *Justiça* são intrínsecos ao Direito. É o Direito que toma para si a tarefa de proteger as liberdades fundamentais ainda que contra-hegemônicas, ou seja, de lhes conferir certa dose de intangibilidade por outros círculos de poder. Foi também pelo Direito que se consolidaram as conquistas sociais.

Do mesmo modo, a concepção de *Justiça* confere ao Direito a oposição ao decisionismo⁷, evitando que princípios fiquem em segundo plano em prevalência exclusiva do

⁶ À *Teoria da Justiça* sucederam percepções filosóficas de *Justiça*, com destaque para as de Dworkin (2014, 2016) também liberalista-igualitárias, que aderem à razão substantiva. Seguiram-se, ainda, subsequentes análises críticas à *Teoria da Justiça* (Gargarella, 2008).

⁷ Pela Teoria Decisionista, é o povo de uma nação o real detentor do poder, independentemente de qualquer pressuposto normativo fundante. Entende que o governo não é da lei, mas da nação e de seu povo, que decide em qualquer situação, sem a escravidão pela norma (Schmitt, 2019).





poder. Essa funcionalidade do Direito subordina a autoridade à ideia agregada de valor moral. É assim que o Direito afirma a igualdade para afastar, sem prejuízo do pluralismo, distinções maniqueístas entre os “nós e outros” e os “amigos e inimigos”.

Finalmente, há um outro último aspecto em que a ideia de *Justiça* pode ajudar. O diálogo entre as Cortes Constitucionais e o aprendizado na proteção de direitos fundamentais se mostraram um caminho profícuo para a afirmação de direitos humanos ao redor do mundo. Em razão disso, se a categoria analítica da soberania estatal e seu derivado monismo jurídico prejudicam em parte a proteção de dados pessoais, a dimensão global da ideia de *Justiça* torna o Direito polivalente, versátil e compartilhado.

Há décadas não é tão importante encontrar soluções para garantir direitos fundamentais perante o revolucionário poder que advém da tecnologia. O alvorecer da IA pode estar ligado à perda de credibilidade da democracia e à mundial ascensão do populismo autoritário (Manheim; Kaplan, 2019). O Índice de Democracia, publicado pelo Economist, tem apontado reduções decorrentes da erosão na confiança no governo e nas instituições públicas (The Economist, 2021).

Na América Latina, o índice caiu pelo quinto ano consecutivo em 2020, influenciado pelas restrições da Covid-19 e pela fragilidade de processos eleitorais (Open Democracy, 2021). A realidade virtual não resolve tudo e pode ser um problema para a ação discursiva e pluralística. Em alguma medida, é provável que o vício das redes atrapalhe o encontro entre as pessoas.

Passando à terceira concepção, que é ligada ao Direito e pode ser útil à proteção de dados, trata-se da *Democracia*. A dissociação entre a política e o Direito é um marco da modernidade. Porém, ambas as ideias convivem em permanente tensão e possuem um vínculo interno simbiótico: a autonomia política é o que viabiliza a liberdade jurídica (Habermas, 1999).

A democracia é uma referência da autonomia e, logo, das liberdades políticas e cívicas. Nesse âmbito analítico, inserem-se consectários, como eleições livres, liberdade de expressão e de imprensa, participação, controle social e dever de prestar contas. Assim, a democracia é tanto afetada incisivamente pela difusão de dados, como também paradoxalmente pode ser um traçado importante nesse novo desenho de mundialidade.

Nada mais atual do que repensar “quem decide” e “como se decide” na democracia diante dos fenômenos da IA e das redes. Na prática, a humanidade se depara com a afluência





de novos modelos de participação democrática para *inputs*, e essa diversidade é valiosa, na medida em que garante aprendizado e legitimidade para além da ideia do voto.

No entanto, os pilares nucleares de *Democracia* que embasam a legitimação jurídica permanecem muito úteis e é essencial que haja uma verificação analítica desses novos processos deliberativos em relação aos postulados de autonomia, liberdade de expressão, justificação racional, inclusão participativa e *accountability*.

O Direito tem tudo a ver com isso. Ao fim e ao cabo, é atribuição do Direito definir como serão as “casas de máquinas” e as esferas públicas. É também ao Direito que compete proceduralizar *inputs* e *outputs*. Por último, o Direito retoma a justificação racional, as liberdades e suas garantias como as bases normativas intrínsecas ao agir comunicativo.

Por causa disso, o Direito pode ajudar em termos de *Democracia*: coibindo danos pelo uso indevido de dados em *fake news* e outras manipulações; e prevendo espaços de legitimação mais substanciais, plurais e inclusivos na tomada de decisão sobre a regulação da proteção de dados em si mesma e sobre as discussões públicas que a rede circunda.

4 CONCLUSÕES

É verdade que nada será como antes. Não faremos mais guerras com paus e pedras. É impossível frear a sucessão de transformações tecnológicas, múltiplas e rápidas. Pode ser que estejamos em meio a uma revolução, no sentido de substituir antigos paradigmas por novas formas de sonhar, conviver e resolver conflitos.

Dentro desse turbilhão, o Direito parece não performar como antes em desempenhos de estabilidade, segurança e justiça. Ele aparenta não dar conta do recado em seus limites em relação ao tempo necessário ao amadurecimento de sua própria gênese, à busca pela justificação racional a partir da previsibilidade fática, à tendência de definição tipológica entre as esferas públicas e privada e ao apego ao monismo estatal.

Mas isso é apenas o que aparenta ser o limite do Direito. Por detrás do véu da ignorância sobre o futuro e seus incertos eventos, permanecem os mesmos riscos a serem enfrentados: opressão, desigualdade e violência. Nisso, nada mudou. Assim, a outra face da moeda é que o Constitucionalismo continua sendo um bom campo de enfrentamento ao arbítrio.

Conceitos, como *Estado de Direito*, *Justiça* e *Democracia*, estão tensionados, mas persistem para garantir liberdade, igualdade e segurança. O Direito ainda é o sistema social





mais apto a regular relações assimétricas e o que melhor considera princípios. A simples reabilitação de valores pela noção de Justiça não é fútil. Nem pode ser desprezada uma antiga vocação do Direito para criar mecanismos de deliberação democrática, nos quais se busca o consenso, mas também se anistia a discordância. De fato, muita coisa mudou, mas o Direito continua tão – ou talvez mais do que nunca – útil à humanidade.

REFERÊNCIAS

ARENDT, Hannah. *Origens do totalitarismo*: antissemitismo, imperialismo, totalitarismo. São Paulo: Companhia das Letras, 2012.

BARCELLOS, Ana Paula de. *Direitos fundamentais e direito à justificativa*: devido procedimento na elaboração normativa. Belo Horizonte: Editora Fórum, 2016.

BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo*. São Paulo: Saraiva, 2016.

CHIRITA, Ana D. Springer-Verlag GmbH Germany, part of Springer Nature 2018 153 M. Bakhoun et al. (ed.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, MPI Studies on Intellectual Property and Competition Law 28. Disponível em: https://doi.org/10.1007/978-3-662-57646-5_7. Acesso em: 20 jun. 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DWORKIN, Ronald. *O império do direito*. São Paulo: Martins Fontes, 2014.

DWORKIN, Ronald. *A virtude soberana*: a teoria e a prática da igualdade. São Paulo: Martins Fontes, 2016.

FULLER, Lon Luvois. *The morality of law*. Yale: Yale University, 1964.

GALLAS, Luciano. *Proteção de dados*: lei apresenta avanços, mas não esgota desafios à privacidade e liberdade de expressão. Disponível em: <http://www.intervozes.org.br/direitoacomunicacao/?p=30241>. Acesso em: 19 jun. 2020.

GARGARELLA, Roberto. *As teorias da justiça de Rawls*: um breve manual de filosofia política de Roberto Gargarella. São Paulo: Martins Fontes, 2008.

HABERMAS, Junger. *Direito e democracia*: entre factibilidade e validade. Rio de Janeiro: Tempo Brasileiro, 2003.

HABERMAS, Junger. *La inclusión del otro*: estudios de teoría política: el vínculo interno entre estado de derecho y democracia. Barcelona: Paidós, 1999.





HART, Herbert. *O conceito de direito*. São Paulo: Martins Fontes, 2009.

HOOFNAGLE, Chris Jay; SLOOT, Bart Van der; BORGESIU, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, v. 28, n. 1, p. 65-98, 2019.

KUHN, Thomas S. *A estrutura das revoluções científicas*. 12. ed. São Paulo: Perspectivas, 2013.

MANHEIM, Karl; KAPLAN, Lyric. Artificial Intelligence: risks to privacy and democracy. *The Yale Journal of Law & Technology*, v. 21, p. 106-188, 2019.

OPEN DEMOCRACY. *América Latina*: índice de democracia cai pelo quinto ano consecutivo. 2021. Disponível em: <https://www.opendemocracy.net/pt/america-latina-democracia-indice-cai-quinto-ano-consecutivo/>. Acesso em: 14 nov. 2024.

POST, Robert; SIEGEL, Reva. Roe Rage: democratic constitutionalism and backlash. *Harvard Civil Rights-Civil Liberties Law Review*, v. 42, n. 373, p. 373-433, 2007.

QUELLE, Claudia. Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level? 2016. Disponível em: <https://ssrn.com/abstract=2726073>. Acesso em: 22 ago. 2021.

RAWLS, John. *Uma teoria da Justiça*. São Paulo: Martins Fontes, 2016.

RAZ, Joseph. *The authority of law: essays on law and morality*. New York: Oxford University Press, 1979.

RODOTÀ Stefano. Proteção de dados como direito fundamental. In: GUTWIRTH, Serge.; POULLET, Yves; DE HERT, Paul; DE TERWANGNE Cécile; NOUWT Sjaak (ed.). *Reinventing Data Protection?* Dordrecht: Springer, 2009.

RYFE, David M. Does deliberative democracy work? *Annu. Rev. Polit. Sci.*, v. 8, p. 49-71, 2005.

SCHMITT, Carl. *O conceito do político*. Lisboa: Edições 70, 2019.

SALDANHA, Nelson. O jardim e a praça: ensaio sobre o lado “privado” e o lado “público” da vida social e histórica. *Ci. & Trop.*, Recife, v. 11, n. 1, p. 108-121, jan./jun. 1983.

TAMANAH, Brian Z. *On the rule of law: history, politics, theory*. Cambridge: Cambridge University Press, 2004. p. 7-59, caps. 1 a 4.

THE ECONOMIST. Global democracy has a very bad year, 2021. Disponível em: <https://www.economist.com/graphic-detail/2021/02/02/global-democracy-has-a-very-bad-year>. Acesso em: 30 ago. 2021.





UNIÃO EUROPEIA. *Cartas dos direitos fundamentais da União Europeia*, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 14 nov. 2024.

VALENTE, Jonas. Facebook notifica usuários que tiveram dados vazados. *Agência Brasil*. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2018-04/facebook-notifica-usuarios-que-tiveram-dados-vazados-443-mil-sao-no-brasil>. Acesso em: 19 jun. 2020.

WEBER, Rolf H. Internet of things: Need for a new legal environment? *Computer Law & Security Review*, n. 25, p. 522-527, 2009.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica. In: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2018, São Paulo. *Anais Rede 2017*. São Paulo, 2018.

DADOS DA PUBLICAÇÃO

Categoria: artigo submetido ao *double-blind review*.

Recebido em: 14/11/2024.

Aceito em: 07/08/2025.

