REVISTA DIREITO MACKENZIE

ISSN 2317-2622 | RDM | Revista Direito Mackenzie | São Paulo | SP | 18(2) | e17135 | 2024
http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

PRIVACIDADE E SEGURANÇA PÚBLICA: NOTAS SOBRE OS LIMITES JURÍDICOS À VIGILÂNCIA DO ESTADO COM O USO DE INTELIGÊNCIA ARTIFICIAL

RECEBIDO EM:	30.5.2024
APROVADO EM:	9.10.2024

Giovani Saavedra

https://orcid.org/0000-0002-5269-3844
Universidade Presbiteriana Mackenzie
São Paulo, São Paulo, Brasil
E-mail: giovani.saavedra@saavedra.adv.br

Juliana Abrusio

https://orcid.org/0000-0002-3745-0748
Universidade Presbiteriana Mackenzie
São Paulo, São Paulo, Brasil
E-mail: juliana.abrusio@mackenzie.br

Chiara Battaglia Tonin

https://orcid.org/0009-0000-5555-3719
Universidade Presbiteriana Mackenzie
São Paulo, São Paulo, Brasil
E-mail: chiarabt@gmail.com

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

· GIOVANI SAAVEDRA
· JULIANA ABRUSIO
· CHIARA BATTAGLIA TONIN

Para citar este artigo: SAAVEDRA, G.; ABRUSIO, J.; TONIN, C. B. Privacidade e segurança pública: notas sobre os limites jurídicos à vigilância do estado com o uso de inteligência artificial. *Revista Direito Mackenzie*, São Paulo, SP, v. 18, n. 2, e17135, 2024. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

RESUMO: Este texto debate a necessidade de ponderação de direitos fundamentais por parte do Estado ao se utilizar de sistemas de inteligência artificial para execução de políticas públicas voltadas à segurança. Assim, o presente artigo tem como enfoque a tensão entre a vigilância contínua propiciada pelo emprego dos algoritmos e os direitos à privacidade e proteção de dados dos indivíduos. Por fim, analisa os riscos e desafios relacionados ao uso de algoritmos, tendo em vista a legislação aplicável e propostas em trâmite.

PALAVRAS-CHAVE: Vigilância; privacidade; algoritmos; segurança pública.

PRIVACY AND PUBLIC SECURITY: NOTES ON THE LEGAL LIMITS TO STATE SURVEILLANCE WITH THE USE OF ARTIFICIAL INTELLIGENCE

ABSTRACT: This paper discusses the need for the State to balance fundamental rights when using artificial intelligence systems to implement public security policies. Thus, this article focuses on the tension between continuous surveillance enabled by algorithms and individuals' rights to privacy and data protection. Finally, it analyzes the risks and challenges of using algorithms, considering the applicable legislation and pending proposals.

KEYWORDS: Surveillance; privacy; algorithms; public security.

1. Introdução

A contraposição entre liberdade e segurança permeia a vida em sociedade e não consiste em dilema propriamente novo – os argumentos contratualistas de Hobbes, Locke e

Rousseau anteciparam tal contenda (Honneth, 2017, p. 33-57; Lopes, 2016; Marques, 2019). Contudo, novos contornos foram conferidos à referida contraposição em razão das transformações vivenciadas pela sociedade pós-moderna, em grande parte associadas à liquidez (Bauman; Lyon, 2013) e perenidade da vigilância (Zuboff, 2019), que colocam em xeque a privacidade em face dos avanços da tecnologia.

O emprego de tecnologia para promoção de segurança pública pelo Estado não se trata de um movimento recente: câmeras (ainda rudimentares) eram instaladas para implantação de circuitos internos de televisão, tecnologia OCR para identificação de veículos roubados, entre inúmeros outros exemplos da aplicação prática de recursos tecnológicos no contexto das políticas públicas.

Entretanto, o desenvolvimento de novas tecnologias e o aperfeiçoamento daquelas já conhecidas potencializaram as possibilidades de vigilância, tanto em espaços públicos quanto privados. Os avanços não apenas permitiram o monitoramento contínuo – que, em sua essência, já desafiam direitos como privacidade e proteção de dados –, mas também viabilizaram o emprego de algoritmos preditivos e generativos, ampliando os riscos e impactos associados à constante vigilância, especialmente em razão de seus potenciais vieses e falhas.

Assim, o presente artigo tem como objetivo analisar os riscos associados ao uso de ferramentas de inteligência artificial para fins de segurança pública, especialmente aqueles relacionados à privacidade, proteção de dados e vieses discriminatórios. No que concerne à metodologia adotada para essa finalidade, utilizar-se-á do método hipotético-dedutivo de Popper (1982), comum em pesquisas jurídicas para cotejo das teorias associadas e identificação de base teórica sólida, embasada por revisão bibliográfica e análise de normas, regras e princípios, que norteiam o tema.

2. Privacidade e proteção de dados pessoais

Os contornos da ideia de privacidade admitem certa flexibilização e contêm insumos de diferentes perspectivas, inclusive jurídica, sociológica, filosófica, antropológica. Justamente em razão de sua natureza multidisciplinar, o termo "privacidade" é por vezes empregado de modo a condensar diferentes atributos da esfera pessoal do ser humano, incluindo sua intimidade e direito à proteção de dados pessoais.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

Contudo, a menção vaga à privacidade, desprovida de rigor acadêmico e conceitual no que concerne aos elementos que compõem a pessoalidade humana, combinada às demandas da sociedade informacional[1], contribui para uma indesejada generalização (Solove, 2021) – e, por que não dizer, banalização – do que se entende por particular, íntimo ou sagrado; consequentemente, pode-se dificultar a adequada proteção jurídica de tais atributos.

A distinção entre privacidade e intimidade encontra interessante fundamentação a partir da doutrina alemã, a qual discorre acerca da chamada teoria das esferas (*sphärentheorie*) de Heinrich Hubmann. Esta reconhece a privacidade por meio de três círculos concêntricos: *privatsphäre*, *intimsphäre* e *geheimsphäre*, de modo que o primeiro representa a esfera da privacidade, o segundo versa sobre a intimidade – sendo, portanto, mais restrito – e o terceiro, por sua vez, contempla a vida íntima em sentido estrito, envolvendo aspectos secretos e espirituais (Vieira, 2007, p. 30).

Tem-se, portanto, que a privacidade reflete apenas a parcela cognoscível da intimidade[2], referindo-se à concretização e consecução de elementos da intimidade por meio de atos efetivamente praticados e passíveis de divulgação, razão pela qual se situa no âmbito jurídico (Alonso, 2005, p. 17). A importância do conceito de privacidade remonta à ideia de propriedade e teve sua essência fortalecida por influência do liberalismo de Stuart Mill, embora ainda não figurasse como um direito autônomo (Sylvestre, 2013, p. 219). Isso porque tinha-se como intuito assegurar a neutralidade do Estado frente a questões privadas[3].

1 A título de contextualização, adotamos a interpretação de Manuel Castells, segundo o qual "[...] o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tomam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico" (Castells; Majer, 2023, p. 84).

2 Ainda que o presente artigo não tenha como intuito se ocupar dos contornos da intimidade, vale ressaltar que esta é entendida como "[...] o âmbito interior da pessoa mais profundo, mais recôndito, secreto ou escondido dentro dela. É, assim, algo inacessível, invisível, que só ela conhece [...]", consistindo, portanto, em um estágio pré-jurídico (Alonso, 2005, p. 17). Assim, Gilmar Ferreira Mendes esclarece que "[...] embora a jurisprudência e vários autores não distingam, ordinariamente, entre ambas as postulações – de privacidade e de intimidade –, há os que dizem que o direito à intimidade faria parte do direito à privacidade, que seria mais amplo. O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas. O direito à privacidade é proclamado como resultado da sentida exigência de o indivíduo "[...] encontrar na solidão aquela paz e aquele equilíbrio continuamente comprometido pelo ritmo da vida moderna" (Mendes, 2009, p. 420).

3 Nesse sentido, Miguel de Godoy ensina que "O liberalismo parte de dois pressupostos teóricos e dois pressupostos institucionais. Os primeiros dizem respeito a (i) sua severa desconfiança em relação ao poder coercitivo estatal e (ii) sua severa confiança nas capacidades de cada sujeito escolher o modo de vida que mais lhe aprouver. Os segundos dizem respeito (i) à defesa de uma declaração de direitos e (ii) à defesa de um sistema de freios e contrapesos".

A referida autonomização, contudo, foi posteriormente defendida por Samuel Warren e Louis Brandeis, por meio do artigo "Right to Privacy" publicado na *Harvard Law Review*, em 1890, com a manifestação do descontentamento da sociedade no que concerne à preservação de sua privacidade.

Contudo, o desenvolvimento da sociedade informacional apresenta novos desafios, demonstrando a insuficiência da abordagem proposta por Warren e Brandeis (Sylvestre, 2013, p. 221) e a necessidade de "reinventar a privacidade" (Abrusio, 2020, p. 129), despontando a necessidade de proteção de dados pessoais, que "[...] pode ser compreendida como uma dimensão do direito à privacidade, que, por consequência, partilha dos mesmos fundamentos: a tutela da personalidade e da dignidade do indivíduo" (Mendes, 2014, p. 35).

Assim, tem-se que o direito à privacidade é estático e se exaure na exclusão da interferência de terceiro (Rodotá, 2008, p. 7), ao passo que o direito à proteção de dados pessoais versa sobre a autodeterminação informativa, que "[...] confere ao indivíduo o poder de ele próprio decidir sobre a utilização e divulgação de seus dados pessoais" (Abrusio, 2020, p. 144). Verifica-se, portanto, que o objetivo maior em torno da proteção à esfera pessoal dos indivíduos é, em realidade, proteger sua liberdade, inclusive para o livre desenvolvimento de sua personalidade (Sarlet; Saavedra, 2020, p. 39).

O presente artigo não tem como intuito exaurir as considerações sobre o direito à privacidade *per se*, tampouco discorrer com profundidade sobre o que o distingue dos direitos à intimidade e à proteção de dados pessoais[4]. Contudo, cabe anotar que

"A desconfiança do liberalismo em relação à ação do Estado se dá pela sua preocupação em assegurar um âmbito de privacidade para cada pessoa. Ou seja, há uma clara preferência pela neutralidade do Estado no que diz respeito a questões privadas, tais como a opção religiosa, a propagação de ideias políticas etc. Dessa forma, cada indivíduo poderia escolher a melhor maneira de viver a sua vida sem sofrer qualquer tipo de interferência do Estado. O principal meio encontrado para assegurar a proteção da esfera privada e evitar ingerências estatais foi a consagração de certos direitos individuais invioláveis. Assim, o sujeito deve ser respeitado em seus reclamos mais básicos, independentemente dos demais. Essa postura põe o indivíduo em primeiro lugar, concebendo-o como um fim em si mesmo de tal forma que nada e nem ninguém podem sacrificá-lo em nome de outro sujeito ou grupo" (Godoy, 2012, p. 59).

4 No que concerne à distinção entre os direitos à privacidade e à proteção de dados pessoais, ressalta-se o entendimento de Peter Blume, segundo o qual "Privacy is concerned with the relationship between the individual and the collective, i.e. other people and traditionally in particular the state. (...) This autonomy implies that the individual has a right to exercise some degree of control in respect to others. (...) Data protection is specifically related to the legal rules that regulate to which extent and under which conditions information related to individual physical persons may be used. (...) In principle anybody may misuse personal data and all relationships ought to be regulated. Data protection is not only a limitation on the state" (Blume, 2010, p. 153-154). Tradução nossa: "A privacidade diz respeito à relação entre o indivíduo e o coletivo, ou seja, outras pessoas e, tradicionalmente, em particular, o Estado. (...) Essa autonomia implica que o indivíduo tem o direito de exercer algum grau de controle em relação aos outros. (...) A proteção de dados está especificamente relacionada às regras jurídicas que regulam até que ponto e sob quais condições as informações relacionadas a pessoas físicas podem ser utilizadas. (...) Em princípio, qualquer pessoa pode fazer mau uso de dados pessoais e todas as relações devem ser regulamentadas. A proteção de dados não é apenas uma limitação imposta ao Estado".

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

o legislador brasileiro se ocupou da regulação dos três[5], o que passamos a analisar no presente estudo para contextualização do problema.

Ao conferir proteção à intimidade e à vida privada, a Constituição Federal (Brasil, 1988) consagra o reconhecimento do direito à privacidade. Sua proteção também se situa no âmbito dos direitos da personalidade e se apresenta como um direito negativo, na medida em que exige abstenção, do Estado ou de terceiros (Bittar, 2014, p. 174). Ainda, verifica-se a tutela da privacidade no âmbito do direito penal, por meio dos artigos 150 a 154 do Código Penal (Brasil, 1940) e das normas de natureza processual, na concepção do segredo de justiça, conforme previsto no artigo 155 da Constituição Federal (Brasil, 1988), sem prejuízo das demais normas infraconstitucionais que tutelam o referido direito[6].

Assim, as disposições legais que apresentam como escopo a proteção ao direito à privacidade não disciplinam, de forma específica, o direito à proteção dos dados pessoais – que, diferentemente do direito à privacidade, não se restringe à natureza de direito negativo, sendo associado também à função de direito positivo ao demandar prestações por parte do Estado e terceiros. Nesse sentido, vale considerar o ensinamento de Sarlet (2020, p. 196):

> Já mediante uma simples leitura do catálogo que segue, enunciado nos arts. 17 e 18 da LGPD, é possível perceber que em grande medida as posições jurídicas subjetivas (direitos) atribuídas ao titular dos dados pessoais objeto da proteção legal, que concretiza e delimita, em parte, o próprio âmbito de proteção do direito fundamental à proteção de dados, coincidem com o rol de posições jurídico-constitucionais diretamente e habitualmente associadas à dupla função de tal direito como direito negativo (defesa) e positivo (a prestações).

Essa temática foi inicialmente contemplada pelo ordenamento jurídico brasileiro via legislação infraconstitucional para, somente em 2022, ser incluída expressamente no rol dos direitos fundamentais, por meio da Emenda Constitucional nº 115 (Brasil,

5 Sobre esse ponto, importa a lição de Álvaro Villaça Azevedo: "[...] entendo que essa enumeração não é taxativa; entretanto, é tão ampla que, praticamente, teve em mira abarcar toda violação à intimidade, à vida privada, quer dizer, aos direitos da personalidade, que se aninham na pessoa, como seu maior tesouro" (Azevedo, 2012, p. 33).

6 A título exemplificativo, destaca-se a Lei de Imprensa, assim denominada a Lei nº 5.250/1967, a Lei dos Direitos Autorais, correspondente à Lei nº 5.988/1973, o Estatuto da Criança e do Adolescente, Lei nº 8.069/1990, e a lei que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal (Brasil, 1988), concernente a interceptações telefônicas, a Lei nº 9.296/1996, bem como o Decreto nº 3.518/2000, que regulamenta o Programa Federal de Assistência a Vítimas e a Testemunhas, previsto no artigo 12 da Lei nº 9.807/1999.

2022), em que pese já fosse assim considerado de forma implícita por parte da doutrina (Sarlet, 2020, p. 186). Referido entendimento decorre de uma leitura sistemática e harmoniosa dos princípios e ditames constitucionais, que têm por essência a proteção de todas as dimensões da personalidade humana[7].

Assim, o *status* de direito fundamental conferido ao direito à proteção de dados pessoais por meio da Emenda Constitucional nº 115 (Brasil, 2022) representa uma atualização dos contornos da proteção à pessoa humana e seus atributos, como autonomia e liberdade (Bezerra Sales Sarlet; Molinaro, 2010, p. 206). Tais contornos ganham ainda mais cor a partir de uma análise sistemática do ornamento jurídico; como dissemos, mesmo antes da atualização constitucional, a legislação infraconstitucional já contemplava o direito à proteção de dados pessoais, de modo indireto em leis esparsas[8] e de forma específica, por meio da Lei Federal nº 13.709/2018, chamada Lei Geral de Proteção de Dados (Brasil, 2018).

Em linha com as discussões históricas em torno da privacidade no que concerne à restrição de ingerências estatais na esfera pessoal dos indivíduos, a aplicabilidade da Lei Geral de Proteção de Dados Pessoais não fica restrita à iniciativa privada, de modo que as disposições devem também ser observadas pelas entidades de direito público. Entretanto, o texto também estabelece hipóteses que afastam sua aplicabilidade, incluindo o tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (Brasil, 2018) – estas, portanto, diretamente relacionadas ao problema proposto por este artigo, dadas as iniciativas voltadas à vigilância contínua, com riscos potencializados pela aplicação de ferramentas de inteligência artificial, a exemplo do reconhecimento facial, como oportuna e pontualmente analisado adiante neste artigo.

Contudo, há que se considerar que a exceção legal abordada acima se restringe à aplicabilidade da lei infraconstitucional e de suas disposições de ordem operacional, não afastando o dever constitucional de observância aos direitos fundamentais à

7 Nesse sentido, tem-se que "[...] possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana, que, de acordo com tradição jurídica já consolidada no direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (mas não se limita ao!) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa (Mota Pinto, 2018, p. 642 e ss.)" (Sarlet; Saavedra, 2020, p. 43).

8 A respeito, destaca-se o Código de Defesa do Consumidor (Brasil, 1990), a Lei de Cadastro Positivo (Brasil, 2011), a Lei de Acesso à Informação (Brasil, 2011) e o Marco Civil da Internet (Brasil, 2014).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

privacidade – contemplado no bojo do direito à intimidade – e à proteção de dados pessoais. Significa dizer, portanto, que a ressalva legal não implica ampla e irrestrita liberdade ao Estado – bem como possíveis abusos – sob o manto das exceções; seu objetivo, em realidade, é reconhecer a importância de tais bens jurídicos e viabilizar sua efetiva proteção. Cabe anotar, nesse imbróglio, que o Estado deve ainda nortear suas ações pelo princípio constitucional da proporcionalidade, ponderando os direitos e interesses, individuais e coletivos, envolvidos em prol do bem comum.

Significa dizer, portanto, que mesmo as políticas públicas voltadas à segurança – que, por essência, têm o escopo de proteger o interesse coletivo – devem observar os limites jurídicos impostos ao Estado, inclusive no que concerne à observância e proteção de direitos individuais, como a intimidade, privacidade e proteção de dados pessoais. Contudo, os desafios associados à ponderação dos direitos e interesses envolvidos em tais iniciativas tornam-se ainda mais complexos quando compreendem o uso de recursos de vigilância ainda mais acurados, a exemplo do emprego de novas tecnologias, como a inteligência artificial empregada em reconhecimento facial, como passamos a analisar a seguir.

3. Inteligência artificial e seu impacto real

Assim, a ponderação que se propõe por meio deste artigo demanda a avaliação das benesses e infortúnios decorrentes da vigilância estatal: se, por um lado, a segurança propiciada pelo Estado confere conforto, equívocos ou abusos podem miná-lo por completo. Nesse sentido, busca-se enfocar o uso de ferramentas dotadas de inteligência artificial que, em um cenário ideal, permitiriam não apenas o monitoramento, mas a identificação precisa de indivíduos e, com isso, uma ação mais célere e assertiva por parte do Estado – a exemplo do reconhecimento facial a distância. Ocorre que essa mesma tecnologia, se mal-empregada ou desenvolvida, poderá perpetuar vieses discriminatórios (Achiume, 2020) e cometer injustiças.

Os riscos não se restringem à forma como a tecnologia é empregada; seu desenvolvimento é tão relevante – senão mais – do que as preocupações *a posteriori*, vez que os algoritmos não são eticamente neutros (Tsamados *et al*., 2020, p. 2). Isso porque, como ensina Luciano Floridi, a tecnologia é sempre projetada com base em valores implícitos ou explícitos, refletindo escolhas e convicções dos envolvidos em sua concepção

(Floridi, 2023, p. 2). Verifica-se, portanto, que os vieses discriminatórios presentes na inteligência artificial por vezes têm origem humana, inclusive decorrendo das crenças de seus desenvolvedores (Rutowitsch Beck *et al.*, 2022, p. 212).

Assim, a tecnologia não é neutra, vez que traz implicações éticas tanto positivas quanto negativas, gerando uma espécie de equilíbrio estático[9]. A compreensão dos componentes éticos que perpassam o desenvolvimento tecnológico e a natureza moral do processo de concepção permitem, portanto, uma avaliação mais lúcida dos riscos e impactos.

Assim, dentre as origens da valoração ética abordada acima, há que se considerar a composição das bases de dados empregadas para fins de treinamento dos modelos algorítmicos. Vale mencionar os estudos de Bolukbasi *et al.* (2016) e Caliskan *et al.* (2017), os quais abordam precisamente o impacto de dados enviesados no treinamento de algoritmos e consequente discriminação.

Nesse sentido, Bolukbasi *et al.* (2016) se utilizam da metodologia de *word embedding*, em que as palavras são representadas por vetores para processamento de linguagem natural e previsão dos elementos seguintes em uma sequência de texto, para demonstrar que, mesmo o treinamento a partir de dados coletados do Google News, gera resultados contendo estereótipos de gênero. Nesse mesmo sentido, os resultados obtidos por Caliskan *et al.* (2017) indicam que a própria linguagem contém impressões de nossos preconceitos históricos, sejam eles moralmente neutros em relação a insetos ou flores, problemáticos em relação à raça ou gênero, ou mesmo simplesmente verídicos.

Assim, os critérios éticos presentes em tais sistemas podem decorrer do aprendizado a partir de comportamentos humanos, ou de regras preestabelecidas pelos desenvolvedores; esta última abordagem, por sua vez, permite correlações de princípios

9 A esse respeito, Floridi (2023, p. 3) indica que "The static equilibrium or double-charge nature of technology looks like neutrality, but it is not. It is based on a tension between opposite forces, and such tension can be exploited to design the wanted equilibria. So, contrary to the neutrality thesis, the double-charged thesis places a significant responsibility on its designers, contrary to what my interlocutor seemed to think. For, it is designers who can have (at least some) control over the values that end up shaping (or equally importantly not shaping) what kind of double-charged technology will be used and how". Tradução nossa: "O equilíbrio estático ou a natureza de dupla carga da tecnologia parece neutralidade, mas não é. É baseado em uma tensão entre forças opostas, e tal tensão pode ser explorada para projetar os equilíbrios desejados. Assim, contrariamente à tese da neutralidade, a tese da dupla carga coloca uma responsabilidade significativa sobre seus projetistas, contrariamente ao que meu interlocutor parecia pensar. Pois são os projetistas que podem ter (ao menos algum) controle sobre os valores que acabam moldando (ou igualmente importante, não moldando) que tipo de tecnologia de dupla carga será usada e como".

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

éticos na própria arquitetura do sistema[10], de modo a nortear todo o seu ciclo de vida, desde a construção até o efetivo emprego cotidiano.

A precisão dos algoritmos por vezes varia quando da análise de dados relativos a minorias, sendo constatadas disparidades na precisão dos sistemas comerciais de classificação por gênero, ao utilizar conjuntos equilibrados por gênero e tipo de pele (Buolamwini; Gebru, 2018, p. 77-91). Considerando o emprego de inteligência artificial no contexto das políticas públicas, especialmente para reconhecimento facial, essa característica se torna ainda mais relevante, uma vez que a imprecisão poderia ensejar, por exemplo, identificação e eventual coerção errôneas.

Assim, importante considerar que a inteligência artificial é caracterizada justamente pelas técnicas de aprendizado de máquina (Mittelstadt *et al.*, 2016, p. 3), de modo que seu julgamento conta com reduzida ou nenhuma intervenção humana (Rutowitsch Beck *et al.*, 2022, p. 215); por essa razão, a previsão antecipada das ações dos algoritmos é comprometida, bem como posterior elucidação do racional que orientou a tomada de decisão (Mittelstadt *et al.*, 2016). Como ensinam Selbst e Barocas (2018, p. 1094), o aprendizado de máquina permite aos algoritmos a identificação de relações sutis em dados, com a aplicação de numerosas regras complexas e interdependentes para tomada de decisão, desafiando o entendimento humano (Selbst; Barocas, 2018, p. 1094).

Tem-se, assim, certa autonomia dos sistemas de inteligência artificial e, consequentemente, a imprevisibilidade de seus resultados, podendo obstar o mapeamento e correção de falhas e vieses em sua concepção e funcionamento (Mittelstadt *et al.*, 2016, p. 11).

Assim, as preocupações éticas relativas ao emprego da inteligência artificial incluem demandas de natureza epistemológica (relativas à qualidade e acuracidade dos dados processados pelos sistemas) e normativa (concernentes às consequências dos resultados, que podem ser injustas ou imprevisíveis), para além das questões associadas à rastreabilidade dos processos algorítmicos, que permeiam todo o debate (Tsamados *et al.*, 2020, p. 3).

10 A esse respeito, "[...] nessa abordagem, os princípios e as vedações são traduzidos em restrições incorporadas no design. Há uma complexidade que envolve essa alternativa, já que ela, de certa forma, requer que o sistema seja programado para responder a casos concretos. O sistema deve ser programado para reagir a determinada situação ou a um conjunto de situações. Nessa abordagem, a finalidade para a qual o sistema será desenvolvido deve contar para que a programação do sistema seja alinhada para casos concretos" (Rutowitsch Beck *et al.*, 2022, p. 212).

Ademais, mesmo resultados previsíveis e explicáveis representam riscos. O autoaprimoramento a partir da interação com um ambiente externo dinâmico (Gutierrez, 2020, p. 83), viabilizado pelas técnicas de aprendizado de máquina, permitem a inferência de informações sensíveis (Abrusio, 2020, p. 215) e atributos da personalidade (Marques; Mucelin, 2020, p. 417), ainda que o titular dos dados não os tenha compartilhado ou não tenha conhecimento da viabilidade técnica de tais inferências.

Além de viabilizarem o processamento de grande volume de dados e a identificação de padrões, os sistemas de inteligência artificial possibilitam inferências e predições, cuja relevância para políticas públicas é inquestionável, vez que municia o Estado de informações capazes de viabilizar uma atuação mais eficaz, proativa e direcionada. Por outro lado, este potencial traz ainda mais cor aos direitos à intimidade, privacidade e proteção de dados pessoais e, consequentemente, aos riscos de violação e discriminação.

Tais riscos ganham mais cor vez que são potencializados pela opacidade dos modelos algorítmicos[11], decorrente de sua natureza *black box*, ou caixa-preta (Abrusio, 2020, p. 20). Desse modo, advêm os entreveros associados à rastreabilidade e explicabilidade dos processos algorítmicos. Isso porque "[...] para além de serem explicáveis, é essencial que os sistemas de inteligência artificial sejam confiáveis" (Abrusio, 2020, p. 321).

A dificuldade em rastrear e explicar o processo de tomada de decisão pode obstar a identificação e correção de máculas, como vieses discriminatórios, inferências equivocadas, tratamento indevido de dados pessoais e violações a direitos de propriedade intelectual, por exemplo. Advém, assim, a *algocracia*[12], conforme ensina Abrusio (2020, p. 213):

> As maiores ameaças afetas ao fenômeno da algocracia consistem nas preocupações veladas e nas preocupações opacas. A primeira se relaciona com a maneira sobre a qual os dados pessoais dos indivíduos são coletados e usados pelos sistemas inteligentes automatizados, porquanto podem ser realizados de forma secreta e escondida, sem o devido consentimento ou outra base legal que o autorize. A segunda está relacionada com as bases racionais desses sistemas, uma vez

11 Destaca-se que o termo "opacidade" é comumente empregado para abordagem conjunta de diferentes características dos algoritmos que obstam, em alguma medida, o entendimento de seu funcionamento (Selbst; Barocas, 2018, p. 1090).

12 A algocracia refere-se ao "[...] termo inicialmente cunhado por A. Aneesh, em 2006, em sua obra Virtual Migration, para indicar os efeitos dos algoritmos no campo das relações de trabalho, e, posteriormente, desenvolvido por John Danaher, em 2016, para alargar o termo a fim de descrever 'a particular kind of governance system, one which is organised and structured on the basis of computer-programmed algorithms'" (Abrusio, 2020, p. 208).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

que a explicação de seu funcionamento permanece inacessível ou opaco, ou seja, a opacidade associada aos algoritmos.

A despeito dos riscos associados ao uso da inteligência artificial, a aplicação desta tecnologia nas esferas pública e privada é uma realidade posta e, em muitos casos, bem-sucedida. Dentre as experiências brasileiras no setor público, ressalta-se o emprego de algoritmos para organização do atendimento conforme prioridade legal em repartições públicas e implantação de semáforos inteligentes (Silveira, 2017, p. 273), bem como uso pelo Poder Judiciário – como o Projeto Victor, que classifica recursos extraordinários em temas de repercussão geral de maior incidência (STF, 2021).

Contudo, a aplicação dessa tecnologia para fins de vigilância estatal demanda uma análise mais detida, dado seu potencial impacto sobre direitos fundamentais e liberdade individual. A inteligência artificial pode ser utilizada para fins de vigilância e monitoramento, mas sua aplicação responsável requer a ponderação de riscos e benefícios, direitos e deveres, como passamos a avaliar.

4. Ponderação entre o público e o privado: a inteligência artificial como fronteira

A falibilidade dos sistemas e a reprodução de vieses discriminatórios podem ser amplificadas pela coleta massiva de dados e macular as iniciativas desta natureza – como já vem ocorrendo. A frequência com que tais riscos se materializam motivou, inclusive, a criação de repositórios globais de erros e incidentes envolvendo sistemas de inteligência artificial, como o AI Incident Database[13] e o AI Incidents Monitor[14].

Nesse ponto, situa-se a reflexão acerca da pertinência e dos limites aplicáveis ao uso de algoritmos de inteligência artificial pelo poder público (Melo; Serra, 2022, p. 205-220), tendo em vista os direitos à privacidade, intimidade e proteção de dados, que devem ser preservados e promovidos concomitantemente. Em que pese os benefícios da aplicação dessa tecnologia sejam notórios, seu emprego de forma inclusiva e não discriminatória impõe significativos desafios ao Estado.

13 Disponível em: https://incidentdatabase.ai. Acesso em: 12 maio 2024.

14 Disponível em: https://oecd.ai/en/incidents?search_terms=%5B%5D&and_condition=false&from_date=2014-01-01&to_date=2024-05-12&properties_config=%7B%22principles%22:%5B%5D,%22industries%22:%5B%5D,%22harm_types%22:%5B%5D,%22harm_levels%22:%5B%5D,%22harmed_entities%22:%5B%5D%7D&only_threats=false&order_by=date&num_results=20. Acesso em: 12 maio 2024.

Assim, a exceção à aplicabilidade da Lei Geral de Proteção de Dados Pessoais sobre as operações de tratamento para segurança do Estado, defesa nacional, segurança pública, investigação e repressão de infrações penais demonstra o reconhecimento do legislador sobre a particularidade dos desafios enfrentados pelo poder público nessa temática, reservando a discussão para normatização específica. Assim, o § 1º do artigo 4º da referida lei estabelece que a norma específica deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, em atenção ao devido processo legal, aos princípios gerais de proteção e aos direitos do titular.

Nesse contexto, cumpre salientar o teor do Projeto de Lei nº 1.515, de 2022 (Brasil, 2022), que se refere à regulamentação da exceção descrita acima. Em que pese o texto ainda se encontre em trâmite, importante considerar que a proposta veda, em seu artigo 20, "[...] a tomada de decisão realizada exclusivamente com base no tratamento automatizado, incluída a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa" (Brasil, 2022). Ainda nesse sentido, dentre outras previsões, destaca-se a vedação à adoção de qualquer medida coercitiva ou restritiva de direitos exclusivamente com base em decisão automatizada, conforme artigo 21, § 3º.

Verifica-se, portanto, que o texto proposto tangencia o emprego de inteligência artificial pelo Estado ao versar sobre decisões exclusivamente automatizadas – tal qual aquelas resultantes dos modelos algorítmicos. Assim, de acordo com a proposta, o emprego dessa tecnologia, a exemplo dos mecanismos de reconhecimento facial, deveria ser complementado pela revisão humana na tomada de decisão.

Contudo, o tema não se trata de contenda exclusivamente brasileira; os sistemas de inteligência artificial já são utilizados como ferramentas em políticas públicas em diversos países (Labati *et al.*, 2016, p. 24:1-24:39; Roberts *et al.*, 2021, p. 59-77). Aplicação comum dessa tecnologia no contexto do poder público pode ser verificada nas práticas de reconhecimento facial a distância (Solarova *et al.*, 2023, p. 625-635); a relevância dos riscos associados à utilização dos sistemas de inteligência artificial para esta finalidade se traduz, inclusive, na abordagem específica de tal aplicação no contexto dos normativos que buscam regular a inteligência artificial – a exemplo do regulamento europeu, chamado AI Act, em processo de aprovação e promulgação (European Parliament and Council, 2021).

Nesse mesmo sentido, o Projeto de Lei nº 2338, de 2023 (Brasil, 2023), considera os sistemas de identificação biométrica a distância em tempo real e em espaços

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

acessíveis ao público – portanto, tecnologias de reconhecimento facial – como de risco excessivo, vedando sua implementação e o uso. Contudo, vale destacar que o texto substitutivo incluiu exceções, permitindo o emprego de tais sistemas, por exemplo, em caso de flagrante delito de certos crimes, bem como recaptura de réus evadidos, cumprimento de mandados de prisão e de medidas restritivas ordenadas pelo Poder Judiciário (Brasil, 2024).

Nesse contexto, também se multiplicam as recomendações de entidades e organizações transnacionais[15] aplicáveis tanto à iniciativa privada quanto ao poder público, quando do emprego de sistemas de inteligência artificial.

A despeito da diversidade e do volume de orientações, Floridi e Cowls (2019, p. 4-5) sugerem que as iniciativas[16] se sobrepõem e podem ser consolidadas, de modo geral, em cinco princípios para uso ético da inteligência artificial, os quais enfatizam a necessidade de a tecnologia beneficiar a humanidade, com a adoção de medidas de precaução contra possíveis malefícios e promovendo justiça e igualdade; destacam a relevância da explicabilidade e transparência e indicam que o poder de decisão delegado aos sistemas deve se dar de forma responsável.

Assim, a aplicação prática de tais norteadores no desenvolvimento dos sistemas de inteligência artificial e no efetivo uso por parte do Estado mostra-se fundamental para que o emprego da tecnologia nas políticas públicas se dê de forma ética, inclusiva e responsável. Contudo, as responsabilidades associadas à construção de tais sistemas parece não se restringir ao Estado, vez que este deverá se valer da iniciativa privada para desenvolvimento e treinamento dos sistemas dada a especificidade e complexidade técnica da matéria (Silveira, 2017, p. 273).

Verifica-se, portanto, que o Estado exerce papel adicional ao empregar os sistemas de inteligência artificial em políticas públicas, devendo não apenas pautar suas estratégias em preceitos éticos em observância aos direitos fundamentais potencialmente impactados, mas também fiscalizar e exigir da iniciativa privada o mesmo rigor no

15 A título exemplificativo, vale referenciar a Recomendação sobre a Ética da Inteligência Artificial aprovada na Conferência Geral da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (United Nations Educational, Scientific and Cultural Organization – Unesco) em 2022, contendo valores e princípios para promoção da confiabilidade em todos os estágios do ciclo de vida dos sistemas de inteligência artificial. Dentre os valores, ressalta-se a garantia da diversidade e inclusão e, como princípios, a justiça e não discriminação.

16 Naquele estudo, mapearam-se seis iniciativas relativas ao emprego de inteligência artificial, as quais foram priorizadas por serem mais recentes, de maior credibilidade e aplicabilidade geral. A partir do mapeamento, identificaram-se 47 princípios que, em análise, poderiam ser consolidados em cinco, como sugerem os autores (Floridi; Cowls, 2019, p. 5).

desenvolvimento da tecnologia a ser disponibilizada ao mercado. Isso porque os possíveis riscos decorrentes do emprego da inteligência artificial e da coleta massiva de informações propiciada pela vigilância também contemplam desvios de finalidade e incidentes envolvendo o comprometimento das informações coletadas e geradas.

5. Conclusão

O poder público pode – e deve – buscar eficiência e se utilizar da tecnologia disponível para exercício de suas atribuições. Entretanto, ainda que o arcabouço legal excetue a segurança pública do escopo da Lei Geral de Proteção de Dados Pessoais, e ainda não haja norma específica promulgada sobre o tema, não significa dizer que as políticas direcionadas à sua preservação não devam considerar os direitos fundamentais aplicáveis – que incluem privacidade e proteção de dados pessoais.

A potencial contribuição da inteligência artificial às políticas públicas é notória ao maximizar a atuação do Estado por intermédio da tecnologia – por vezes, até mesmo com maior acuracidade do que o seu efetivo humano. Entretanto, há que se considerar que o processo algorítmico e a relativa autonomia conferida ao sistema em razão de autoaprimoramento também suscitam dilemas éticos – seja por reproduzir vieses discriminatórios humanos ou por falhas sistêmicas.

Dessa forma, verifica-se que o desenvolvimento e emprego da tecnologia pode, sim, ser viabilizado pela construção de sistemas que, desde a origem, observem valores e princípios que transcendem a regulação local ao versar, essencialmente, sobre direitos humanos. O Estado, portanto, ao empregar a tecnologia, deve se atentar a tais elementos e, ao se utilizar de soluções desenvolvidas pela iniciativa privada, exigir dela o mesmo rigor.

REFERÊNCIAS

ABRUSIO, J. *Proteção de dados na cultura do algoritmo*. São Paulo: D'Plácido, 2020.

ACHIUME, T.; UN. HUMAN RIGHTS COUNCIL. SPECIAL RAPPORTEUR ON CONTEMPORARY FORMS OF RACISM, R. D. *Racial discrimination and emerging digital technologies*: a human right analysis. Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance. 18 Jun. 2020.

ALONSO, F. R. Pessoa, intimidade e o direito à privacidade. *In*: MARTINS, I. G. da S.; PEREIRA JR., A. J. (coord.). *Direito à privacidade*. Aparecida: Ideia & Letras; São Paulo: Centro de Extensão Universitária, 2005.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

ANANNY, M.; CRAWFORD, K. Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 2016.

ARENDT, H. *A condição humana*. 10. ed. Rio de Janeiro: Forense Universitária, 2007.

AZEVEDO, A. V. *Teoria geral do direito civil*: parte geral. São Paulo: Atlas, 2012.

BAUMAN, Z.; LYON, D. *Vigilância líquida*. Rio de Janeiro: Zahar, 2013.

BEZERRA SALES SARLET, G., & MOLINARO, C. A. (2020). Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. *Revista Brasileira De Direitos Fundamentais & Justiça*, *13*(41), 183–212. https://doi.org/10.30899/dfj.v13i41.811

BITTAR, C. A. *Os direitos da personalidade*. 8. ed. Rio de Janeiro: Saraiva Jur, 2014.

BLUME, P. *Data protection and privacy* – basic concepts in a changing world, 2010. p. 151-164, v. 56.

BOLUKBASI, T. *et al*. Man is to computer *programmer as woman is to Hhmemaker?* Debiasing word embeddings. 2016. Disponível em: http://arxiv.org/abs/1607.06520. Acesso em: 6 out. 2024.

BRASIL. *Código Civil*. Lei n.º 10.406, de 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 24 nov. 2023.

BRASIL. *Código de Defesa do Consumidor*. Lei n.º 8.078, de 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acesso em: 30 nov. 2023.

BRASIL. *Código Penal* (1940). Decreto-lei n.º 2.848, de 7 de dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 27 nov. 2023.

BRASIL. *Constituição* (1988). Constituição da República Federativa do Brasil. Texto constitucional promulgado em 5 de outubro de 1988, atualizado até a Emenda Constitucional n.º 131/2023. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 nov. 2023.

BRASIL. *Emenda Constitucional n.º 115, de 10 de fevereiro de 2022*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 27 nov. 2023.

BRASIL. *Lei n.º 12.414, de 9 de junho de 2011*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 27 nov. 2023.

BRASIL. *Lei n.º 12.527, de 18 de novembro de 2011*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 27 nov. 2023.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 nov. 2023.

BRASIL. *Lei Geral de Proteção de Dados Pessoais*. Lei n.º 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 nov. 2023.

BRASIL. Câmara dos Deputados. *Projeto de Lei n.º 1.515, de 7 de junho de 2022*. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300&fichaAmigavel=nao. Acesso em: 6 out. 2024.

BRASIL. Senado. *Projeto de Lei n.º 2.338, de 3 de maio de 2023*. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 6 out. 2024.

BRASIL. Comissão Temporária Interna sobre Inteligência Artificial no Brasil. *Relatório Legislativo sobre o Projeto de Lei n.º 2.338, de 3 de maio de 2023*. Brasília: Senado, 2024. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9683716&ts=1726246478273&rendition_principal=S&disposition=inline. Acesso em: 6 out. 2024.

BROWN, S.; DAVIDOVIC, J.; HASAN, A. The algorithm audit: Scoring the algorithms that score us. *Big Data & Society*, v. 8, n. 1, p. 205395172098386, jan. 2021. Disponível em: https://doi.org/10.1177/2053951720983865. Acesso em: 11 nov. 2022.

BUOLAMWINI, J.; GEBRU, T. Gender shades: intersectional accuracy disparities in commercial gender classification. *In*: PROCEEDINGS OF THE 1ST CONFERENCE ON FAIRNESS, ACCOUNTABILITY AND TRANSPARENCY [*s.l.*]: PMLR, 2018, p. 77-91. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a.html. Acesso em: 15 mar. 2024.

BURRELL, J. How the machine 'thinks': understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, p. 205395171562251, 5 jan. 2016. Disponível em: https://doi.org/10.1177/2053951715622512. Acesso em: 30 nov. 2023.

CALISKAN, A.; BRYSON, J. J.; NARAYANAN, A. Semantics derived automatically from language corpora contain human-like biases. *Science*, v. 356, n. 6334, p. 183-186, 2017.

CASTELLS, M.; MAJER, R. V. *A sociedade em rede*. 24. ed. Rio de Janeiro: Paz & Terra, 2023.

EUROPEAN PARLIAMENT AND COUNCIL. *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. 2021.

FLORIDI, L.; COWLS, J. *A Unified Framework of Five Principles for AI in Society*. Issue 1, 23 jun. 2019. Disponível em: https://doi.org/10.1162/99608f92.8cd550d1. Acesso em: 30 nov. 2022.

FLORIDI, L. On good and evil, the mistaken idea that technology is ever neutral, and the importance of the double-charge thesis. *Philosophy & Technology*, v. 36, n. 3, p. 60, 2023.

FLORIDI, L.; TADDEO, M. What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, v. 374, n. 2083, p. 20160360, 28 dez. 2016. Disponível em: https://doi.org/10.1098/rsta.2016.0360. Acesso em: 30 nov. 2022.

GODOY, M. de. *Col. Direito, desenvolvimento e justiça*: série produção científica - constitucionalismo e democracia: uma leitura a partir de Carlos Santiago Nino e Roberto Gargarella. São Paulo: Saraiva, 2012.

GUTIERREZ, A. É possível confiar em um sistema de inteligência artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de accountability. *In*: FRAZÃO, A. de O.; MULHOLLAND, C. *et al.* (coord.). *Inteligência artificial e Direito*: ética, regulação e responsabilidade. 2. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2020.

HONNETH, A. *Das Recht der Freiheit. Grundriß einer demokratischen Sittlichkeit*. 3. ed. Frankfurt am Main: Suhrkamp, 2017.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

LABATI, R. D. *et al.* Biometric recognition in automated border control: a survey. *ACM Computing Surveys*, v. 49, n. 2, p. 24:1-24:39, 2016.

LOPES, H. F. Os conceitos de liberdade e segurança em Thomas Hobbes: conjunção ou disjunção? *In*: Observatório Político. *Working Paper #59*, mar. 2016. Disponível em: https://www.observatoriopolitico.pt/wp-content/uploads/2016/03/WP_59_HFL.pdf. Acesso em: 1º maio 2024).

MARQUES, C. L.; MUCELIN, G. Inteligência artificial e "opacidade" no consumo: a necessária revalorização da transparência para a proteção do consumidor. *In*: SILVA, R. da G.; TEPEDINO, G. (coord.). *O direito civil na era da Inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2020.

MARQUES, J. O. de A. Forçar-nos a ser livres? O paradoxo da liberdade no Contrato social de Jean-Jacques Rousseau. *In*: *Cadernos de Ética e Filosofia Política*, v. 1, n. 16, 2019, p. 99-114. Disponível em: https://www.revistas.usp.br/cefp/article/view/82596. Acesso em: 1º maio 2024.

MELO, P. V.; SERRA, P. Tecnologia de reconhecimento facial e segurança pública nas capitais brasileiras: apontamentos e problematizações. *Comunicação e sociedade*, n. 42, p. 205-220, 2022.

MENDES, G. F. *Curso de direito constitucional*. 4. ed. São Paulo: Saraiva, 2009.

MENDES, L. S. *Privacidade, proteção de dados e defesa do consumidor*. São Paulo: Editora Saraiva, 2014.

MITTELSTADT, B. D.; ALLO, P.; TADDEO, M.; WACHTER, S.; FLORIDI, L.. The ethics of algorithms: mapping the debate. *Big Data & Society*, jul./dez. 2016. p. 3 e ss.

MOTA PINTO, P. *Direitos de personalidade e direitos fundamentais*: estudos. Coimbra: Gestlegal, 2018.

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

POPPER, K. R. *Conjecturas e refutações*. Brasília: Editora Universidade de Brasília, 1982.

ROBERTS, H. *et al.* The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & SOCIETY*, v. 36, n. 1, p. 59-77, 2021.

RODOTÀ, S. *A vida na sociedade da vigilância*: a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSENAU, J. Governança, ordem e transformação na política mundial. *In*: ROSENAU, J.; CZEMPIEL, E-O. (org.). *Governança sem governo*: ordem e transformação na política mundial. Tradução Sérgio Bath. Brasília: Editora UnB/Imprensa Oficial do Estado, 2000.

RUTOWITSCH BECK, C. A. M.; MANZONI BOFF, M.; COVATTI PIAIA, T. Lei Geral de Proteção de Dados e a revisão de decisões automatizadas: os mecanismos de regulação baseados em uma inteligência artificial ética. *Revista Eletrônica Direito e Política*, [*s. l.*], v. 17, n. 2, p. 509-546, 2022. Doi: 10.14210/rdp.v17n2.p509-546. Disponível em: https://periodicos.univali.br/index.php/rdp/article/view/19067. Acesso em: 30 nov. 2023.

SARLET, I. W. *A eficácia dos direitos fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

SARLET, I. W. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. *Revista Brasileira de Direitos Fundamentais & Justiça*, v. 14, n. 42, p. 179-218, 10 ago. 2020.

SARLET, I. W.; SAAVEDRA, G. A. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. *Direito Público*, v. 17, n. 93, 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315. Acesso em: 12 maio 2024.

SCHERER, M. U. Regulating artificial intelligence systems: risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, [*s. l.*], p. 354-400, set. 2016.

SELBST, A. D.; BAROCAS, S. *The intuitive appeal of explainable machines*. Rochester, NY, 2 mar. 2018. Disponível em: https://papers.ssrn.com/abstract=3126971. Acesso em: 11 mar. 2024.

SERRANÍA, V. J.; ABRUSIO, J. Big data e a competição baseada em dados. *Revista de Direito Brasileira*, v. 28, n. 11, p. 387, 2021.

SILVEIRA, S. A. Governo dos algoritmos. *Revista de Políticas Públicas*, v. 21, n. 1, p. 267, jul. 2017.

SOLAROVA, S.*et al*. Reconsidering the regulation of facial recognition in public spaces. *Ai and Ethics*, v. 3, n. 2, p. 625-635, 2023.

SOLOVE, D. J. The myth of the privacy paradox. *George Washington Law Review*, v. 89, n. 1, p. 1-51, 2021.

STF. STF apresenta inovações em seminário sobre Corte Constitucional Digital. *Supremo Tribunal Federal*, 2021. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=464769&ori=1. Acesso em: 22 out. 2024.

SYLVESTRE, F. Z. O direito fundamental à privacidade em face da administração pública: uma análise à luz da teoria geral dos direitos fundamentais. *In*: LIMA, J. (coord.). *Direitos fundamentais*: uma perspectiva de futuro. São Paulo: Atlas, 2013.

TSAMADOS, A. *et al*. *The ethics of algorithms*: key problems and solutions. 2020. Disponível em: https://papers.ssrn.com/abstract=3662302. Acesso em: 12 maio 2024.

VIEIRA, T. M. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Ed., 2007.

ZUBOFF, S. *The age of suveillance capitalism*. Public Affairs: New York, 2019.

Giovani Saavedra

Professor do Programa de Pós-Graduação em Direito Político e Econômico da Universidade Presbiteriana Mackenzie (SP). Doutor em Direito e Filosofia pela Johann Wolfgang Goethe – Universidade de Frankfurt am Main. Mestre e graduado em Direito pela PUCRS. Sócio-fundador do Saavedra & Gottschefsky – Sociedade de Advogados. Lattes: http://lattes.cnpq.br/5594109824546097.
Universidade Presbiteriana Mackenzie
São Paulo, São Paulo, Brasil
E-mail: giovani.saavedra@saavedra.adv.br

Juliana Abrusio

Doutora em Direito pela Pontifícia Universidade Católica de São Paulo (2019). Mestra em Sistema Jurídico Romanístico, Unificação do Direito e Direito da Integração pela Università degli Studi di Roma Tor Vergata (2006), com diploma revalidado pela Universidade de São Paulo (2008). Pós-graduada em

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(2) | e17135
2024 | v. 18 | n. 2 | p. 1-20 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n217135

Direito Empresarial pela Universidade Presbiteriana Mackenzie (2003). Graduada em Direito pela Universidade Presbiteriana Mackenzie (2001). Professora da Faculdade de Direito e docente permanente do Programa de Pós-Graduação *Stricto Sensu* em Direito Político e Econômico da Universidade Presbiteriana Mackenzie. Lattes: http://lattes.cnpq.br/1847187277633756.
Universidade Presbiteriana Mackenzie
São Paulo, São Paulo, Brasil
E-mail: juliana.abrusio@mackenzie.br

Chiara Battaglia Tonin

Mestranda em Direito Político e Econômico na Universidade Presbiteriana Mackenzie. Especialista em Direitos dos Contratos pela Fundação Getúlio Vargas. Pesquisadora no IBChain – The Blockchain Authority e do Grupo de Pesquisa "Governança Corporativa, Compliance e Proteção de Dados" da Universidade Presbiteriana Mackenzie. Lattes: https://lattes.cnpq.br/6330724396442052.
Universidade Presbiteriana Mackenzie
São Paulo, São Paulo, Brasil
E-mail: chiarabt@gmail.com