REVISTA DIREITO PÚBLICO

INTERSECÇÕES ENTRE A INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS NO DIREITO BRASILEIRO[1]

INTERSECTIONS BETWEEN ARTIFICIAL INTELLIGENCE AND DATA PROTECTION IN BRAZILIAN LAW

INTERSECCIONES ENTRE LA INTELIGENCIA ARTIFICIAL Y LA PROTECCIÓN DE DATOS EN EL DERECHO BRASILEÑO

Marcos Catalan[2]

Rede Agendas de Direito Civil Constitucional. Porto Alegre/RS. Brasil.

Marcos Ehrhardt Junior[3]

Universidade Federal de Alagoas (UFAL) e Centro Universitário Cesmac. Maceió/AL. Brasil.

Eduardo Luiz Busatta[4]

Universidade Estadual do Oeste do Paraná (UNIOESTE). Cascavel/PR. Brasil

RESUMO: Este artigo tem como pano de fundo algumas das inafastáveis intersecções havidas entre a *inteligência artificial* e os dados pessoais dos quais ela se alimenta, tendo como objetivo primário avaliar se o Direito brasileiro é apto a tutelar, considerado o atual estágio da técnica, os titulares de dados pessoais tratados cotidianamente. Ao ser alinhavado sob os influxos da crítica metodológica, da imaginação jus-sociológica e do método exploratório, a pesquisa permitiu inferir que uma hermenêutica sistêmica pautada pela fundamentalidade do direito à proteção de dados pessoais, o direito subjetivo a

[1] Esta investigação científica foi desenvolvida no contexto do programa de estágio pós-doutoral oferecido pelo *Mediterranea International Center for Human Rights Research* sob a supervisão do primeiro autor, embora, todos os subscritores desta pesquisa tenham contribuído, igualmente, na elaboração do projeto de pesquisa, escolha da metodologia, seleção das fontes, condução da investigação, validação da hipótese antecipada enquanto possibilidade e, enfim, ao longo do processo de redação desde os primeiros rascunhos até a versão final e preparação para esta publicação.

[2] https://orcid.org/0000-0002-4775-7161

[3] https://orcid.org/0000-0003-1371-5921

[4] https://orcid.org/0000-0002-8570-2890

inferências razoáveis e a imperiosidade de tratamento de dados inferidos, a autorização inequívoca do titular para o treinamento de algoritmos de inteligência artificial e, ainda, a modulação dos deveres impostos aos agentes de tratamento, tendo em vista a natureza, escala, sensibilidade e eventuais danos havidos nesse processo, são fundamentais à adequada tutela da pessoa humana.
PALAVRAS-CHAVE: Inteligência artificial; Dados pessoais; Transformações das Relações Privadas; Direito e tecnologia; Lei Geral de Proteção de Dados Pessoais.

ABSTRACT: This article explores some of the undeniable intersections between artificial intelligence and the personal data on which it feeds, with the aim of investigating whether Brazilian law, considering the current stage of the technique, can adequately protect the holders of personal data processed daily, considering the current stage of the technique. Aligned under the influences of methodological criticism, jus-sociological imagination and the exploratory method, the research allowed to infer that a systemic hermeneutics based on the fundamentality of the right to protection of personal data, the subjective right to reasonable inferences and the imperativeness of processing inferred data, the unequivocal authorization of the holder for the training of artificial intelligence algorithms and the modulation of duties imposed on processing agents taking into account the nature, scale, sensitivity and possible damages that may arise from the processing of personal data are fundamental to the adequate protection of the human person.
KEYWORDS: Artificial Intelligence; Personal Data; Transformations of Private Relations; Law and Technology; General Data Protection Act.

RESUMEN: Este artículo explota algunas intersecciones entre la inteligencia artificial y los datos personales de los que se alimenta, con el objetivo principal de evaluar si la legislación brasileña es capaz de proteger, considerando el estado actual de la técnica, a los titulares de datos personales tratados diariamente. Al estar alineada bajo las influencias de la crítica metodológica, de la imaginación jussociológica y del método exploratorio, la investigación permitió inferir la relevancia de una hermenéutica sistémica guiada por la fundamentalidad del derecho a la protección de datos personales, la existencia de un derecho subjetivo a inferencias razonables, ser imperativo el procesamiento de los datos inferidos, ser necesaria la autorización inequívoca del titular para el entrenamiento de algoritmos de inteligencia artificial y, también, la necesidad de modulación de los deberes impuestos a los agentes procesadores, teniendo en cuenta la naturaleza, la escala, la sensibilidad y los posibles daños causados en este proceso, premisas fundamentales a la adecuada protección de la persona humana.

PALABRAS CLAVE: Inteligencia artificial; Datos personales; Transformaciones de las Relaciones Privadas; Derecho y tecnología; Ley General de Protección de Datos Personales.

Breves notas a título de introito

O crescente recurso a tecnologias dependentes da *inteligência artificial* inegavelmente tem impactado a vida humana. O acesso à saúde, o mercado financeiro, a educação, a segurança pública e privada, o entretenimento e o turismo, bem como o *e-commerce*, emergem como campos nos quais essa interação parece ser mais evidente, ladeados pelo inconteste e incontrolável processo de automação da indústria e, mais recentemente, do setor de serviços.

A *literal* revolução em curso carreia consigo uma miríade de questões inquietantes, entre elas as que procuram identificar a adequação do Direito brasileiro ao cenário fenomênico hodierno e, ainda, a sua capacidade de lidar com os desafios inerentes às mutações no modo de vida em sociedade, mormente quando se antevê o surgimento de tecnologias generativas, de processos de tomada de decisão sem controle humano, e ainda, de *caixas-pretas* guardando segredos sob o argumento de que é imperiosa a proteção da propriedade industrial.

Atualmente, parece difícil negar que a ausência de regulação específica da *inteligência artificial* no Brasil potencializa os riscos inerentes ao avanço da técnica, uma vez que além de explorar vulnerabilidades humanas, elas têm o condão de exponenciar heurísticas e vieses concretamente identificados, amplificar a desigualdade social tão conhecida nos países latino-americanos e, ainda, fomentar processos altamente discriminatórios, tudo isso redundando na violação de inúmeros direitos civis.

Exemplos notórios incluem algoritmos de reconhecimento facial que segregam pessoas com amparo em traços raciais, étnicos ou de gênero, ou, ainda, algoritmos que negam, à margem da lei, o acesso ao crédito, à educação ou à saúde (VÉLIZ, 2020 e 2021). Tais escolhas, longe de serem simples falhas técnicas – já que notadamente

enviesadas –, espelham a complexidade ética e normativa que aflora na delegação, às máquinas, da tomada de decisões que impactam a vida humana.

Paralelamente, a opacidade fundida a distintos aparatos que recorrem à *inteligência artificial*, exatamente por conta da névoa que intencionalmente envolve seus complexos fluxogramas de funcionamento, dificulta o fomento e a adoção de ações preventivas e, quando necessária, a responsabilização dos lesantes, pilares fundamentais em qualquer sistema jurídico que se afirme democrático, afinal, a impossibilidade de compreender aspectos afetos a *como* e *por que* uma decisão foi tomada, além de afrontar a normatividade pulsante do princípio da transparência, mina a confiança imperiosa à vida em sociedade.

É impossível não perceber, então, o paradoxo havido na identificação de que enquanto os projetos arquitetônicos de *sites* e outros espaços projetados visando à sedução dos consumidores – e, de forma cada vez mais frequente, a modulação do comportamento humano (DELEUZE, 2008; CASSINO, 2021; DARMODY, ZWICK, 2020; HUR, 2018; SILVEIRA, 2017) – são protegidos a sete chaves, a privacidade e a intimidade são desnudadas (LACE, 2005; SIBILIA, 2008; VÉLIZ, 2020), comercializadas e consumidas sem qualquer pudor, até porque o excesso de informação disponível na *Internet,* em vez de projetar alguma luz na escuridão (HAN, 2017), tem intensidade suficiente para ofuscar mesmo os olhares mais críticos.

No mais, a escorreita compreensão das possibilidades deletérias imanentes ao avanço da técnica – moldura que, obviamente, não esgota o universo de preocupações envolvendo os efeitos pernósticos concretamente projetados desde a *inteligência artificial* (EHRHARDT JUNIOR, CATALAN, NUNES, 2023*,* tampouco as inúmeras vantagens que carreia consigo – redunda na conclusão de que a esperada regulação do tema, no Brasil, não deverá limitar-se a tratar a reparação, nem a fomentar o dueto prevenção e precaução.

Será preciso garantir que a inovação tecnológica se dê de forma a respeitar a promessa de vidas dignas levada a cabo em 1988, bem como os direitos fundamentais

gestados na normatividade identificada no acoplamento da liberdade com a igualdade substancial e a solidariedade social, sem ignorar, ademais, o valor social da livre-iniciativa.

Não se pode ignorar a existência de estreita relação entre a regulação aguardada e a legislação erigida, visando à tutela de dados pessoais no Brasil, tema que ganhou destaque nos últimos anos com a promulgação da Lei Geral de Proteção de Dados, importante marco na proteção do direito à privacidade e à segurança da informação. Isso se deve, em especial, ao sucesso dos sistemas impulsionados pela *inteligência artificial,* que depende, em grande medida, da coleta, tratamento e processamento massivo de dados.

É possível frisar que no contexto brasileiro, na ausência de legislação específica sobre o assunto, tem-se defendido que a Lei Geral de Proteção de Dados deve servir como baliza normativa a impor obrigações quando sistemas automatizados forem alimentados por dados pessoais, de modo a evitar práticas que comprometam tanto a privacidade como outros direitos atribuídos aos titulares dos dados tratados. Uma vez identificada a violação, cumpre sancionar as condutas normativamente qualificadas como reprováveis (BUSATTA, 2024).

Nesse diapasão, a regulação da *inteligência artificial* deve buscar complementar o quadro normativo existente no Brasil, garantindo que a inovação tecnológica se oriente por limites éticos matizados por vieses não utilitaristas e, ainda, pela imperiosa e inegociável tutela de toda pessoa humana.

É verdade que referida perspectiva não resta imune às críticas daqueles que temem que a regulação excessiva obste que as potencialidades imanentes à *inteligência artificial* possam ser plenamente exploradas em benefício da sociedade (DOMINGOS, 2015). Tais preocupações, entretanto, parecem não resistir à imperiosidade de diálogo entre as muitas fontes a serem usadas na construção das respostas normativas esperadas no tratamento da matéria, um diálogo que deverá inexoravelmente ter como atrator o equilíbrio entre o aguardado e, até mesmo, bem-vindo desenvolvimento

tecnológico e a inafastável proteção das muitas vulnerabilidades humanas. Outro não parece ser o caminho indicado pela Constituição Federal vigente desde 1988.

A discussão sobre a regulação da *inteligência artificial*, ao menos à primeira vista, parece transbordar a simples adaptação da legislação existente no país, requerendo a revisão semântica de *signos* como responsabilidade, privacidade, segurança e autonomia, à luz das possibilidades afetas às tecnologias disruptivas gestadas na Revolução Digital e, ainda, das muitas angústias fundidas ao modelo de racionalidade que informa os contornos dados pela Modernidade à autonomia privada e ao seu consequente lógico, a *pacta sunt servanda*.

Sem descurar as lições assentadas nos parágrafos precedentes, a abordagem regulatória expectada no futuro próximo deverá ser também colorida com tons pinçados dos princípios abstratamente aplicáveis às distintas tecnologias, atentando, especialmente, às especificidades de cada mecanismo, técnica ou mercado concretamente mapeado e, sobretudo, à interdependência que permeia a inovação e a proteção dos muitos direitos consagrados nas searas constitucional e infraconstitucional, mesmo que esses, recorrentemente, demandem um melhor detalhamento de sua posologia normativa abstratamente prevista na legislação e, por que não, em suas manifestações nos meandros da *law in movement*.

No mais, antes que este breve introito alcance o seu fim, é preciso anotar que as reflexões que vivificam essa pesquisa foram intencionalmente grafadas sob os influxos da crítica metodológica (GUSTIN, DIAS, 2013) e da imaginação jus-sociológica (JACOBSEN, TESTER, 2015), escolhas científica e literária conscientemente incorporadas ao texto. O método utilizado tem viés exploratório, legitimando a pesquisa a tatear elementos ocultos nas sombras do porvir.

Dados pessoais alimentam a *inteligência artificial*: um horizonte de preocupações

Antes de seguir a trilha antecipada, parece ser oportuna a formulação de um acordo semântico acerca do que vem a ser a *inteligência artificial*, afinal, se de um lado,

pensamento e inteligência são características que diferenciam a humanidade de outras espécies, de outro, a alteridade é uma marca indelével em cada pessoa, um acordo que pressupõe perceber que o intelecto do *Homo sapiens* serviu como chave ao incremento de habilidades cognitivas extremamente avançadas, como a linguagem, o raciocínio abstrato, a capacidade de resolução de problemas complexos e a criatividade.

É aparentemente inquestionável a constatação de que a aptidão à crítica e ao raciocínio analítico permitiu ao ser humano melhor compreender o mundo, questionar o conteúdo de crenças e tradições e, ainda, lapidar explicações teóricas para fenômenos naturais e artificiais, dado que reforça a explicação de porque a expressão *Homo sapiens* foi eleita como o nome científico para designar toda a espécie humana, afinal. É que o adjetivo *sapiens* enaltece a inteligência como traço definidor da espécie, característica crucial à adaptação e sobrevivência em diferentes ambientes, à criação de ferramentas, à comunicação e, no limite, à própria vida em sociedade.

A inteligência, então, é um atributo humano, talvez exclusivamente humano, algo apenas simulado em sistemas autônomos impulsionados pelo que se convencionou denominar *inteligência artificial*. Sublinhe-se, todavia, que mesmo não sendo escorreita, a expressão foi mantida ao longo do texto, visando a evitar desnecessários desacordos semânticos.

Anote-se, então, de modo a permitir que o texto flua, que a *inteligência artificial* reflete nada mais que a aptidão de um sistema cibernético para *copiar*, *imitar* ou *emular* funções cognitivas humanas, identificando e resolvendo problemas de modo autônomo e absorvendo a experiência adquirida (FÜRST, BÜRGUER, 2023) de modo a dar-lhe uso prático. De forma muito simplificada, ela consiste na simulação de processos cognitivos visando à solução de questões com distintos graus de complexidade (JESUS DIÁZ, CORDÓN GARCIA, HERRERA, 2022).

Tema candente há mais de meio século, curiosamente, são diversas as aproximações mapeadas na literatura entre *ela* e a racionalidade humana. Em termos gerais, há alusões ao fato de que as máquinas tentam pensar como humanos, tomar

decisões fundadas em idêntica racionalidade, agir racionalmente ou, ainda, atuar como se fossem seres de carne de osso (RUSSELL, NORVIG, 2010). Mesmo que se escolha qualquer outra moldura envolvendo a ideia, resta patente que, ao menos metaforicamente, o coração que impulsiona tais máquinas tem em sua composição algoritmo(s) desenhado(s) por seres humanos com propósitos práticos no intuito de dar conta de problemas da vida mundana cotidiana (SAUX, 2023).

Sem diminuir sua importância, mais que mero atributo de mecanismos autossuficientes, a *inteligência artificial* é o elemento cardeal que lhes garante essa qualificação ao permitir-lhes desempenhar as funções para as quais foram projetados sem nenhuma forma de controle ou intervenção humana direta. Sozinhos, com amparo nos dados que estão ao seu alcance, tais algoritmos elegerão os caminhos que lhes pareçam mais escorreitos e, quando oportuno, adaptarão sua configuração às exigências do ambiente que os envolve (HANSEN BECK, BERNARDES, 2023).

Ocorre que, como a *inteligência artificial* busca emular a inteligência humana em aspectos específicos, principalmente naqueles relacionados ao processamento de informações, reconhecimento de padrões, tomada de decisões visando à solução de problemas, nota-se que ela precisa conhecer o comportamento humano, o que exige que se alimente de dados, de uma imensa quantidade de dados.

No que toca à sua operação, é igualmente factível antecipar que agentes autônomos estarão cada vez mais presentes no cotidiano da vida em sociedade, impulsionando a realização de tarefas repetitivas e, ainda, facilitando a interação das pessoas com distintas máquinas dotadas de interfaces como assistentes virtuais, sistemas de reconhecimento de voz e imagem, ou mesmo, em um futuro cada vez mais próximo, com a tecnologia ciborgue ou os muitos metaversos antecipados nas narrativas contemporâneas.

O processo de automação, interação e aceitação social da *inteligência artificial* inegavelmente aumentará a produtividade e eficiência em diversas atividades, revolucionando áreas como a Medicina – com o desenvolvimento de sistemas de

diagnóstico mais precisos, tratamentos personalizados ou cirurgias robóticas –, a Indústria – com a otimização de processos de produção e logística – e, ainda, as Ciências – possibilitando avanços em pesquisas e descobertas de novos processos, técnicas etc. –, ainda que, como exposto, provavelmente seguirá sendo incapaz de replicar, por inteiro, toda a complexidade fundida à inteligência e à sagacidade humanas.

É preciso atentar ainda ao fato de que um algoritmo pode analisar padrões e preferências com base em dados pessoais para fornecer recomendações e experiências personalizadas, prática utilizada em plataformas de *streaming*, comércio eletrônico e publicidade *online*, além de, obviamente, ser o coração das redes sociais.

O cenário hodierno vê, assim, interações digitais transformadas em perfis detalhados que mapeiam tendências, preferências, desejos e, certamente, vulnerabilidades humanas, algo que interessa sobremodo aos grandes *players* do ramo da tecnologia. Cada clique, e até mesmo a quantidade de atenção dedicada a determinado conteúdo exposto em um *site* ou aplicativo, é registrado e tratado, viabilizando a criação de perfis detalhados dos usuários, bem como o recurso a estratégias sofisticadas de modulação comportamental (VERBICARO, HOMCI, 2024). A tecnologia hodiernamente existente é tão avançada que consegue identificar a parte da tela – do computador, do *tablet* ou mesmo do telefone celular – que fisgou a atenção do usuário ao mapear a direção do olhar preso às imagens pulsantes na superfície do écran.

Se há algum acerto na afirmação de que os dados impulsionam a economia digital como o petróleo impulsionou a Segunda Revolução Industrial – metáfora que peca por ignorar o fato de que o petróleo é um bem finito –, não se pode ignorar que nesse ambiente a *inteligência artificial* atuaria como uma refinaria a processar o óleo bruto, visando gerar valor econômico. Assim, da mesma forma que refinarias transformam o petróleo em diversos produtos refinados como a gasolina e o diesel, aquela obtém informações significativas e *insights* acionáveis a partir de dados em estado bruto.

Este processo alimenta-se da exploração de heurísticas e vieses cognitivo-comportamentais de forma perigosamente individualizada, emergindo como um risco ao

exercício de liberdades positivas, pois, provavelmente, mais que influenciar de forma genérica decisões pessoais nos cenários forjados na Sociedade de Consumo, literalmente, modula a conduta humana ao desprezar o fato de que "a liberdade de escolha não se resume à ausência de coerção, pressupondo o acesso a informações claras, precisas, adequadas e suficientes sobre os produtos e serviços adquiridos, o esclarecimento do consumidor acerca das características, riscos e benefícios concretos daquilo que lhe é ofertado e, ainda, a ausência de modulação, intencional, de quaisquer atos de consumo" (CARTA DE BELÉM DO PARÁ, 2024.).

Sublinhe-se que aspectos como o *frequently bought together* e as recomendações de produtos são exemplos clássicos de como os algoritmos podem direcionar as escolhas dos usuários de maneira quase imperceptível (CRUZ, 2021), a despeito de se alimentarem de seu rastro digital. A mesma preocupação é identificada quando alimentam artificialmente a escassez por meio ofertas limitadas no tempo, cuidadosamente apresentadas visando maximizar a adesão dos consumidores (SANTOS, 2022) mediante recurso ao *fear of missing out*.

De outro lado, a personalização excessiva construiu câmaras de eco nas quais as escolhas de cada usuário são continuamente reforçadas por meio de sugestões baseadas em suas atividades anteriores, limitando a exposição a novas ideias e perspectivas (WOLFGANG, 2022), castrando, portanto, a liberdade humana. O pantagruélico apetite do mercado cresce a cada vantagem comercial (ZUBOFF, 2020) que consegue identificar, mesmo quando muitas delas tenham brotado em pastos semeados sob solo sagrado.

Ocorre que a normalização da dependência dos algoritmos guiando escolhas diárias, ladeada pela homogeneização e segregação de informações, pelo fomento ao preconceito e pela discriminação, estimula a formulação de questões que buscam saber não apenas quem controla os algoritmos ou quais são seus verdadeiros propósitos, mas, especialmente, quais os limites éticos e normativos de sua influência sobre as vidas humanas (WOLFGANG, 2022; SUSSER, ROESSLER, NISSENBAUM, 2019).

Não se olvida que a *inteligência artificial* pode ser uma importante ferramenta a serviço da humanidade. O ponto é que ela se alimenta de dados pessoais ante a constante necessidade de treinamento e compreensão do mundo: aprendizado de máquina, computação em nuvem, *big data* e internet das coisas são tecnologias fortemente ligadas à coleta do rastro digital deixado pelas pessoas, problema que cresce exponencialmente com o advento da versão generativa da *inteligência artificial* baseada em grandes modelos de linguagem e, portanto, que opera predominantemente com dados extraídos da *Internet,* mediante processo conhecido como *raspagem* (KING, MEINHARDT), o que dificulta ainda mais o controle desse processo, pois nem sequer é possível identificar os atores sociais ligados a referidas ações.

Um brevíssimo diálogo entre o Norte e o Sul: sobre leis destinadas a regrar a *inteligência artificial* e a promover a proteção de dados pessoais

Demonstrada a íntima relação entre *inteligência artificial* e dados pessoais, é indubitável que as leis que visam à proteção de dados serão aplicadas quando aquela os utilize mesmo na hipótese de treinamento, afinal, tais leis regulamentam o tratamento de dados pessoais, independentemente do método ou da finalidade inerente ao uso (WINAU, 2023).

Na hipótese, em um primeiro momento, duas são as possíveis consequências: (a) caso exista, em determinado sistema jurídico, uma lei específica regulando a *inteligência artificial* e outra cuidando dos dados pessoais, haverá a necessidade de aplicação sistemática de referidas leis; por outro lado, (b) na ausência de lei regulamentando pontualmente a *inteligência artificial* – como sói ocorrer, atualmente, no Brasil –, não haverá vácuo normativo quando a tecnologia for utilizada para o tratamento de dados pessoais, pois a legislação correlata será aplicada.

A União Europeia, ao que tudo indica, escolheu trilhar a primeira via, com a aprovação do Regulamento Europeu sobre *inteligência artificial*. A evidente sobreposição dos cenários normativos foi reconhecida pelo legislador europeu, que

recorreu à expressão "dados pessoais" em aproximadamente oitenta ocasiões (PARLAMENTO EUROPEU), sendo inegável que a concretização do Regulamento Europeu destinado ao regramento do assunto enfrentará dificuldades devido a possíveis conflitos com o Regulamento Geral de Proteção de Dados (GDPR).

Consoante leciona Mona Winau, o principal desafio parece estar atado ao fato de que enquanto o Regulamento Europeu destinado ao tratamento do tema busca estabelecer normas técnicas gerais para sistemas de *inteligência artificial* complexos e em constante evolução, o Regulamento Geral de Proteção de Dados aborda questões de proteção de dados de forma mais contextual, o que sugere que a conciliação de abordagens tão diferentes pode exigir a redução do nível de abstração identificado no primeiro, a fim de acomodar a avaliação caso a caso exigida no segundo diploma normativo para determinadas questões (WINAU, 2023).

De outra banda, como antecipado, o Brasil se enquadra no segundo grupo de casos. Ao menos por ora, inexiste no país um diploma legislativo que se dedique à regulação da *inteligência artificial*.

Em verdade, a proposta em trâmite no Congresso Nacional, por uma série de razões, não parece ter tração suficiente para que, no curto ou médio prazo, venha a se transformar em lei, o que avulta a importância de buscar uma gramática de proteção de dados pessoais que tenha em conta as especificidades da *inteligência artificial,* de modo a fazer frente aos desafios colossais existentes na contemporaneidade. Não se pode olvidar, ademais, que ao menos de modo pontual, o Anteprojeto de Código Civil também poderá impactar o regramento do assunto.

A proteção de dados pessoais ante o avanço da técnica: uma hermenêutica possível

A inafastável aplicação das leis de proteção de dados pessoais, nas ocasiões em que estes são tratados por meio de técnicas de *inteligência artificial*, é algo tão óbvio que defendê-lo não passaria de uma trivialidade desnecessária. De outra banda, é imprescindível sublinhar a imperiosidade da construção de uma sólida hermenêutica

jurídica, de modo a fornecer as chaves de leitura necessárias para que as leis de proteção de dados cumpram seu papel em contextos tecnológicos deveras desafiadores, porquanto o universo da *inteligência artificial* usualmente envolve situações marcadas pelo ineditismo.

É preciso, então, definir como os princípios e as demais balizas normativas previstas na legislação responsável pela proteção de dados no Brasil devem ser aplicados concretamente nos casos que envolvem a *inteligência artificial*, razão pela qual, sem descurar a relevância da adaptação de todas as regras da Lei Geral de Proteção de Dados ao contexto fenomênico que alimenta as reflexões alinhavadas neste texto, este estudo enfatiza cinco vetores hermenêuticos considerados essenciais à concretização do direito fundamental à proteção de dados.

Tais vetores – ou atratores normativos, não parece equivocado afirmar – abordam questões críticas, atuando como forças orientadoras ou como vias interpretativas robustas, direcionadas a um objetivo específico: a ampla tutela da pessoa humana.

Os signos *vetor* ou *atrator*, intencionalmente pinçados no vernáculo, procuram cinzelar o dinamismo, a intencionalidade e a capacidade de impulsionar um movimento e, ainda, sublinhar que muito além das usuais abstrações dogmáticas tão caras ao direito civil clássico, atuam como vias aptas a conduzir à efetivação do direito à proteção de dados – *também* – em suas intersecções com a *inteligência artificial*.

Mais que isso, tem-se que cada um dos pontos destacados nesta investigação emerge como medida, requisito ou diretriz normativa necessária para que o direito à proteção de dados seja assegurado no contexto específico do desenvolvimento e uso da *inteligência artificial*.

Ainda: cada proposição há de atuar como um vetor que, aliado aos demais, implique uma resultante robusta na proteção de dados em ambientes envoltos pela tecnologia emergente no século XXI, pois, como salienta Morin, o todo é maior que a simples soma das partes (MORIN, 2003).

Dito isso, cabe salientar que o primeiro entre os vetores sobrelevados pode ser identificado no *direito fundamental à proteção de dados pessoais*, previsto na Constituição e esmiuçado no regramento estabelecido na Lei Geral de Proteção de Dados. Ressalte-se a necessidade de novo acordo semântico envolvendo os *princípios* previstos na Lei 13.709/2018, terminologia mantida a despeito das dúvidas acerca do acerto no recurso ao retrocitado signo linguístico.

Embora a Constituição não especifique salvaguardas detalhadas ao tratar desse direito, a lei referida traz, em seu artigo 6º, dez *princípios* basilares que formam a "coluna vertebral" na proteção de dados pessoais no Brasil. Referidos *princípios*, entre os quais se destacam a finalidade e a adequação, a necessidade, o livre acesso e a transparência, sintetizam a lógica, a função e os aspectos mais relevantes na estruturação de referido direito fundamental. Boa parte da apontada lei densifica os meios de aplicação dessas premissas legais.

Ato contínuo, tendo em vista a ausência de diretrizes constitucionais específicas, é correto defender que tais *princípios* passam a integrar o conteúdo constitucional do direito à proteção de dados, formando um bloco de constitucionalidade (COELHO, 1994), a representar as salvaguardas constitucionalmente adequadas à efetivação do direito pautado por estas reflexões. De fato, representam o que há de mais legítimo e atual na proteção de dados pessoais, mesmo que estejam aquém do que se encontra previsto no Regulamento Geral de Proteção de Dados da União Europeia, bem como do progressivo desenvolvimento do tema no continente europeu.

Desse modo, parece ser perfeitamente defensável que, embora não estejam literalmente tracejados na Constituição, os *princípios* elencados na Lei Geral de Proteção de Dados absorvem conteúdo materialmente constitucional, dando forma ao coração desse direito que, se ferido, não terá como alimentar com a energia necessária a complexa estrutura pensada para a proteção de dados pessoais no Brasil.

Em síntese, é possível afirmar que o direito fundamental à proteção de dados pessoais forjado no país ganhou vida com a existência e a eficácia dos *princípios*

previstos no artigo 6º da Lei Geral de Proteção de Dados, vetores que devem ser interpretados sistematicamente com a Constituição por meio de um "círculo hermenêutico"[5] apto a dar-lhe concretude e legitimidade mediante parâmetros orientadores de sua interpretação e aplicação.

O retrocitado vetor normativo tem como principal relevância prática, além de permitir maior refinamento e concretização do direito fundamental à proteção de dados pessoais, tornar os princípios constantes da Lei Geral de Proteção de Dados aplicáveis às relações que, em princípio, seriam refratárias às soluções oferecidas por referida lei. De fato, a LGPD não é aplicável no tratamento de diversos dados pessoais, conforme expressa disposição do Art. 4º.

A aporia aparente pode ser transposta quando se vislumbra que o tratamento de dados pessoais *imunes* à LGPD é matizado pelo direito fundamental à proteção de dados pessoais. Assim, ao integrar os referidos *princípios* ao conteúdo material do direito fundamental à proteção de dados pessoais, identifica-se um claro aumento do espectro de proteção dos titulares de dados pessoais sujeitos àqueles tratamentos.

O segundo atrator tem como pano de fundo a noção de cadeia de dados. Em síntese, há dados mais importantes que outros, embora dados considerados inferiores permitam a derivação, a inferência ou a construção de dados superiores – estes últimos, muito mais relevantes para os fins que motivam o seu tratamento no contexto do sistema econômico capitalista.

Nesse cenário, os dados de ordem inferior, como cliques, páginas visitadas, tempo de visualização etc., sozinhos, possuem pouquíssima relevância. O acoplamento desses dados, entretanto, mormente diante do aumento da capacidade de processamento e do recurso a ferramentas de *inteligência artificial*, produz novos dados – agora, de ordem superior –, o que é feito em escala e complexidade analítica sem precedentes. É possível inferir, com elevado grau de precisão, o estado gestacional das

[5] A reflexão tem em conta que por ocasião de atribuição de sentido ao direito fundamental à proteção de dados pessoais caberá ao intérprete ir da parte ao todo e do todo à parte (STRECK, 2017).

consumidoras por meio da identificação de padrões de compra de cosméticos sem fragrância (NISSENBAUM, 2019).

Dados de ordem superior podem exigir formas de proteção distintas dos dados de ordem inferior, ao contrário do que tem sido comumente defendido, pois, se uma bomba pode ser construída tendo adubo como matéria-prima, ou uma bebida letal pode ser produzida com base em um líquido inócuo, não parece razoável defender que, também no âmbito da proteção de dados, a matéria-prima e seus produtos recebam idêntico tratamento normativo (NISSENBAUM, 2019). Isso significa que os dados inferidos ou construídos por meio de ferramentas alimentadas pela *inteligência artificial* devem ser qualificados como dados pessoais, uma condição *sine qua non* para a sua adequada proteção no cenário hodierno.

A chave de leitura proposta parece ter sido indiretamente reconhecida pela própria Lei Geral de Proteção de Dados Pessoais ao estabelecer (a) o direito à revisão das decisões tomadas com base no tratamento de dados pessoais quando – ainda que o recurso ao *signo* interesse, sem sinonímia com *direito*, possa dar margem à tutela de subjetividades e fomentar o solipsismo – afetem os interesses das pessoas (Art. 20), bem como (b) o direito à explicabilidade de referidas decisões (Art. 20, § 1°), dispositivos que evidenciam a necessidade de considerar as inferências e construções algorítmicas como dados pessoais, de modo a garantir a efetividade desses direitos.

Resta patente que se tais inferências estiverem relacionadas a uma pessoa identificada ou identificável, serão consideradas dados pessoais, na forma do Art. 5°, I, da Lei Geral de Proteção de Dados, afinal, não há como dissociar informações construídas por algoritmos da ideia de dado pessoal, uma vez que se referem, diretamente, a pessoas específicas.

A questão ganha relevância na emergência da *inteligência artificial* generativa, em especial com os grandes modelos de linguagem (LLM), como o *ChatGPT*, o *ChatSonic*, o *Jasper Chat*, o *Youchat*, a *Perplexity AI* ou o *Character AI*, treinados para processar e gerar textos em linguagem natural. À medida que tais sistemas podem fornecer dados sobre

pessoas, às vezes, tendenciosos ou falsos, parece imprescindível que referidas informações sejam tratadas como dados pessoais sujeitos às salvaguardas e direitos estampados no Direito pátrio, mitigando, assim, os riscos associados a cada vez mais comum disseminação de informações enganosas ou discriminatórias por meio dessas tecnologias.

O terceiro atrator que se procura lapidar tem como lastro um fato notório: o uso da *Inteligência Artificial* no tratamento de dados para a obtenção de inferências não intuitivas é uma prática deveras comum na contemporaneidade.

Referidas inferências frequentemente resultam em discriminações negativas, o que evidencia a necessidade de ultrapassar a regulação simplista, aludindo a quais tipos de dados podem ser coletados, aspecto que parece ter primazia nas discussões sobre privacidade e autodeterminação informativa na atualidade.

É imprescindível refletir sobre aspectos que tangenciam *como* e *para que* os dados pessoais serão tratados enquanto pressupostos na edificação de um "direito a inferências razoáveis" (WACHTER, MITTELSTADT, 2019), fomentando a possibilidade de controle *ex ante* do uso dos dados pessoais pelo agente de tratamento. Isso pressupõe a avaliação de três aspectos fundamentais: (a) a legitimidade da utilização de determinada base de dados para a inferência específica pretendida, pois nem todas as bases de dados são adequadas ou legítimas; (b) a checagem da relevância e adequação da inferência buscada para o propósito do processamento, afinal, mesmo que se recorra a uma base de dados adequada, algumas inferências podem ser desnecessárias, injustificadas ou potencialmente discriminatórias, porquanto violam direitos e liberdades individuais; e (c) a garantia de que os dados e métodos utilizados para gerar as inferências sejam precisos, confiáveis e baseados em evidências científicas sólidas, já que inferências derivadas de algoritmos enviesados, dados inconsistentes ou técnicas opacas representam um risco significativo aos titulares dos dados.

Uma abordagem hermenêutica com amparo na ideia de um "direito a inferências razoáveis" (WACHTER, MITTELSTADT, 2019) legitima repensar hermeneuticamente as

soluções previstas na(s) lei(s) de proteção de dados a partir de práticas identificadas fenomenicamente (GRUNDMANN, MICKLITZ, RENNER, 2021) na era do *Big Data* e da *inteligência artificial*, muitas vezes atuando sob o manto da ilicitude. A ideia implica o estabelecimento de critérios rigorosos para o uso legítimo e ético dos dados pessoais, de forma a mitigar os riscos afetos à discriminação, violação da privacidade e consequências de decisões enviesadas ou opacas.

Em suma, embora a regulação sobre a coleta de dados seja importante, é fundamental ampliar o escopo da proteção de dados pessoais, abordando também aspectos que abarquem *como* e *para que* esses dados são tratados, especialmente em contextos que envolvem *inteligência artificial* e inferências não intuitivas.

O quarto ponto de relevância hermenêutica a ser enfatizado liga-se empiricamente ao uso secundário de dados pessoais para o treinamento de sistemas de *inteligência artificial*, aspecto considerado crítico nesta investigação científica, razão pela qual merece uma especial atenção.

Qualquer reflexão sobre o tema não pode desprezar o fato de que, consoante estabelecido pela Lei Geral de Proteção de Dados Pessoais, dados pessoais tratados para determinada finalidade não podem ser reutilizados para finalidades incompatíveis com a que fora originalmente estabelecida. Trata-se de uma disposição crucial para proteger a legítima confiança, bem como a autodeterminação informativa dos titulares dos dados.

A noção de *incompatibilidade* notadamente não se refere à impossibilidade física, mas à sua feição jurídica, e deve ser identificada quando o tratamento ulterior não guardar relação de proximidade ou conexão lógica com o tratamento inicial. Se ele ocorrer, haverá violação da expectativa razoável do titular dos dados, o que ocorreria, por exemplo, quando dados pessoais coletados para fins de *marketing* vierem a ser reutilizados na análise de crédito.

A partir daí, a utilização de dados pessoais para o treinamento de algoritmos de *inteligência artificial* deve ser considerada finalidade incompatível com a finalidade

original da coleta, exceto se houver uma nova autorização, expressa, do titular, afinal, o treinamento de sistemas de *inteligência artificial* envolve processos complexos e imprevisíveis.

A atribuição de sentido ao *signo incompatibilidade* deve ser feita com lastro na boa-fé objetiva, levando em consideração a legítima expectativa do titular em relação ao uso de seus dados pessoais, e não necessariamente às necessidades e práticas postas em movimento pelo sistema de mercados. Embora os agentes de tratamento geralmente adotem finalidades amplas e abrangentes em suas políticas de privacidade, isso não deve ser interpretado como uma carta branca para a reutilização indiscriminada de dados para qualquer finalidade. Em princípio, permissões para a reutilização de dados previstas nas condições gerais de contratação deverão ser consideradas como não escritas, mormente se houver *overload* informativo, dificuldade de compreensão da linguagem utilizada ou ausência de relação direta entre os fins propostos.

No aspecto prático, a questão do uso secundário de dados pessoais para treinamento de *inteligência artificial* enfrenta desafios que transitam pela dificuldade de controle e fiscalização do uso pelos titulares e autoridades competentes. No entanto, é fundamental que sejam estabelecidos mecanismos efetivos de transparência, consentimento informado e prestação de contas de modo a garantir que os direitos e as liberdades individuais sejam respeitados.

A utilização de dados pessoais para o treinamento de algoritmos de *inteligência artificial* deve, assim, ser considerada uma nova finalidade, exigindo uma autorização específica e inequívoca do titular, abordagem essencial para preservar a confiança e a autodeterminação informativa das pessoas, e apta a garantir que seus dados sejam tratados de forma transparente, lícita e dentro dos limites do consentimento fornecido.

Finalmente, não se pode deixar de sublinhar que tanto a Lei Geral de Proteção de Dados como o Regulamento Geral sobre a Proteção de Dados reconhecem a existência de um amplo espectro de risco no tratamento de dados pessoais, a variar consoante diversos fatores relevantes – tipos de dados, escala de tratamento, natureza do

tratamento, escopo, finalidade, tecnologia envolvida etc. –, variação esta que deve ser observada na imposição e modulação de deveres aos agentes de tratamento. Tal abordagem decorre, em última instância, da compatibilização dos princípios constitucionais da solidariedade, isonomia material e livre- iniciativa, bem como da imposição constitucional de proteção eficiente ou adequada dos direitos fundamentais envolvidos.

No Brasil, o Art. 44 da Lei Geral de Proteção de Dados estabelece que o tratamento de dados será considerado irregular quando não observar a legislação ou quando não fornecer a segurança que o titular possa razoavelmente esperar. O Art. 46, por sua vez, ao tratar do dever de segurança dos agentes de tratamento de dados, determina que, caso a autoridade nacional estabeleça padrões técnicos mínimos, deverá considerar a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis.

Por seu turno, ao abordar as boas práticas, o § 1º do Art. 50 determina que devem ser levados em consideração o escopo, a natureza, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular. Da mesma forma, o § 2º institui que, na densificação dos princípios da segurança e da prevenção, o controlador deve observar 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. Além disso, a implementação de programas de governança deve ser adaptada à estrutura, à escala e ao volume de suas operações, e ainda, à sensibilidade dos dados tratados (inciso I, “c”).

Resta patente que a Lei Geral de Proteção de Dados adota uma “abordagem baseada em riscos” (QUELLE, 2020; KARJALAINEN, 2022), na qual deveres e obrigações dos agentes de tratamento devem ser modulados de acordo com a natureza, escala, sensibilidade e potenciais danos envolvidos no tratamento de dados pessoais. Essa abordagem visa equilibrar a proteção dos direitos e liberdades individuais, modulando a

conduta esperada dos agentes de tratamento, com lastro nos princípios constitucionais e na necessidade de proteção eficiente e adequada.

O uso da *inteligência artificial* deve ser considerado atividade de alto risco, exigindo a aplicação das mais rigorosas salvaguardas e obrigações previstas no direito pátrio. Isso se deve, principalmente, à escalabilidade e à opacidade inerentes aos sistemas de *inteligência artificial*.

A escalabilidade refere-se à capacidade desses sistemas de processarem e gerarem inferências a partir de enormes volumes de dados, exponenciando os impactos de eventuais falhas, enviesamentos ou violações de privacidade. A opacidade, por sua vez, diz respeito não apenas à dificuldade de compreender e auditar os processos internos de algoritmos, que muitas vezes se encontram em *caixas-pretas* insondáveis – mesmo para seus desenvolvedores –, mas também está ligada à imprevisibilidade e à autonomia crescente desses sistemas. É que muitos sistemas de *inteligência artificial*, especialmente aqueles baseados em aprendizado profundo, exibem comportamentos emergentes e imprevisíveis, sendo difícil antecipar e mitigar seus riscos potenciais.

Essas características representam riscos significativos para os direitos e liberdades dos titulares de dados, como discriminações injustificadas, decisões automatizadas enviesadas, violações de privacidade e falta de transparência e prestação de contas, razão pela qual o tratamento de dados pessoais por meio de *inteligência artificial* deve ser submetido aos mais elevados padrões de segurança, privacidade desde a concepção, avaliações de impacto, auditorias independentes e mecanismos de supervisão humana.

Um epílogo, eternamente, provisório

A relevância da Lei Geral de Proteção de Dados como base para a proteção do direito fundamental à privacidade e à segurança dos dados pessoais no Brasil é um dado de realidade que parece irrefutável, carregando em seu ventre os vetores interpretativos para a prevenção e a solução de problemas que, direta ou indiretamente, envolvem o

tratamento de dados pessoais capturados ou inferidos por sistemas de *inteligência artificial* com lastro naqueles.

Tais inferências, em especial quando decorrentes de sistemas de *inteligência artificial*, potencialmente afetam direitos e liberdades individuais, mormente no contexto da tecnologia generativa, apta a produzir textos, emular vozes e imagens com crescente perfeição, dado de realidade que exige a lapidação de critérios éticos e normativos ante o risco de discriminação e violação da privacidade, entre outras formas de lesão.

Outro ponto relevante consiste na exigência de consentimento expresso para o uso secundário de dados pessoais no treinamento de modelos de *inteligência artificial*, de modo a preservar a confiança e a autodeterminação informativa dos titulares dos dados.

O uso de *inteligência artificial* no tratamento de dados pessoais deve ser considerado como atividade de alto risco, a demandar a aplicação das mais rigorosas salvaguardas previstas na Lei Geral de Proteção de Dados, devido à escalabilidade, à opacidade e à autonomia imanentes à retrocitada tecnologia, sobremodo porque podem gerar impactos significativos aos direitos dos titulares dos dados utilizados.

A efetividade dos direitos fundamentais no contexto da *inteligência artificial* depende de uma regulação que atue nos campos da precaução e da prevenção, não apenas antecipando os desafios que surgirão no porvir, mas criando incentivos e moldando *nudges* que estimulem todas as personagens envolvidas, para que saiam da inércia fundida à natureza humana. Enfim, a *inteligência artificial* tem o potencial de transformar a sociedade de maneiras profundamente positivas, o que ocorrerá, entretanto, apenas se for desenvolvida e utilizada dentro de um quadro regulatório que priorize o bem-estar humano, leia-se, de todo ser humano.

Referências

BUSATTA, Eduardo Luiz. **Dados pessoais e reparação civil.** Rio de Janeiro: Forense, 2024.

CARTA DE BELÉM DO PARÁ. **XIII Agendas de Direito Civil Constitucional**. Belém do Pará: UFPA / CESUPA. 2024.

CASSINO, João Francisco. Modulação deleuzeana, modulação algorítmica e manipulação midiática. In: SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu da (Org.). **A sociedade de controle**: manipulação e modulação nas redes digitais. São Paulo: Hedra, 2021.

COELHO, Bernardo Leôncio Moura. O bloco de constitucionalidade e a proteção à criança. **Revista de Informação Legislativa**, Brasília, v. 31, n. 123, p. 259-266, jul./set. 1994.

CRUZ, Sylvio Augusto. Big data e o fim do livre arbítrio: a democracia manipulada. **Pensar Acadêmico**, Manhuaçu, v. 19, n. 3, p. 186-187, 2021.

DARMODY, Aron; ZWICK, Detlev. Manipulate to empower: hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. **Big Data & Society**, Hampshire, v. 7, n. 1, [*s.p.*], 2020.

DELEUZE, Gilles. **Conversações**. Trad. Peter Pál Pelbart. São Paulo: 34, 2008.

DOMINGOS, Pedro. **O algoritmo mestre**: como a inteligência artificial vai redesenhar o mundo. São Paulo: Novatec, 2015.

EHRHARDT JUNIOR, Marcos; CATALAN, Marcos; NUNES, Cláudia Ribeiro Pereira (Org.). **Inteligência artificial e relações privadas**: possibilidades e desafios. Belo Horizonte: Fórum, 2023.

EHRHARDT JUNIOR, Marcos; CATALAN, Marcos; NUNES, Cláudia Ribeiro Pereira (Org.). **Inteligência artificial e relações privadas**: relações existenciais e a proteção da pessoa humana. Belo Horizonte: Fórum, 2023.

EHRHARDT JUNIOR, Marcos; CATALAN, Marcos; NUNES, Cláudia Ribeiro Pereira (Org.). **Inteligência artificial e relações privadas**: relações patrimoniais: entre o consumo, os contratos e os danos. Belo Horizonte: Fórum, 2023.

FÜRST, Maria Eduarda; BÜRGUER, Marcelo. Inteligência artificial: conceitos introdutórios e algumas de suas aplicações. In: EHRHARDT JUNIOR, Marcos; CATALAN, Marcos; NUNES, Cláudia Ribeiro Pereira (Org.). **Inteligência artificial e relações privadas**: possibilidades e desafios. Belo Horizonte: Fórum, 2023.

GRUNDMANN, Stefan; MICKLITZ, Hans-Wolfgang; RENNER, Moritz. New private law theory: the core ideas. In: GRUNDMANN, Stefan; MICKLITZ, Hans-Wolfgang; RENNER, Moritz. **New private law theory**: a pluralist approach. Cambridge: Cambridge, 2021.

GUSTIN, Miracy; DIAS, Maria Tereza Fonseca. **Repensando a pesquisa jurídica**. 4. ed. Belo Horizonte: Del Rey Editora, 2013.

HAN, Byung-Chul. **A sociedade da transparência**. Trad. Enio Paulo Giachini. Petrópolis: Vozes, 2017.

HANSEN BECK, Felipe Quintela; BERNARDES, Marília Bengtsson. Reconhecimento da personalidade jurídica dos agentes artificiais autônomos como entes de capacidade reduzida. In: EHRHARDT JUNIOR, Marcos; CATALAN, Marcos; NUNES, Cláudia Ribeiro Pereira (Org.). **Inteligência artificial e relações privadas**: possibilidades e desafios. Belo Horizonte: Fórum, 2023.

HUR, Domenico Uhng. Deleuze e a constituição do diagrama de controle. **Fractal**, Niterói, v. 30, n. 2, p. 173-179, 2018.

JACOBSEN, Michael Hviid; TESTER, Keith. Introdução. In: BAUMAN, Zygmunt. **Para que serve a sociologia?** Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2015.

JESUS DIÁZ, María José Del; CORDÓN GARCIA, Óscar; HERRERA, Francisco. Una visión actual de la inteligencia artificial: recorrido histórico, datos y aprendizaje, y responsabilidad en el diseño y uso. In: PERALTA, Alfonso; SALVADOR TORRES, Leopoldo; HERRERA, Francisco (Org.). **El derecho y la inteligencia artificial**. Granada: Universidad de Granada, 2022.

KARJALAINEN, Tuulia. All talk, no action? The effect of the GDPR accountability principle on the EU data protection paradigm. **European Data Protection Law Review**, Berlin, v. 8, n. 1, p. 19-30, 2022.

KING, Jennifer; MEINHARDT, Caroline. **Rethinking privacy in the AI Era***:* policy provocations for a data-centric word. Disponível em: https://hai.stanford.edu/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world. Acesso em: 15 mai. 2024.

LACE, Susanne. **The glass consumer**: life in a surveillance society. Bristol: Policy, 2005.

MORIN, Edgar. **A cabeça bem-feita**: repensar a reforma, reformar o pensamento. Trad. Eloá Jacobina. 8. ed. Rio de Janeiro: Bertrand Brasil, 2003.

NISSENBAUM, Helen. Contextual integrity up and down the data food chain. ***Theoretical Inquiries in Law****, Berlin, v.* 20, p. 221-256, 2019.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard, 2015.

QUELLE, Claudia. The 'risk revolution' in EU data protection law: we can't have our cake and eat it, too. In: LEENES, Ronald et al. (Ed.). *Data* **protection and privacy**: the age of intelligent machines. London: Hart, 2020.

RUSSELL, Stuart; NORVIG, Peter. **Artificial intelligence***:* a modern approach. 3. ed. New Jersey: Pearson, 2010.

SANTOS, Isabela. A vulnerabilidade dos titulares de dados diante de grandes plataformas e big techs: um paralelo entre as violações ao GDPR e à LGPD no que tange à base legal do consentimento. **Revista dos Estudantes de Direito da Universidade de Brasília**, Brasília, v. 18, n. 1, p. 241-262, 2022.

SAUX, Edgardo Ignacio. La inteligencia artificial: un antes y un despues en el derecho. In: EHRHARDT JUNIOR, Marcos; CATALAN, Marcos; NUNES, Cláudia Ribeiro Pereira (Org.). **Inteligência artificial e relações privadas**: possibilidades e desafios. Belo Horizonte: Fórum, 2023.

SIBILIA, Paula. **O show do eu**: a intimidade como espetáculo. Rio de Janeiro: Nova Fronteira, 2008.

SILVEIRA, Sergio Amadeu da. **Tudo sobre todos**: redes digitais, privacidade e venda de sados pessoais (e-PUB). São Paulo: SESC, 2017.

STRECK, Lenio Luiz. **Dicionário de hermenêutica**: quarenta temas fundamentais da teoria do direito à luz da crítica hermenêutica do Direito. Belo Horizonte: Letramento / Casa do Direito, 2017.

SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. Technology, autonomy, and manipulation. **Internet Policy Review**, Berlin, v. 8, n. 2, [*s.p.*], 2019.

VÉLIZ, Carissa. Moral zombies: why algorithms are not moral agents. **AI & SOCIETY**, [*s.l.*]. n. 36, p. 487-497, 2021.

VÉLIZ, Carissa. **Privacy is power**: why and how you should take back control of your data. Londres: Transworld, 2020.

VERBICARO, Dennis; HOMCI, Janaina Vieira. O tratamento de dados pessoais por serviços simbióticos no consumo digital. **Revista de Direito do Consumidor**, São Paulo, v. 152, a. 33, p. 75-100, 2024.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. **Columbia Business Law Review**, New York, n. 2, [*s.p.*], 2019.

WINAU, Mona. Areas of tension in the application of AI and Data Protection Law. **European Data Protection Law Review**, Berlin, v. 9, n. 2, p. 123-135, 2023.

WOLFGANG, Hoffmann-Riem. **Teoria geral do direito digital**. Trad. Ítalo Fuhrmann. 2. ed. Rio de Janeiro: Forense, 2022.

ZANFIR, Gabriela. Forgetting about consent: why the focus should be on “suitable safeguards” in Data Protection Law. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (Ed.). **Reloading data protection**. [*s. l.*]: Springer / Dordrecht, 2014.

ZUBOFF, Shoshana. ***A era do capitalismo de vigilância***: a luta por um futuro humano na nova fronteira do poder. Trad. George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

Sobre os(as) autores(as):

Marcos Catalan | *E-mail:* marcoscatalan@uol.com.br

Pesquisador sênior (CNPq). Doutor summa cum laude pela Faculdade do Largo do São Francisco. *Visiting researcher* na *Università degli studi di Parma* (2025-2026). Estágio pós-doutoral na *Facultat de Dret da Universitat de Barcelona* (2015-2016) e no *Mediterranea International Center for Human Rights Research* (2020-2021). *Visiting Scholar* no *Istituto Universitario di Architettura di Venezia* (2015-2016). Cofundador da Rede de Pesquisas Agendas de Direito Civil Constitucional.

Marcos Ehrhardt Junior *E-mail:* marcosehrhardtjr@uol.com.br

Doutor em Direito pela Universidade Federal de Pernambuco. Professor de Direito Civil dos cursos de mestrado e graduação da Universidade Federal de Alagoas e do Centro Universitário Cesmac. Editor da Revista Fórum de Direito Civil. Cofundador da Rede de Pesquisas Agendas de Direito Civil Constitucional.

Eduardo Luiz Busatta | *E-mail:* elbusatta@gmail.com

Doutor em Direito Público pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos. Mestre em Direito Negocial pela Universidade Estadual de Londrina. Professor da Universidade Estadual do Oeste do Paraná. Procurador do Estado do Paraná.

Taxonomia

Marcos Catalan	Conceitualização; Curadoria de Dados; Análise Formal; Aquisição de Financiamento; Investigação; Metodologia; Administração de Projeto; Programas; Recursos; Supervisão; Validação; Visualização; Escrita (rascunho original); e, Escrita (revisão e edição)
Marcos Ehrhardt Junior	Conceitualização; Curadoria de Dados; Análise Formal; Aquisição de Financiamento; Investigação; Metodologia; Administração de Projeto; Programas; Recursos; Supervisão; Validação; Visualização; Escrita (rascunho original); e, Escrita (revisão e edição)
Eduardo Luiz Busatta	Conceitualização; Curadoria de Dados; Análise Formal; Aquisição de Financiamento; Investigação; Metodologia; Administração de Projeto; Programas; Recursos; Supervisão; Validação; Visualização; Escrita (rascunho original); e, Escrita (revisão e edição)

Datas do Processo Editorial / Editorial Process Dates

(Link do texto)

Data de submissão / Submission date: 11 de março de 2025

Data da Triagem de Diretrizes / Guidelines Screening Date: 11 de março de 2025

Data da Triagem de Qualidade / Date of Quality Screening: 11 de março de 2025

Data do Envio para Avaliação / Date of Submission for Evaluation: 22 de julho de 2025

Data da Primeira Avaliação / Date of First Evaluation:01 de agosto de 2025

Data da Segunda Avaliação / Date of Second Evaluation:05 de setembro de 2025

23 de setembro de 2025

Data do Envio para Correção / Date Sent for Correction:25 de novembro de 2025

Data de Aceite / Date of Acceptance:16 de dezembro de 2025

Corpo Editorial:

Editor-Chefe: J.P.B

Editora-Adjunta: L.S.G

Editora Associada: L.S.G.

Pareceristas: 3