

UMA PERSPECTIVA ANALÍTICA DA APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL (IA) À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Luize Gaggiola Nardi¹
Daniela Courtes Lutzky²

RESUMO

O presente artigo tem como objetivo analisar a aplicação da Inteligência Artificial (IA) no manuseio de dados pessoais, destacando os momentos históricos em âmbito nacional e europeu que incentivaram a criação da Lei Geral de Proteção de Dados Pessoais (LGPD). Dessa forma, utilizando-se do método dedutivo, apoiado em pesquisa doutrinária e jurisprudencial, sempre que possível, este artigo analisará os desafios quanto ao uso de ferramentas inteligentes na manipulação de dados pessoais. Ademais, será apresentado um cenário da IA como uma solução no vazamento de dados pela criação de instrumentos de segurança cibernética. Será exposta, ainda, uma análise quanto à responsabilização civil por danos causados por robôs, oportunidade em que será tratada a conveniência da atribuição de personalidade aos sistemas de IA, bem como a criação de um seguro de responsabilidade civil para tais danos. Discorrer-se-á, ao fim, acerca dos limites éticos na aplicação da IA no manuseio de dados pessoais.

Palavras chaves: Inteligência Artificial; Lei Geral de Proteção de Dados Pessoais; dados pessoais; segurança cibernética; método dedutivo.

SUMÁRIO: 1. Introdução; 2. Momentos históricos de maior relevância na proteção de dados pessoais; 2.1. A evolução da proteção de dados pessoais em cenário nacional e as influências provenientes da legislação europeia; 2.2. O contexto da necessidade de edição da Lei Geral de Proteção de Dados Pessoais (LGPD) e as suas finalidades; 2.3. A abrangência da LGPD e a categoria de dados que são abarcados pelo diploma legal; 3. A Inteligência Artificial (IA) e os ditames atuais referentes à proteção de dados pessoais; 3.1. O impacto do uso da Inteligência Artificial na proteção de dados pessoais; 3.2. Os desafios da conciliação da LGPD e a Inteligência Artificial; 4. A Inteligência Artificial como uma alternativa de solução no vazamento de dados pessoais; 4.1. O manuseio de dados pessoais pela Inteligência Artificial; 4.2. A criação de uma personalidade jurídica eletrônica (*E-personality*) atribuída aos sistemas de Inteligência Artificial; 4.3. A conveniência da criação de um seguro de responsabilidade civil relacionado à Inteligência Artificial; 5. Os limites éticos da aplicação da Inteligência Artificial no manuseio de dados pessoais; 6. Considerações finais.

1. INTRODUÇÃO

Os avanços tecnológicos revolucionaram a maneira através da qual os dados pessoais são processados. Dentro dessa conjuntura, o advento da Inteligência Artificial trouxe importantes impactos no manuseio desses dados e, principalmente, à Lei Geral de Proteção de Dados Pessoais. Tal análise demonstra a importância do tema do presente artigo diante do aumento exponencial de operações que passaram a fazer uso da Inteligência Artificial.

De início, o trabalho versará sobre o contexto em que a matéria de proteção de dados pessoais ganhou importância, perpassando por relevantes momentos históricos que

¹ Graduanda do Curso de Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). E-mail: luize.nardi@edu.pucrs.br.

² Orientadora do artigo. Doutora em Direito pela PUCRS. E-mail: daniela@jaegeradv.com.br.

impulsionaram o fomento por uma regulação específica sobre o assunto, que tutelasse o direito dos indivíduos à privacidade de seus dados.

A positivação constitucional da inviolabilidade da privacidade criou uma lacuna na legislação, uma vez que não existiam ferramentas aptas a garantir esse direito, dotado de um *status* com tamanha relevância. Portanto, o anseio pela criação de uma legislação nacional sobre o assunto cresceu paralelamente à previsão da privacidade com um direito de personalidade. Assim, será construída uma espécie de linha do tempo entre diversas legislações brasileiras, como a Lei do Cadastro Positivo e Código de Defesa do Consumidor, que auxiliaram a criação do que posteriormente viria a ser chamada de Lei Geral de Proteção de Dados Pessoais.

Nesse cenário, será sinalizada a intensa repercussão nacional da legislação europeia sobre o assunto, o Regulamento Geral de Proteção de Dados (RGPD) ou *General Data Protection Regulation (GDPR)*. Este diploma legal trouxe inúmeras previsões que seriam mais tarde transplantadas para a legislação brasileira sobre dados.

No contexto da matéria abordada pela LGPD, será realizado um exame quanto aos dados abarcados pela legislação, desde a definição de dados pessoais adotada pela legislação e suas respectivas nuances, até uma categoria mais específica e que, por exigir maior cuidado, ganhou uma significação própria, qual seja, a espécie dos dados sensíveis. Nesse sentido, restará constatado que as presentes circunstâncias não poderiam excluir a previsão de algo que está gradativamente ganhando mais atenção, o manuseio dos dados pessoais pela Inteligência Artificial.

Desse modo, será efetuada uma análise dos atuais ditames entre a proteção de dados e a IA e se perceberá que existe, hodiernamente, uma discussão bastante controversa quanto à revisão das decisões alcançadas por sistemas de Inteligência Artificial, denominadas pela doutrina como decisões automatizadas.

A despeito da existência de percalços na aplicação da IA ao manuseio de dados, os avanços tecnológicos trazidos pelas ferramentas inteligentes possibilitaram a criação de inúmeros instrumentos de segurança cibernética. Será realizada, assim, uma análise quanto à eventual possibilidade da IA ser utilizada como um mecanismo de prevenção ao vazamento de dados, agindo como uma aliada à LGPD.

Da mesma maneira, se demonstrará imprescindível discorrer acerca da responsabilização civil por danos causados por ferramentas inteligentes. Isso, porque diversas operações, como a mensuração dos riscos nos seguros, são realizadas por robôs e independem da racionalidade humana. Assim, serão expostas discussões com relação à atribuição de personalidade aos sistemas de Inteligência Artificial, bem como quanto à conveniência da criação de um seguro de responsabilidade civil relacionado à Inteligência Artificial.

Ao fim, serão traçados os limites éticos da aplicação da IA ao manuseio de dados, uma vez que a matéria da ética de dados pressupõe a utilização consciente das ferramentas inteligentes, observando ao máximo a IA como um objeto a ser conduzido pela racionalidade humana e em prol da vontade humana.

Assim, a partir de um método dedutivo, efetuado mediante pesquisa jurisprudencial e bibliográfica, tem o presente artigo o objetivo de analisar a eficácia e os desafios da aplicação da IA à LGPD, apresentando situações práticas que buscam a reflexão acerca das nuances do tema, desde a responsabilização por eventuais danos causados pelos robôs até os limites éticos da discussão.

2. MOMENTOS HISTÓRICOS DE MAIOR RELEVÂNCIA NA PROTEÇÃO DE DADOS PESSOAIS

A preocupação com relação à tutela da privacidade surgiu quando se percebeu que a privacidade é um pressuposto do exercício de liberdades individuais. Na década de 1940, o

professor Georges Ripert, professor e reitor da Faculdade de Direito de Paris, já advertia que “quando o direito ignora a realidade, a realidade se vinga, ignorando o direito”³. Nesse contexto, mudanças políticas, sociais e econômicas acarretaram no reconhecimento de novos direitos para que fosse possível a adaptação do sistema jurídico com as demandas da sociedade.

Primordialmente, a tutela da privacidade esteve intimamente relacionada à proteção da propriedade, cenário em que a defesa do domicílio foi considerada elemento substancial, a partir da qual seria possível a proteção do homem perante o Estado e terceiros.

A subsunção do direito à privacidade como um direito patrimonial fez com que se tornasse uma prerrogativa reservada a uma camada social mais abastada. Sugere-se que isso é decorrente da função do instituto do direito à privacidade estar na mão de alguns poucos, sendo, costumeiramente, utilizado por celebridades que tinham informações pessoais vazadas⁴.

Esse viés patrimonial do direito à privacidade trouxe consigo um aspecto de caráter individualista e até elitista, que veio a sofrer uma mudança em meados da década de 1960 com o fomento do desenvolvimento tecnológico e consequente criação de métodos com maior capacidade de recolher, processar e utilizar as informações. Assim, a camada social mais abastada da sociedade deixou de ser o único enfoque dessa ofensa à privacidade, passando a ser uma parcela muito maior da população⁵.

Como obra emblemática que marcou o início da discussão do direito à privacidade na modernidade, destaca-se o artigo de Louis Dembitz Brandeis e Samuel Dennis Warren, *The right to privacy*⁶, publicado em 1890. Nele, possível verificar que o desenvolvimento das leis que visavam proteger dados pessoais foi inevitável. Foi citado como exemplo as empresas jornalísticas, que impulsionaram o interesse da população por especulações acerca da vida alheia, as quais, mesmo quando aparentemente inofensivas, no momento em que são reiteradamente circuladas, tornam-se invasivas e hostis.

Resta constatado, desse modo, que a importância no que tange à regularização ou criação de diplomas legais que assegurassem aos indivíduos uma tutela quanto a sua vida privada surgiu quando do interesse de terceiros em dados pessoais alheios, tanto fosse por questões pessoais, quanto financeiras, políticas ou econômicas. Tal interesse, conforme Danilo Doneda, é justificado por dois fatores, o controle e a eficiência⁷. É o que se passa a explicar.

No princípio, havia a predominância do uso estatal de informações pessoais. Isso, porque o custo para a coleta e processamento dos dados era bastante elevado para empresas privadas. Assim, evidente que o conhecimento apurado da população pela realização de, por exemplo, censos e pesquisas, aumentou exponencialmente a eficiência da administração pública. Não obstante, o conhecimento de dados e informações particulares aumentou o poder de controle do Estado sobre a vida das pessoas.

O desenvolvimento de novas tecnologias informáticas, contudo, facilitou a coleta de dados pessoais, diminuindo os custos relacionados à operação e aumentando o leque de possibilidades de utilização dessas informações.

Nesse cenário, percebe-se que atualmente o perfil da utilização de dados pessoais mudou substancialmente, uma vez que há uma série de interesses que giram em torno dessas

³ RIPERT, Georges. **Aspectos Jurídicos do Capitalismo Moderno**. São Paulo: Red Livros, 2002, p. 33.

⁴ VITALIS, André. **Informartique, pouvoir et libertés**. Paris: Econômica, 1981, p. 148.

⁵ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. E-book. 2. Ed. São Paulo: Thomson Reuters, 2020.

⁶ WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The right to privacy. **Harvard Law Review**, Boston, vol. 4, n. 5, 1890, p. 193–220. Disponível em: <https://www.jstor.org/stable/1321160>. Acesso em: 25 mar. 2023.

⁷ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. E-book. 2. ed. São Paulo: Thomson Reuters, 2020.

informações, não exclusivamente o estatal. Nesse sentido, conforme dita Stefano Rodotà⁸, a tutela da privacidade ultrapassou o quadro individualista e se alongou para uma proteção coletiva de um indivíduo que se vê imerso em um grupo social.

No Brasil, o fomento por uma maior proteção da tutela da privacidade cresceu paralelamente à positivação desse instituto jurídico como um direito de personalidade, através da sua previsão constitucional no artigo 5º, inciso X⁹, como um direito inviolável e sua alusão específica no artigo 21 do Código Civil de 2002¹⁰. Assim, passa-se a analisar o crescimento da importância do tema da tutela da privacidade de dados pessoais em cenário nacional, sendo indispensável traçar um paralelo das influências provenientes da União Europeia, berço do tema da proteção de dados.

2.1. A EVOLUÇÃO DA PROTEÇÃO DE DADOS PESSOAIS EM CENÁRIO NACIONAL E AS INFLUÊNCIAS PROVENIENTES DA LEGISLAÇÃO EUROPEIA

O tema jurídico da proteção de dados remonta à década de 70, quando da edição da Lei de Proteção de Dados do Estado alemão de Hesse (*Hessisches Datenschutzgesetz*), considerada o primeiro diploma legal a tratar sobre essa disciplina jurídica. Sob o protagonismo do jurista Spiros Simitis, conhecido como o “Pai da proteção de dados”, relata-se que o contexto da edição da referida lei se deu quando da modernização de hospitais públicos, que dispunham de uma multiplicidade de dados, sobretudo dados sensíveis¹¹.

O prestígio de Spiros Simitis à época se evidenciou, do mesmo modo, pela decisão proferida pelo Tribunal Constitucional Federal Alemão, durante sua gestão, no famoso caso do censo demográfico de 1983¹², em que foi reconhecido o direito fundamental à autodeterminação informativa, pensado para garantir aos cidadãos o controle do alcance da repercussão de um dado pessoal, uma vez que uma ordem social, na qual os cidadãos não tivessem mais controle sobre os seus dados, não seria compatível com a autodeterminação na informação.

Ao analisar o caso, o Tribunal adotou o entendimento de que os avanços tecnológicos resultariam numa capacidade de processamento de dados nunca antes visitada, o que, certamente, acarretaria no reexame e reinterpretção de princípios e direitos fundamentais, ocasionados pelo surgimento de riscos à vida privada.

Nesse sentido, segundo dados da Pesquisa Nacional por Amostra de Domicílios realizada em setembro de 2022¹³, 90% dos lares brasileiros já tem acesso à internet no Brasil,

⁸ RODOTÀ, Stefano. *Tecnologie e diritti*. Bologna: Il Mulino, 1995, p. 22 – 23 *apud* DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. *E-book*. 2. ed. São Paulo: Thomson Reuters, 2020.

⁹ Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

¹⁰ Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

¹¹ DONEDA, Danilo. Fundamentos teóricos e históricos da proteção de dados pessoais. *In*: BIONI, Bruno; MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (Coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. *E-book*. ISBN 9788530992200. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 02 abr. 2023. p. 22 – 23.

¹² MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados do mundo. *In*: MIGALHAS, [s.l.], 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo>. Acesso em: 23 abr. 2023.

¹³ BRASIL. Casa Civil. **90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa**. Brasília: Casa Civil, 2022. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa>. Acesso em: 15 abr. 2023.

o que significa, em outras palavras, que são 65,6 milhões de domicílios conectados. Não há dúvidas que o advento da tecnologia facilitou e tornou mais céleres diversas atividades que antes exigiam mais tempo para serem feitas. Essa facilidade, contudo, trouxe consigo novas práticas ilícitas, que têm como principal instrumento os meios informáticos.

Tendo isso em vista, surgiu a necessidade de adaptação das leis à realidade cibernética, a fim de assegurar aos cidadãos uma proteção adequada na seara tecnológica. Assim, passa-se, agora, à análise da evolução do tema da proteção de dados e privacidade na legislação brasileira e, por derradeiro, o contexto em que a Lei Geral de Proteção de Dados Pessoais (LGPD)¹⁴ veio a ser implementada em cenário nacional. Para isso, traçar-se-á uma breve análise da presença do tema da proteção de dados em esfera constitucional e infraconstitucional.

As primeiras constituições brasileiras iniciaram o tratamento do tema com o sigilo das correspondências. Nesse sentido, como exemplo, a Constituição do Império de 1824, que garantia a inviolabilidade do Segredo das Cartas. A Constituição de 1891, por sua vez, conservou a inviolabilidade das correspondências e atribuiu ao domicílio dos cidadãos o *status* de asilo inviolável, o que perdurou nas Constituições de 1934, 1946 (Constituição dos Estados Unidos do Brasil) e 1967 (Constituição “Militar”).

A Constituição da República Federativa do Brasil de 1988 assegurou aos cidadãos brasileiros a inviolabilidade da intimidade, privacidade, honra e imagem, protegendo a esfera particular da ingerência de terceiros, bem como trouxe o debate referente ao *habeas data*, que garantiu a pessoas físicas e jurídicas o direito à retificação das suas informações¹⁵.

O século XXI, no entanto, trouxe um maior risco à invasão da privacidade dos indivíduos, causado principalmente pelo aumento dos meios de coletas de informação, o que possibilitou uma publicização de relações e a conseqüente intensificação da cobiça de terceiros pelos dados dos cidadãos. A necessidade de uma regulação específica acerca da proteção de dados pessoais mostrou-se inevitável. E tal incumbência foi assumida pela legislação infraconstitucional, como se passará a demonstrar.

2.2. O CONTEXTO DA NECESSIDADE DE EDIÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E AS SUAS FINALIDADES

Com a entrada do século XXI, revelou-se uma 4ª Revolução Industrial, marcada pela fusão de diferentes tecnologias e uma correlação entre os domínios físicos, digitais e biológicos. Tal movimento foi marcado pelas ideias do engenheiro e economista Klaus Schwab¹⁶, que afirmou que essa corrente se expressou como uma mudança crucial na forma como os valores são criados e distribuídos, bem como que acarretaria no surgimento de desafios para os Estados-Nação.

Nesse sentido, a mudança do cenário mundial, decorrente da facilitação na troca de informações entre os países, ocasionou uma internacionalização de dados pessoais, de modo que os diferentes países precisaram adaptar seus diplomas legais no intuito de assegurar aos cidadãos uma maior segurança nas transações das mais diversas naturezas entre nações.

¹⁴ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 02 abr. 2023.

¹⁵ DONEDA, Danilo. Fundamentos teóricos e históricos da proteção de dados pessoais. In: BIONI, Bruno; MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (Coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. *E-book*. ISBN 9788530992200. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 02 abr. 2023. p. 22 – 23.

¹⁶ SCHWAB, Klaus. The Fourth Industrial Revolution - FOREWORD. **Journal of International Affairs Editorial Board**, Nova Iorque, v. 72, n. 1, 2018, p. 13. Disponível em: <https://www.jstor.org/stable/26588338>. Acesso em: 15 abr. 2023.

Em âmbito nacional, antes de existirem dispositivos legais que tratassem especificamente da relação entre o direito e as novas tecnologias, o tema da proteção de dados era, de forma recorrente, utilizado na seara do direito do consumidor. O Código de Defesa do Consumidor de 1990 dispôs sobre o direito do consumidor de obter acesso às informações e dados pessoais constantes em cadastros, fichas e registros¹⁷. Isso canalizou a edição da Lei 12.414/2011¹⁸, ou Lei do Cadastro Positivo, que abriu espaço para debate com relação à definição de objetividade, clareza e fácil compreensão das informações, bem como sua sensibilidade ou excessividade.

No mesmo ano foi editada a Lei 12.527/2011¹⁹, ou Lei de Acesso à Informação, que tratou do princípio da transparência quanto ao tratamento de informações pessoais, com respeito à intimidade, vida privada, honra e imagem das pessoas. Constatou-se a aparição da figura do consentimento, que seria posteriormente detalhada pela Lei Geral de Proteção de Dados.

Nessa perspectiva, em 2014, com o objetivo de estabelecer um diálogo entre o Direito e a internet, foi promulgada a Lei 12.965/2014²⁰, também conhecida como Marco Civil da Internet (MCI). A sua importância se revela na tentativa do legislador de regulamentar as interações concebidas no meio virtual da Internet. Essa legislação trouxe uma breve alusão aos dados pessoais, matéria que viria a ser legislada em diploma legal específico.

Dentro dessa conjuntura, constatou-se a necessidade de uma proteção mais pontual concernente ao livre desenvolvimento da personalidade da pessoa natural, bem como da padronização de regulamentos e práticas para promover uma proteção dos dados pessoais dos cidadãos brasileiros.

Diante disso, em 2018, quando entrou em vigor o Regulamento Geral de Proteção de Dados (RGPD) ou *General Data Protection Regulation (GDPR)*²¹, cresceram os clamores pela criação de uma norma brasileira que visasse especificamente a proteção de dados. Nesse sentido, por iniciativa do responsável pelo Projeto de Lei nº 53, deputado Milton Monti, que viria a ser convertida na LGPD, entra em vigor, em setembro de 2020, a primeira lei de proteção de dados no Brasil, a Lei nº 13.709/2018 (LGPD).

O mencionado diploma legal, com o intuito de estabelecer uma proteção abrangente e, simultaneamente, pontual, dividiu os dados pessoais em diferentes categorias. Tal divisão levou em consideração alguns aspectos, como o grau de complexidade e sensibilidade dos dados, a partir dos quais é possível estabelecer uma tutela maior dessas informações. Passa-se agora à análise das espécies de dados abarcadas pela Lei Geral de Proteção de Dados.

¹⁷ Art. 43: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

¹⁸ BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm. Acesso em: 15 abr. 2023.

¹⁹ BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 15 abr. 2023.

²⁰ BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 15 abr. 2023.

²¹ UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretriz 95/46/CE. **Jornal Oficial da União Europeia**, Estrasburgo, 04 maio 2016. Disponível em: <https://gdpr-info.eu/>. Acesso em: 15 abr. 2023.

2.3. A ABRANGÊNCIA DA LGPD E A CATEGORIA DE DADOS QUE SÃO ABRACADOS PELO DIPLOMA LEGAL

A Lei Geral de Proteção de Dados Pessoais adotou um conceito abrangente de dado pessoal, assim como o Regulamento europeu (GDPR) em seu Considerando 26²², sendo ele descrito como uma informação atrelada a uma pessoa natural identificada ou identificável²³. O conceito de identificabilidade pode ser extraído do art. 4º, (1) da GDPR, que dita que uma pessoa singular identificável:

[...] is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person²⁴.

Da análise do mencionado diploma, conclui-se que se tratam de dados sobre uma pessoa singular que, num primeiro olhar, não aparentam ser relevantes, mas uma vez cruzados ou organizados, têm o condão de resultar em dados específicos sobre ela, capazes de determinar a identidade de seu titular.

Em seguida, a LGPD trouxe a definição de dado pessoal sensível, atribuindo mais proteção em decorrência de seu maior potencial lesivo ao titular, se expostas essas informações sem o seu consentimento. Essa categoria de dados abarca elementos informacionais pessoais relativos às perspectivas, concepções e ideologias de um sujeito, e traz consigo a exigência da figura do consentimento do titular do dado, trazendo hipóteses taxativas nas quais esta anuência é dispensável, para que se garanta mais segurança a essas informações.

A jurisprudência do Supremo Tribunal de Justiça (STJ) é uníssona no sentido que os dados pessoais sensíveis são aqueles previstos no art. 5º, inciso II da LGPD, que preceitua o seguinte:

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

O entendimento do Colendo Tribunal delimitou a definição de dados sensíveis, excluindo da categoria os dados pessoais de natureza comum, mas não íntimos, passíveis apenas de identificação de pessoa natural. Veja-se:

PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. **DADOS COMUNS E SENSÍVEIS**. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais. II - A sentença julgou os pedidos improcedentes, tendo

²² *Recital 26: The principles of data protection should apply to any information concerning an identified or identifiable natural person.* Tradução nossa: “Considerando 26: Os princípios de proteção de dados devem ser aplicados a qualquer informação relativa a uma pessoa física identificada a identificável”.

²³ TEFFÉ, Chiari Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro v.9, n.1, 2020, p. 2. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em: 15 abr. 2023.

²⁴ Tradução nossa: “é aquela que pode ser identificada direta ou indiretamente, nomeadamente por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador em linha ou uma ou mais características especiais que exprimam a identidade física, fisiológica, genética, psicológica, econômica, cultural ou social dessas pessoas singulares”.

a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa. [...] **IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais, mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis.** V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido²⁵. (Grifou-se).

No mesmo sentido, a Lei do Cadastro Positivo dispõe, em seu art. 3º, § 3º, inciso II, que “informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas”.

Outra espécie de dado trazido pela LGPD é o dado anonimizado, que, conforme o art. 5º, inciso III, é o “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. Contudo, de acordo com o art. 12 da LGPD²⁶, os dados anonimizados não são considerados dados pessoais, de modo que a proteção legal não se estende a eles. Nesse sentido, os dados perdem sua pessoalidade se tiverem sido tornados anônimos e não puderem mais ser desanonimizados²⁷.

A LGPD partiu da concepção de que todo dado pessoal tem importância e valor. Por esse motivo, adotou como regra geral, em seu primeiro artigo²⁸, que qualquer pessoa que trate dados pessoais, seja ela natural ou jurídica, de direito público ou privado, inclusive nos meios digitais, deverá ter uma base legal para fundamentar os tratamentos desses dados, sempre com o cerne de proteger os direitos fundamentais da liberdade e privacidade, garantindo aos titulares dos dados o direito à autodeterminação informativa.

Nesse sentido, surge uma preocupação referente aos potenciais interesses que os agentes que controlam e operam esses dados poderiam vir a ter sobre essas informações. Não obstante todos os meios previstos pela LGPD para evitar o uso desses dados de maneira inidônea, bem como as sanções previstas na Resolução nº 4 da Autoridade Nacional de Proteção de Dados (ANPD), a tarefa de controle de dados, quando manuseada pela mente humana, está suscetível a prejulgamentos dotados de certa arbitrariedade.

Na era das hipertecnologias mostra-se cada vez mais inverossímil que a LGPD, estatuto dirigido à proteção da pessoa humana, ignore o tratamento de dados baseado em decisões automatizadas. Nessa conjuntura, ganha destaque a figura da Inteligência Artificial (IA), dotada

²⁵ BRASIL. Supremo Tribunal de Justiça (2ª Turma). **Agravo em Recurso Especial nº 2130619 SP 2022/0152262-2**. Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravada: Maria Edite de Souza. Relator: Ministro Francisco Falcão. Brasília. Data do julgamento: 07 de março de 2023. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp>. Acesso em: 14 maio 2023.

²⁶ Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

²⁷ HOFFMANN-RIEM, Wolfgang. Big data e Inteligência Artificial: desafios para o direito. Tradução por: Gabriella Bezerra Sales Sarlet e Carlos Alberto Molinaro. **Revista de Estudos Institucionais**, [s.l.], v. 6, n. 2, p. 431 – 506, maio/ago.2020. DOI: 10.21783/rei.v6i2.484. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/484>. Acesso em: 22 abr. 2023.

²⁸ Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

da “habilidade de acumular experiências próprias e extrair delas aprendizado, como um autodidata”²⁹. Dessa forma, mostra-se aconselhável o exame da aplicação da Inteligência Artificial à LGPD como meio de promoção da proteção de dados e é o que se passa a analisar.

3. A INTELIGÊNCIA ARTIFICIAL (IA) E OS DITAMES ATUAIS REFERENTES À PROTEÇÃO DE DADOS PESSOAIS

Em 2015, quando o Google Fotos, serviço de compartilhamento e armazenamento de fotos desenvolvido pela Google, foi disponibilizado, um episódio demonstrou uma grande irregularidade e instabilidade no software: um sujeito, ao carregar fotos com sua amiga no sistema, ambas as pessoas envolvidas negras, constatou que o sistema havia vinculado suas fotos à denominação “Gorilas”³⁰.

Irresignado com a situação, o usuário, que dizia entender a essência do problema, fez uma reclamação no Twitter, questionando qual teria sido a base de dados de amostra que teria alimentado o sistema para que resultasse nesse resultado. A Google se disse “triste e constrangida”, bem como que trabalharia para que esse tipo de situação não voltasse a ocorrer.

É inegável a existência de diversos impasses quando se incumbe a uma pessoa natural a tarefa de manejar dados pessoais de um terceiro. Isso, porque os seres humanos são moldados por concepções sociais, históricas, filosóficas e culturais, que moldam seu comportamento e personalidade, lhes atribuindo, mesmo que de forma involuntária, preconceitos e julgamentos. Portanto, estão sujeitas a reproduzir esses preconceitos, havendo um risco que depositem no tratamento de dados eventual discriminação. Contudo, não é possível aferir com convicção que decisões automatizadas estariam imunes desse tipo de adversidade e que seriam mais prudentes que a mente humana.

Apesar disso, uma afirmação é incontestável: a utilização de decisões tomadas por máquinas dotadas de Inteligência Artificial cresceu exponencialmente no decorrer do último século. Isso se explica por diversas razões, dentre elas, a redução de diversos custos operacionais, bem como a otimização de processos que antes eram desnecessariamente duradouros. Diante desse cenário, a humanidade se viu diante de um problema que havia de ser regulado.

Em vista disso, os tribunais nacionais entenderam pela necessidade da adoção de valores constitucionais, de modo a impedir que empresas de tecnologia se valham da facilidade do uso de algoritmos para violarem princípios constitucionais e normas nacionais. Colaciona-se abaixo jurisprudência do Egrégio Tribunal de Justiça do Estado de Minas Gerais (TJMG) nessa orientação:

AGRAVO DE INSTRUMENTO - AÇÃO DE TUTELA ANTECIPADA EM CARÁTER ANTECEDENTE - PERDA DE OBJETO - NÃO OCORRÊNCIA - WHATSAPP E FACEBOOK - GRUPO ECONÔMICO - BANIMENTO - BLOQUEIO DE CONTA EM APLICATIVO - COMUNICAÇÃO PRÉVIA FUNDAMENTADA - NECESSIDADE - DIREITO DO CONSUMIDOR - ALTERNATIVIDADE DA CLÁUSULA RESOLUTIVA DO CDC - DEVER DE INFORMAÇÃO - CONTRADITÓRIO - AMPLA DEFESA - LIBERDADE DE EXPRESSÃO E COMUNICAÇÃO - AMBIENTE VIRTUAL - TROCA DE

²⁹ PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da Inteligência Artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, [s.l.], v. 7, n. 3, p. 239 – 259, 2017. Disponível em: <https://doi.org/10.5102/rbpp.v7i3.4951>. Acesso em: 22 abr. 2023.

³⁰ HARADA, Eduardo. Fail épico: sistema do Google identifica pessoas negras como gorilas, **Tecmundo**, [s.l.], jul. 2015. Disponível em: <https://www.tecmundo.com.br/google-fotos/82458-polemica-sistema-google-fotos-identifica-pessoas-negras-gorilas.htm>. Acesso em 09 jun. 2023.

DADOS - LEI 12.965/2014 - MARCO CIVIL DA INTERNET - EFICÁCIA IMEDIATA E HORIZONTAL DOS DIREITOS HUMANOS - MÁQUINAS - ALGORITMOS - INTELIGÊNCIA ARTIFICIAL - RESPONSABILIDADE DA EMPRESA PELAS DECISÕES E CONSEQUÊNCIAS - TUTELA ANTECIPADA DE URGÊNCIA - REQUISITOS PREENCHIDOS. [...] **Uma vez que o uso de recursos digitais de comunicação e de compartilhamento de dados tornou-se imprescindível no ambiente social, profissional e político, torna-se necessário imprimir coerência às relações jurídicas privadas modernas por meio da adoção de valores constitucionais, em conformidade com a eficácia imediata e horizontal dos direitos humanos, de modo a impedir que empresas de tecnologia, por meio de algoritmos, máquinas e inteligência artificial, violem princípios da Constituição da República e normas nacionais, em especial as dispostas no Marco Civil da Internet e no Código de Defesa do Consumidor**³¹. (Grifou-se).

Nessa perspectiva, popularizou-se a ideia de *privacidade e igualdade por design*³², que ampliou a percepção de que a tecnologia deveria ser usada para estimular a proteção de direitos. Esse conceito surgiu para desmistificar a ideia de que os sistemas automatizados são neutros por natureza e imunes às subjetividades humanas, na medida em que (i.) tais sistemas são desenvolvidos por seres humanos, que podem transferir seus vieses políticos, sociais e culturais; (ii.) as tecnologias são desenvolvidas, sobretudo, para servir a determinados agentes do mercado, dotados de interesses por aumentar seus lucros e negócios; e (iii.) o domínio desses sistemas estão ainda sob o comando de camadas da sociedade mais abastadas³³.

O controle do uso de novas tecnologias deve ser regulado política e juridicamente. No Brasil, entrou em pleno vigor no ano de 2021 a LGPD, que, como supramencionado, regulou o uso de dados pessoais. Com relação ao uso da Inteligência Artificial, que presume o manuseio automatizados de dados digitais, há a formação de medidas normativas, como a Resolução

³¹ BRASIL. Tribunal de Justiça do Estado de Minas Gerais (16ª Câmara Cível). **Agravo de Instrumento nº 10000205976319001/MG**. Agravante: Facebook Serviços Online do Brasil LTDA. Agravado: Drograria E Perfumaria Dornela LTDA. Relator: Marcos Henrique Caldeira Brant. Data de julgamento: 23/06/2021. Disponível em: https://www5.tjmg.jus.br/jurisprudencia/pesquisaNumeroCNJEspelhoAcordao.do?jsessionid=9A36C660515962DF443E4192600B539E.juri_node2?numeroRegistro=1&totalLinhas=1&linhasPorPagina=10&numeroUnico=1.0000.20.597631-9%2F001&pesquisaNumeroCNJ=Pesquisar. Acesso em: 14 maio 2023.

³² Segundo Maria Cristine Branco Lindoso, a privacidade por *design* está interligada com a concepção de que a tecnologia é um instrumento para satisfação de necessidades humanas, de modo que deve ser utilizada para fins de assegurar proteção de direitos. Por outro lado, a igualdade por *design* é referente a uma forma de democratização algorítmica, partindo-se do pressuposto que os vieses incorporados à IA devem ser eliminados, uma vez que prejudicam os grupos minoritários. (LINDOSO, Maria Cristine Branco. Igualdade por design: novas formas de pensar o fim da discriminação por algoritmos e data mining. **Revista de Direito e as Novas Tecnologias**, São Paulo, n. 13, ano IV, 2021, p. 2 - 10. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em: <https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc600000188b08cf59e69c9549c&docguid=I6fd33110533011ecbc698533b2d39e4e&hitguid=I6fd33110533011ecbc698533b2d39e4e&spos=1&epos=1&td=1&context=24&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 23 abr. 2023).

³³ LINDOSO, Maria Cristine Branco. Igualdade por design: novas formas de pensar o fim da discriminação por algoritmos e data mining. **Revista de Direito e as Novas Tecnologias**, São Paulo, n. 13, ano IV, 2021, p. 4. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em: <https://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc600000188b08cf59e69c9549c&docguid=I6fd33110533011ecbc698533b2d39e4e&hitguid=I6fd33110533011ecbc698533b2d39e4e&spos=1&epos=1&td=1&context=24&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 23 abr. 2023.

332/2020 (LGL/2020/11266) do Conselho Nacional de Justiça³⁴, que prevê a ética e transparência na utilização da IA no Poder Judiciário, bem como o Projeto de Lei 21/20, que cria o Marco Legal da Inteligência Artificial³⁵.

Considerando, no entanto, que nenhum desses dispositivos tem plena eficácia legislativa até o presente momento, imperioso reconhecer a LGPD como o início da regulação da IA no Brasil, principalmente quando da análise do art. 20³⁶ do diploma legal, que dispõe acerca do direito do titular dos dados à explicação nas decisões automatizadas. Assim, mostra-se necessária a análise do impacto do uso da Inteligência Artificial no manuseio de dados pessoais para que, enfim, seja possível passar ao exame dos desafios de conciliação entre a LGPD e a IA, bem como a IA como uma solução ao problema do vazamento de dados.

3.1. O IMPACTO DO USO DA INTELIGÊNCIA ARTIFICIAL NA PROTEÇÃO DE DADOS PESSOAIS

Wolfgang Hoffmann-Riem, estudioso alemão dos principais temas relacionados ao fenômeno da digitalização no Direito, em sua obra denominada “Big Data e Inteligência Artificial: Desafios para o Direito”³⁷, realizou uma analogia, através da qual demonstra de forma evidente a importância dos dados pessoais nos dias atuais, ao compará-los com petróleo bruto. Tal analogia faz alusão à importância econômica e as diversas formas de utilização do petróleo e dos dados brutos, bem como as inúmeras possibilidades tecnológicas que resultam da disponibilidade destas matérias-primas.

Diante da atual conjuntura, os mais diversos contextos adaptaram-se aos mecanismos automatizados, desde decisões acerca de concessões de créditos, até apólices de seguros e seleção de currículos. Tais técnicas de IA têm funcionamentos próprios, através dos quais buscam identificar padrões a partir de uma lógica matemática, denominada algoritmos. Por esse motivo, surge um questionamento acerca da diferenciação da IA de um algoritmo convencional. A resposta se encontra justamente na habilidade da IA de acumular experiências próprias e tirar de cada uma delas aprendizados, de forma que o sistema passa a se autoalimentar, tornando-se, praticamente, autodidata. Tal processo é denominado *machine learning*³⁸.

O surgimento de sistemas autônomos na tomada de decisões, sobretudo a Inteligência Artificial, serviu para revolucionar a maneira que os dados são processados atualmente, uma vez que proporcionou uma capacidade de armazenamento de dados impressionante. Esses

³⁴ CONSELHO NACIONAL DE JUSTIÇA. **Resolução Nº 332 de 21/08/2020**: Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Brasília, DF, 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 23 abr. 2023.

³⁵ SOARES, Marcos José Porto. Impacto da evolução tecnológica no reconhecimento de novos direitos: proteção dos dados pessoais e uso adequado da inteligência artificial. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 15, ano 5, abr.-jun. 2022, p. 2. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em: <https://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2022-9795>. Acesso em: 22 abr. 2023.

³⁶ Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

³⁷ HOFFMANN-RIEM, Wolfgang. Big data e Inteligência Artificial: desafios para o direito. Tradução por: Gabriella Bezerra Sales Sarlet e Carlos Alberto Molinaro. **Revista de Estudos Institucionais**, [s.l.], v. 6, n. 2, p. 431 – 506, maio/ago.2020. DOI: 10.21783/rei.v6i2.484. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/484>. Acesso em: 22 abr. 2023.

³⁸ PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da Inteligência Artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, [s.l.], v. 7, n. 3, p. 239 – 259, 2017. Disponível em: <https://doi.org/10.5102/rbpp.v7i3.4951>. Acesso em: 22 abr. 2023.

sistemas de armazenamento gradativamente foram implementados em rotinas diárias dos procedimentos em âmbito empresarial com um certo compromisso e expectativa de garantia agilidade e efetividade para diferentes operações.

Esse movimento, contudo, não veio acompanhado da devida preocupação com relação à quantidade de dados que viria a ser processada nesses sistemas de IA. Imprudentemente, os sujeitos passaram a alimentar esses sistemas com seus dados e, por muitas vezes, através de um *click*, autorizar a divulgação pública dessas informações sem raciocinar as repercussões disso.

Tais informações disponibilizadas pelos titulares dos dados alimentam os mais diversos sistemas, como, por exemplo, bases de armazenamento de currículos, conforme mencionado anteriormente, para processos de seleção. Através da análise desses dados, os sistemas de IA chegam em determinadas decisões, denominadas decisões automatizadas. Cumpre analisar, desse modo, a possibilidade que esses resultados sejam revistos, garantindo ao titular do dado um direito à explicação, uma vez que se mostra como um desafio de conciliação entre a LGPD e a IA.

3.2. OS DESAFIOS DA CONCILIAÇÃO DA LGPD E A INTELIGÊNCIA ARTIFICIAL

Para que seja assegurada uma possível reconsideração das deliberações por parte da IA, é indispensável uma investigação acerca da tomada de decisões por ferramentas inteligentes, de modo que o direito à explicação nas decisões automatizadas, já previsto no art. 20 da LGPD, seja garantido aos titulares dos dados e, ainda, que essas decisões sejam passíveis de correção pelos seres humanos (auditores das máquinas), para que se evitem eventuais discriminações geradas pelo uso da IA³⁹.

O Projeto de Lei nº 4496/2019, de autoria do senador Styvenson Valentim (Podemos/RN), sugere uma análise mais minuciosa acerca do art. 20 da LGPD, sob a justificativa que o comando legal carece de aperfeiçoamentos e, também, para lhe assegurar mais efetividade. Assim, visa a inclusão do conceito de “decisão automatizada” nos seguintes termos:

Art. 5º XX – decisão automatizada: processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou score, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, inteligência artificial, aprendizado de máquina, ou outra técnica computacional.

Essa definição demonstra, de forma clara, a abrangência do conceito de decisão automatizada, bem como o início de sua regulação pela LGPD. Nesse ponto, surge uma discussão quanto ao agente que realizaria a revisão dessa decisão automatizada, na medida em que a Medida Provisória nº 869/2018 afastou a menção expressa “*por pessoa natural*” da letra da lei, restando dúvidas se a decisão automatizada seria novamente analisada por um sistema de IA. Através de uma linha de pensamento, a alteração legislativa teria suprimido a possibilidade da revisão da decisão automatizada por pessoa natural. Entretanto, por outra linha hermenêutica, o afastamento da expressão teria apenas suprimido a obrigatoriedade dessa revisão por pessoa natural, sendo possibilitada a revisão por outra decisão automatizada⁴⁰.

³⁹ CAMARGO, Everson da Silva; CASSOL, Jessica. A inteligência artificial e o processo de seleção: entre a discriminação e o direito à explicação. *In*: FINCATO, Denise Pires; WUNSCH, Guilherme (Coord.). **Redes de tecnologia e relações de trabalho**. Porto Alegre: Lex/ASRDT, 2022, p. 342 – 360.

⁴⁰ LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil – RBDCivil**, [s.l.], v. 26, p. 227 – 246, out./dez. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584>. Acesso em: 22 abr. 2023.

Percebe-se, da análise do artigo, que o direito à explicação é garantido quando a decisão é integralmente automatizada, afeta os interesses dos titulares desses dados ou quando se destina a definir seu perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade. Nesse sentido, verifica-se que a regra do art. 20 da LGPD restringe sua aplicabilidade a decisões tomadas inteiramente por ferramentas inteligentes. Contudo, há de se considerar, dentro dos complexos processos decisórios dos dias atuais, a existência de resultados simultâneos de automação e decisões humanas.

Com o objetivo de conferir efetividade ao direito à explicação, a LGPD previu o direito ao titular de solicitar uma auditoria da Autoridade Nacional de Proteção de Dados (ANPD), na hipótese de o controlador se recusar a fornecer as informações solicitadas pelos titulares dos dados, sob o fundamento de segredo comercial e industrial. Contudo, há de ser considerada a recusa do controlador sob outro fundamento não previsto em lei. Nessa última ocasião, surge um questionamento sobre a possibilidade de a Autoridade intervir, na medida em que, sem essa proteção ao titular, este se veria desamparado pela lei e, por vezes, a situação seria merecedora da intervenção da Autoridade⁴¹.

Nesse contexto, levando em consideração, em primeiro lugar, a incerteza acerca de quem revisaria a decisão automatizada no caso de o titular dos dados exercer seu direito à explicação e, em segundo lugar, no cenário de recusa do controlador em fornecer informações solicitadas pelos titulares dos dados sob alguma justificativa que não se enquadra nas hipóteses do artigo, surgem desafios para a conciliação da LGPD com a IA.

Não obstante a existência de empecilhos quando da aplicação da Inteligência Artificial ao manuseio de dados pessoais, há de ser analisada, da mesma maneira, a utilização das diversas técnicas de IA em prol da sociedade. Surge, nesse sentido, uma hipótese da utilização de algoritmos como uma solução no vazamento de dados pessoais, eis que, em tese, seriam desprovidos de vieses humanos que pudessem acarretar na utilização irregular desses dados e é sobre isso que se passa a discorrer.

4. A INTELIGÊNCIA ARTIFICIAL COMO UMA ALTERNATIVA DE SOLUÇÃO NO VAZAMENTO DE DADOS PESSOAIS

Em maio de 2017 foi anunciada a criação da Associação Brasileira de Inteligência Artificial (ABRIA), que tem como objetivo o fomento à inovação e a aceleração de adoção de técnicas de IA que melhorem a qualidade de vida das pessoas e a produtividade da economia nacional. Em parceria com o Governo Federal, a Associação tem como iniciativas a incorporação da IA e a análise de dados nos processos de formulação de políticas públicas, a promoção do intercâmbio de dados abertos entre entidades da Administração Pública e o setor privado, estímulo aos órgãos públicos que promovam a conscientização do uso da IA, dentre outros.

Esse movimento demonstra a importância dos impactos que a Inteligência Artificial gera na economia nacional, bem como a assimilação pelos órgãos nacionais dessa importância, que se mostra através da previsão, como ações estratégicas, da promoção de intercâmbio livre de dados entre a Administração Pública e o setor privado, nos limites dos direitos à proteção de dados pessoais, bem como o anseio pelo desenvolvimento de parcerias de Projetos de Pesquisa, Desenvolvimento e Inovação (PD&I) voltadas para a IA.

Como explica André Carlos Ponce de Leon Ferreira de Carvalho, a menção do uso da Inteligência Artificial pelas empresas se tornou praticamente um sinônimo de selo de qualidade

⁴¹ LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil – RBDCivil**, [s.l.], v. 26, p. 227 – 246, out./dez. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584>. Acesso em: 22 abr. 2023.

dos produtos oferecidos e a utilização de ferramentas inteligentes passou a servir como garantia que o serviço oferecido por uma empresa é superior aos oferecidos pelas concorrentes. Explica o autor que o protagonismo internacional dos países em IA ficou atrelado com a sua soberania nacional, otimizando a balança comercial dos países e trazendo novos investimentos⁴².

Para fins de exemplificação desse protagonismo, em 2018, o governo francês, através do discurso conduzido pelo presidente Emmanuel Macron, instituiu uma política de dados que alia a IA com o avanço da França e União Europeia, denominado “*AI for humanity*”. O projeto buscou a construção de uma “inteligência artificial confiável” e em prol do interesse geral e do desempenho público⁴³. Este projeto contou com 3 principais objetivos, que estão intrinsecamente relacionados com a promoção de políticas de proteção de dados. São eles: o incentivo do compartilhamento de dados entre empresas/atores do mesmo setor para a criação de um banco de dados comum, com base na reciprocidade, cooperação e compartilhamento; a abertura, de forma progressiva, do acesso a dados por motivos de interesse público; bem como o incentivo ao direito de portabilidade de dados⁴⁴.

Desse modo, percebe-se que a utilização da IA, quando feita de forma ponderada, impulsiona uma economia eficiente e a criação de um mercado global, que permite a realização de operações planejadas com menor esforço e custo. O fator que leva as empresas optarem por automatizarem seus processos decisórios é, sem dúvidas, a velocidade de respostas a diferentes demandas e a redução de custos⁴⁵.

Essa demanda gradativa por celeridade nos processos, no entanto, evidencia a necessidade de que os líderes empresariais encontrem maneiras para equilibrar a relação entre a velocidade das operações com os respectivos riscos⁴⁶. É justamente nesse cenário que se evidencia a importância da implementação de sistemas automatizados de Inteligência Artificial, com o intuito de prevenir, manejar e remediar ataques cibernéticos às bases de dados de empresas de maneira eficaz.

Os sistemas habilitados com a tecnologia da IA têm se mostrado capacitados para a detecção, de modo ágil, de invasões cibernéticas, mediante o envio de alertas de possíveis ataques ou até, como costumeiramente conhecido, através do bloqueio de mensagens não desejadas, também conhecidas como *spams*. Isso acarretou na otimização de processos e minimização do esforço humano para identificação de possíveis ataques cibernéticos. Nesse sentido:

En todos los casos, la inteligencia artificial busca la optimización y detección más eficaz de intrusiones, razón por la cual son variadas las técnicas de IA que se han implementado en sistemas informáticos, lo que ha permitido reducir el esfuerzo

⁴² CARVALHO, André Carlos Ponce de Leon Ferreira de. **Inteligência Artificial: riscos, benefícios e uso responsável**. São Paulo: Universidade de São Paulo, Instituto de Ciências Matemáticas e de Computação, 2021, p. 21. Disponível em: <https://doi.org/10.1590/s0103-4014.2021.35101.003>. Acesso em: 20 maio 2023.

⁴³ RIVELLI, Fabio. O projeto “AI for Humanity” a estratégia francesa. In: MIGALHAS, [s.l.], 2021. Disponível em: <https://www.migalhas.com.br/coluna/ia-em-movimento/376364/o-projeto-ai-for-humanity-a-estrategia-francesa>. Acesso em: 20 maio 2023.

⁴⁴ De acordo com o art. 20 da GDPR, o direito de portabilidade de dados (*Right do data portability*) significa que o dono dos dados terá direito de transmitir seus dados pessoais diretamente de um controlador para o outro, migrando suas informações entre ecossistemas sem perder seu histórico de dados.

⁴⁵ REIS, Nazareno César Moreira; FURTADO, Gabriel Rocha. Decisões automatizadas: definição, benefícios e riscos. **Civilistica.com**, Rio de Janeiro, v. 11, n. 2, 2022, p. 25 - 27. Disponível em: <http://civilistica.com/decisoes-automatizadas/>. Acesso em: 21 maio 2023.

⁴⁶ SÊMOLA, Marcos. Vazamento de informações. In: PINHEIRO, Patricia Peck. **Segurança Digital – Proteção de Dados nas Empresas**. Rio de Janeiro: Grupo GEN, 2020. *E-book*. ISBN 9788597026405. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026405/>. Acesso em: 21 maio 2023. p. 75 – 76.

humano por construir sistemas detectores de intrusos y mejorar el rendimiento de estos⁴⁷.

O escritor Dom Philmlee, estrategista de tecnologia, faz menção à importância da IA em duas fases de um ataque ou possível ataque cibernético. A primeira diz respeito à análise simultânea de quantidade incrível de dados, enquanto o *machine learning* cria uma base de referência, permitindo uma comparação entre os dados, até que enfim se chegue a uma decisão de acionar um alerta ao usuário do sistema acerca de alguma atividade irregular ou, até, bloqueie um hacker de imediato. A segunda, por outro lado, consiste na análise prematura de dados com a finalidade de prevenir ataques cibernéticos. Tal análise se dá através do monitoramento de, por exemplo, chats de conversa da *deep web*⁴⁸.

É mencionada, ainda, a importância da implementação de sistemas automatizados habilitados com a IA, a fim de auxiliar indivíduos a identificarem a integridade de um site ou link antes mesmo de acessá-los. Não obstante, seria eficaz na eliminação da hegemonia das senhas, aprimorando as autenticações biométricas, tanto digitais, quanto fotográficas⁴⁹.

Em último lugar, e em plena consonância com a LGPD, que dispõe expressamente em seu artigo 46⁵⁰ que os agentes de tratamento de dados devem adotar medidas de segurança aptas a proteger os dados pessoais de acessos não autorizados ou eventual tratamento inadequado, a IA se mostra eficiente na criação de políticas de segurança mais eficazes, na medida em que, através do *machine learning*, os sistemas automatizados conseguem vislumbrar padrões e observar minuciosamente o tráfego de rede, de modo que se mostram capazes de sugerir maneiras diversas e mais eficazes de prevenção ao vazamento de dados⁵¹.

O relatório de custo da violação de dados de 2022 realizado pelo IBM Security realizou uma análise entre o custo da violação de dados e a IA e automação na segurança. O estudo concluiu um aumento exponencial de 65% para 70%, entre 2021 e 2022, de empresas que implementaram parcial ou totalmente a IA em sua segurança. Para mais, o relatório apontou que as empresas com IA e automação na segurança tiveram um custo menor, em uma diferença que totaliza o montante de US\$ 3,05 milhões, quando comparadas com uma empresa sem IA e automação na segurança. Essa foi a maior redução de custos no estudo⁵².

Ao fim do estudo restou constatado uma agilidade muito maior das empresas com IA e automação em segurança na detecção de violações aos sistemas. Nesse sentido, enquanto as empresas com sistemas automatizados levaram o período de 181 dias para identificar uma

⁴⁷ Tradução nossa: “Em todos os casos, a inteligência artificial busca otimizar e detectar intrusões de forma mais eficaz, razão pela qual várias técnicas de IA foram implementadas em sistemas de computador, reduzindo o esforço humano para criar sistemas de detecção de intrusões e melhorando seu desempenho”. (TORRES, Alisson B.; RENDÓN, Fredy F.; GUTIÉRREZ, Juan F. Revisión de las técnicas de inteligencia artificial aplicadas en seguridad informática. **Revista Ontare**, [s.l.], v. 8, 2020, p. 99 – 115. Disponível em: <https://doi.org/10.21158/23823399.v7.n0.2019.2612>. Acesso em: 21 maio 2023).

⁴⁸ PHILMLEE, Don. Practice Innovations: Fighting back fast – Artificial Intelligence Comes to Cybersecurity. In: THOMSON REUTERS. [homepage], 2020. Disponível em: <https://www.thomsonreuters.com/en-us/posts/legal/practice-innovations-january-ai-cybersecurity/>. Acesso em 02 jun. 2023.

⁴⁹ PHILMLEE, Don. Practice Innovations: Fighting back fast – Artificial Intelligence Comes to Cybersecurity. In: THOMSON REUTERS. [homepage], 2020. Disponível em: <https://www.thomsonreuters.com/en-us/posts/legal/practice-innovations-january-ai-cybersecurity/>. Acesso em 02 jun. 2023.

⁵⁰ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

⁵¹ PHILMLEE, Don. Practice Innovations: Fighting back fast – Artificial Intelligence Comes to Cybersecurity. In: THOMSON REUTERS. [homepage], 2020. Disponível em: <https://www.thomsonreuters.com/en-us/posts/legal/practice-innovations-january-ai-cybersecurity/>. Acesso em 02 jun. 2023.

⁵² IBM SECURITY. **Relatório de custo da violação de dados em 2022**. São Paulo: ITM Brasil Ltda, 2022, p. 22 – 24.

violação e 68 dias para conter a violação, as empresas sem automatização levaram 232 dias para identificação e 88 dias para contenção.

Cumprе mencionar um exemplo prático de uma empresa que fomenta uma visão da IA como uma ferramenta de resposta proativa a ameaças. Esse é o caso da empresa Microsoft Corporation, que criou uma plataforma SIEM (*Security Information and Event Management*), denominada Microsoft Sentinel, para o gerenciamento de eventos de segurança da nuvem e utiliza a IA para a análise de uma quantidade volumosa de dados de uma empresa de maneira rápida. Essa tecnologia permite a coleta de dados na escala de nuvem, a detecção de ameaças com um índice baixíssimo de falsos positivos, a investigação através da IA por atividades suspeitas e resposta a incidentes de maneira ágil.

Diante do que foi exposto nesse tópico, verifica-se a existência de diversos cenários em que a IA, uma vez utilizada de maneira responsável e consciente, poderá otimizar processos, diante de sua surpreendente desenvoltura, fazendo as operações serem menos custosas e, ainda, fomentando o *compliance* das empresas com as normas da LGPD, através da segurança informática. Cabe ilustrar, na sequência, um caso prático do manuseio dos dados pessoais pela Inteligência Artificial, a fim de exemplificar a maneira pela qual essa interação se concretiza.

4.1. O MANUSEIO DE DADOS PESSOAIS PELA INTELIGÊNCIA ARTIFICIAL

Com o objetivo de ilustrar como se concretiza o manuseio de dados pessoais pela Inteligência Artificial, realiza-se, a partir de agora, um recorte para a área dos seguros, ao tempo que tal tecnologia ofertou diversos novos produtos securitários, bem como trouxe novos modos de exercício dessa atividade securitária, multiplicando os métodos de mensuração de risco.

As tecnologias da IA levaram a um método inovador de mensuração de risco, uma vez que aumentaram exponencialmente os modos de coleta de dados, de modo que o segurador passou a ter acesso a dados concernentes ao segurado e seu estado de risco antes inacessíveis. Diversos sistemas possibilitaram essa facilitação, como as *wearable technologies* (“tecnologias visíveis”)⁵³, bem como os mais diversos aplicativos em smartphones que rastreiam nossas atividades e são capazes de transmitir ao sistema as mais diversas emoções e sentimentos dos segurados. Esse novo modelo de mensuração de risco acarretou em duas consequências: a individualização dos perfis dos segurados e o monitoramento constante do risco⁵⁴.

Destaca-se, nesse contexto, o incremento das *insurtechs*⁵⁵, que possibilitaram a digitalização das etapas de uma relação contratual de seguro, desde a cotação até a formalização do contrato e adimplemento das obrigações contratadas. Os autores Bruno Miragem e Luíza Petersen ilustram essa situação a partir de um exemplo concernente ao monitoramento do

⁵³ As tecnologias visíveis ou *wearable technologies* são definidas como qualquer tipo de serviço eletrônico desenhado para ser usado no corpo do usuário. Cita-se, como exemplo, os relógios inteligentes. (YASAR, Kinza. *Wearable technology*. TECHTARGET, [homepage], 2022. Disponível em: <https://www.techtargеt.com/searchmobilecomputing/definition/wearable-technology#:~:text=Wearable%20technology%20is%20any%20kind,clоthing%20or%20elements%20of%20clothing>. Acesso em: 29 maio 2023).

⁵⁴ MIRAGEM, Bruno; PETERSEN, Luíza. **Direito dos Seguros**. Porto Alegre: Grupo GEN, 2022. *E-book*. ISBN 9786559645435. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559645435/>. Acesso em: 29 maio 2023. p. 279 – 280.

⁵⁵ De acordo com Bruno Diniz, as *insurtechs* atuam em vários pontos da cadeia de seguros, “desde a entrega de soluções tecnológicas, que modernizam a gestão das seguradoras, até aplicações voltadas para facilitar a vida dos consumidores”. Essa tecnologia possibilitou a redução do valor de uma apólice, agilizou os processos nos casos de sinistros e diminuiu as burocracias da comunicação entre segurador e segurado. (DINIZ, Bruno. **O Fenômeno Fintech**. Rio de Janeiro: Editora Alta Books, 2020. *E-book*. ISBN 9788550815459. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788550815459/>. Acesso em: 29 maio 2023. p. 58).

comportamento do segurado através de drones, regulando os sinistros⁵⁶, possibilitando que, em muitas situações, o segurador conheça mais o risco do que o próprio segurado⁵⁷.

Não obstante os diversos benefícios relacionados ao processamento dos dados pessoais do segurador pelo segurado através da Inteligência Artificial, há de ser observada a incidência da LGPD, que preceitua existirem direitos e obrigações entre o segurado e o segurador. Desse modo, se mostra necessário garantir ao segurado que possua conhecimento de quais dados estão sendo obtidos e por quais objetivos estão sendo analisados, a fim de que possa verificar se concedeu ou não o seu consentimento, evitando uma eventual violação à privacidade do indivíduo⁵⁸.

A despeito do recorte feito especificamente para a área de seguros, verifica-se um aumento exponencial da utilização da IA nos mais diversos setores da economia e sociedade. A disseminação de uma nova tecnologia, todavia, traz consigo um importante encargo, qual seja, a responsabilização por eventuais danos causados por ela⁵⁹. Nos próximos tópicos, se passará por uma análise dos possíveis cenários quanto a essa responsabilização. Fala-se em “possíveis” e “hipotéticos”, uma vez que não existe, ainda, regulação da IA no Brasil.

4.2. A CRIAÇÃO DE UMA PERSONALIDADE JURÍDICA ELETRÔNICA (*E-PERSONALITY*) ATRIBUÍDA AOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Diante do aumento exponencial da utilização da IA no manuseio de dados pessoais, cumpre analisar a possível atribuição de personalidade aos entes dotados de inteligência artificial, na medida em que essa releitura “acompanha a tendência de funcionalização dos institutos jurídico”⁶⁰. O estudo acerca da atribuição de personalidade aos sistemas de IA não

⁵⁶ MIRAGEM, Bruno; PETERSEN, Luíza. **Direito dos Seguros**. Porto Alegre: Grupo GEN, 2022. *E-book*. ISBN 9786559645435. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559645435/>. Acesso em: 29 maio 2023. p. 281.

⁵⁷ SILVA, Anthony Charles de Novaes da; OLIVO, Carlos Augusto Acosta. O futuro é hoje: o impacto da tecnologia nos seguros. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 15, ano 5, abr.-jun, 2022, p. 6. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em: <https://revistadotribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000188a1654ff5f07683e0&docguid=I689d3f70e3be11ec8b36b35cb5d3a37f&hitguid=I689d3f70e3be11ec8b36b35cb5d3a37f&spos=3&epos=3&td=3&context=105&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 29 maio 2023.

⁵⁸ SILVA, Anthony Charles de Novaes da; OLIVO, Carlos Augusto Acosta. O futuro é hoje: o impacto da tecnologia nos seguros. **Revista de Direito e as Novas Tecnologias**. vol. 15. ano 5. São Paulo: Ed. RT, abr.-jun. 2022, p. 6. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em: <https://revistadotribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad6adc60000188a1654ff5f07683e0&docguid=I689d3f70e3be11ec8b36b35cb5d3a37f&hitguid=I689d3f70e3be11ec8b36b35cb5d3a37f&spos=3&epos=3&td=3&context=105&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 29 maio 2023.

⁵⁹ De acordo com Caroline Vaz, o desenvolvimento industrial e o aumento do uso das máquinas impulsionaram o surgimento de novas teorias e uma tendência à proteção das vítimas. Não obstante, trouxe obstáculos na identificação da culpa pelo dano e causador do dano. Percebe-se que, nos dias atuais, mais do que nunca, o debate acerca responsabilização de diferentes agentes no âmbito das tecnologias ganhou relevância. (VAZ, Caroline. Revisitando a Responsabilidade Civil: aspectos relevantes da antiguidade à contemporaneidade pandêmica. **Revista do Ministério Público do RS**, Porto Alegre, n. 87, jan. 2020 – jun. 2020, p. 128 - 129. Disponível em: <https://www.revistadomprs.org.br/index.php/amprs/article/view/190/80>. Acesso em: 29 maio 2023).

⁶⁰ PEREIRA, João Sérgio dos Santos Soares. E-personality aos robôs dotados de inteligência artificial: uma terceira via de personalidade? Utopia ou Realidade? – A necessidade de discutir a interação entre seres humanos e robôs. **Revista de Direito e as Novas Tecnologias**, São Paulo, v.7, 2020, p. 5. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em:

almeja a resolução do tema, mas sim uma análise acerca dessa necessidade verificada na sociedade de proteger os indivíduos de eventuais danos causados por ferramentas inteligentes, evitando a impunibilidade dos agentes envolvidos no manuseio de dados pessoais.

O legislador do Código Civil de 2022 determinou, no artigo 52, que: “Aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade”. O mencionado diploma legal permitiu a proteção da personalidade às pessoas jurídicas, não podendo, no entanto, ser tal proteção confundida com a concessão às pessoas jurídicas de valores inerentes à pessoa. Nesse sentido:

Acerca do conteúdo do referido Artigo, agiu bem o legislador ao não conferir às pessoas jurídicas direitos informados por valores inerentes à pessoa, mas sim ao **permitir a aplicação, por empréstimo, da técnica de proteção da personalidade às pessoas jurídicas**, uma vez que estas não têm todos os elementos justificadores da proteção à personalidade, apreciáveis em situações existenciais. Soma-se a isso o conteúdo da Súmula 227 do STJ: “As pessoas jurídicas podem sofrer danos morais”⁶¹. (Grifou-se).

Nesse mesmo sentido é a passagem exposta por Anderson Schreiber, no que se refere à concepção da personalidade sob dois aspectos distintos, o subjetivo e o objetivo. O primeiro deles relaciona-se com a capacidade que todas as pessoas (físicas e jurídicas) têm de serem titulares de direitos e obrigações. Já o segundo aspecto relaciona-se ao conjunto de características e atributos da pessoa humana⁶². Inegável, desse modo, a inexistência de impedimentos para a concepção de personalidade ao ente robô.

No ano de 2017, o Parlamento Europeu editou uma Resolução que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL))⁶³. Dentre todo o conteúdo exposto na Resolução, insta salientar o disposto no item 59, alínea f⁶⁴, que propõe como uma das soluções jurídicas possíveis do impacto da utilização da IA no manuseio de dados pessoais a criação de um estatuto jurídico para os robôs a longo prazo, aplicando, eventualmente, a personalidade eletrônica aos casos em que os robôs tomem decisões autônomas ou interajam com terceiros independentemente de intervenção humana.

Já em outubro do ano de 2020, o Parlamento Europeu aprovou, por meio de três relatórios, iniciativas para regulamentar o uso da IA. O primeiro relatório, elaborado por Ibán Garcia de Blanco, diz respeito à criação de um código de ética da IA. O segundo, de relatoria de Axel Voss, abordou a temática da responsabilidade civil por danos causados pela IA. O

<https://revistadoatribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b00000188975bca442ffe9bbd&docguid=Ic014af30a48811ea9c19bc57168f93fc&hitguid=Ic014af30a48811ea9c19bc57168f93fc&spos=2&epos=2&td=4&context=181&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 26 maio 2023.

⁶¹ LUTZKY, Daniela Courtes. **A reparação de danos imateriais como direito fundamental**. Porto Alegre: Livraria do Advogado Editora Ltda, 2012, p. 73 – 74.

⁶² SCHREIBER, Anderson. **Direitos da personalidade**. 2. ed. São Paulo: Editora Atlas S/A, 2013, p. 6.

⁶³ UNIÃO EUROPEIA. Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)). **Jornal Oficial da União Europeia**, [s.l.], 2017. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52017IP0051>. Acesso em: 28 maio 2023.

⁶⁴ Item 59: Insta a Comissão a explorar, analisar e ponderar, na avaliação de impacto que fizer do seu futuro instrumento legislativo, as implicações de todas as soluções jurídicas possíveis, tais como:

f) Criar um estatuto jurídico específico para os robôs a longo prazo, de modo a que, pelo menos, os robôs autônomos mais sofisticados possam ser determinados como detentores do estatuto de pessoas eletrônicas responsáveis por sanar quaisquer danos que possam causar e, eventualmente, aplicar a personalidade eletrônica a casos em que os robôs tomam decisões autônomas ou em que interagem por qualquer outro modo com terceiros de forma independente.

último relatório, redigido por Stéphane Séjourné, discorreu acerca dos direitos de propriedade intelectual⁶⁵.

O enfoque aqui recai sobre o segundo relatório. Conforme dispõe o Autor Filipe Medon⁶⁶, ao sintetizar as ideias expostas pelo deputado Axel Voss, a tendência geral sinaliza para o fato de que os sistemas de inteligência artificial deverão ser desenvolvidos sob a supervisão humana. Nessa lógica:

[...] o relatório de autoria do deputado Axel Voss conclui que (i) não é necessária uma revisão completa das normas de responsabilidade civil existentes, mas deve ser levado em consideração que a complexidade, opacidade, capacidade de modificação e autoaprendizado da IA, associadas à participação de inúmeros atores na sua programação, representam um grande desafio à efetividade das normas; (ii) que como quase sempre os danos causados pela IA são, em alguma medida, resultado da participação e do envolvimento de um ser humano, não seria necessário garantir personalidade jurídica própria aos sistemas comandados por Inteligência Artificial, sendo por isso, recomendado não lhes atribuir tal condição.

Nesse mesmo artigo é pontuada uma ressalva importante com relação à retirada do trecho legal que previa a revisão das decisões automatizadas por uma pessoa humana do artigo 20 da LGPG, uma vez que há uma tendência mundial em assegurar a utilização da Inteligência Artificial intrinsecamente pautada na presença humana. Contudo, verifica-se que o § 1º do mencionado artigo⁶⁷, que determina que o controlador dos dados deverá fornecer informações claras a respeito dos procedimentos adotados para a decisão automatizada, mostra-se como um possível garantia da intervenção humana.

Decorre do exposto acima que, considerando não haver impedimentos legais nas legislações nacionais quanto ao reconhecimento da personalidade aos sistemas de IA, desde que a lei assim defina, a necessidade de análise do tema é inquestionável, não só pela questão da responsabilidade civil e eventual ressarcimento dos prejudicados, mas sim com relação aos direitos intelectuais eventualmente atribuíveis aos sistemas de IA. Quanto ao tema da responsabilidade civil decorrente da utilização de robôs inteligentes, surge como uma solução tangível um seguro obrigatório para eventuais danos causados por robôs dotados de IA.

4.3. A CONVENIÊNCIA DA CRIAÇÃO DE UM SEGURO DE RESPONSABILIDADE CIVIL RELACIONADO À INTELIGÊNCIA ARTIFICIAL

O advento da Inteligência Artificial trouxe impactos de extrema relevância no tocante à matéria de seguros. Isso se demonstra tanto pela criação de novos produtos securitários,

⁶⁵ UNIÃO EUROPEIA. Parlamento Europeu. **Parlamento na vanguarda das normas europeias sobre inteligência artificial**. [S.l.], 2020. Disponível em: <https://www.europarl.europa.eu/news/pt/press-room/20201016IPR89544/parlamento-na-vanguarda-das-normas-europeias-sobre-inteligencia-artificial>. Acesso em: 27 maio 2023.

⁶⁶ MEDON, Filipe. Tendências para a responsabilidade civil da Inteligência Artificial na Europa: a participação humana ressaltada. *In*: MIGALHAS, [s.l.], 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/335801/tendencias-para-a-responsabilidade-civil-da-inteligencia-artificial-na-europa--a-participacao-humana-ressaltada>. Acesso em: 27 maio 2023.

⁶⁷ Art. 46, § 1º: A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

conforme já discorrido no tópico do manuseio dos dados pessoais pela IA⁶⁸, quanto pelo aumento de situações de risco a serem cobertas pelos seguros. É sobre a segunda hipótese que se passará a discorrer no presente ponto.

Conforme aduzido anteriormente, a discussão acerca da responsabilidade civil dos operadores de máquinas dotadas de Inteligência Artificial ganhou maior atenção pela entrada da denominada 4ª Revolução Industrial, que alterou substancialmente a vida em sociedade, criando um maior número de riscos quanto ao vazamento de dados pessoais e a possível violação do patrimônio do segurado.

A Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, destaca que uma possível solução para a complexidade dos danos causados pelo vazamento de dados é a criação de um regime de seguros obrigatórios, sendo que poderia ser baseado na obrigação do produtor de contratar um seguro para os robôs autônomos que produz. Menciona, para além, que esse regime poderia ser complementado por um fundo de reparação de danos.

Ao ilustrarem o tema, Bruno Miragem e Luíza Petersen utilizam como exemplo prático o caso dos veículos autônomos, que se movimentam sem a intervenção humana. Partindo-se da hipótese de um acidente ocasionado com a mencionada categoria de veículos, surge a discussão acerca da responsabilização pelos danos causados (apresentam-se como os possíveis agentes a serem responsabilizados o proprietário do veículo, o fabricante do veículo, o fornecedor da tecnologia da IA ou todos de maneira solidária)⁶⁹.

Como uma tendência que poderá servir como inspiração para a criação de um seguro para danos causados pelos sistemas dotados de IA, destaca-se uma modalidade de seguro já existente, o seguro de risco cibernético. A autora Patrícia Peck Pinheiro assevera que existe uma maior complexidade quanto a essa categoria de seguro, o que é explicado por dois motivos.

O primeiro diz respeito à necessidade de muitas coberturas de seguro atuais demandarem a existência de uma ação judicial para serem acionadas, sendo que se mostra improvável que empresas de tecnologia ou empresas que utilizam a tecnologia para a execução de suas atividades desejem esse tipo de exposição para acionar o seguro. Ainda, se mostra complexa a atividade de quantificar o valor do prêmio e das coberturas, uma vez que tal atividade demanda o exame das vulnerabilidades de um sistema eletrônico e o mercado não detém, ainda, amplo conhecimento sobre esses riscos cibernéticos⁷⁰.

Para demonstrar o acima mencionado seguro cibernético, cita-se como exemplo a seguradora Allianz, que oferta o produto denominado “Allianz Riscos Cibernéticos”, o qual consiste em um seguro para empresas, que visa proteger o patrimônio do segurado e indenizar terceiros pelas perdas e despesas financeiras decorrentes de danos causados por ataques cibernéticos. Essa cobertura abarca a violação de privacidade e confidencialidade, segurança de rede, responsabilidade de mídia, custos regulatórios e coberturas de multas, custos de gerenciamento de crise e extorsão cibernética. Prevê, ainda, certas coberturas adicionais, como lucros cessantes por interrupção de negócios, custos de defesa emergencial, entre outros.

⁶⁸ Conforme doutrina Bruno Miragem e Luíza Petersen, a Inteligência Artificial auxiliou na inovação das técnicas de gerenciamento de risco e dos novos modelos de garantia. Nesse sentido: “A Inteligência Artificial incrementa as técnicas de gerenciamento do risco à disposição do segurador. Primeiro, porque multiplica os métodos de previsão e mensuração do risco, para além do modelo estatístico tradicional; segundo, porque fornece inúmeras técnicas de prevenção e controle do risco, de forma eficiente e a baixo custo”. (MIRAGEM, Bruno; PETERSEN, Luíza. **Direito dos Seguros**. Porto Alegre: Grupo GEN, 2022. *E-book*. ISBN 9786559645435. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559645435/>. Acesso em: 27 maio 2023. p. 278).

⁶⁹ MIRAGEM, Bruno; PETERSEN, Luíza. **Direito dos Seguros**. Porto Alegre: Grupo GEN, 2022. *E-book*. ISBN 9786559645435. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559645435/>. Acesso em: 27 maio 2023. p. 285.

⁷⁰ PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2021. *E-book*. ISBN 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 08 jun. 2023. p. 175 – 177.

Criando-se uma correlação com o tópico anterior, referente à atribuição de personalidade aos sistemas dotados de IA, o autor Carlos Affonso Souza cria um debate bastante relevante sobre a capacidade de se assegurar uma justa e efetiva reparação de danos causados pela IA. Assevera o escritor que a criação de uma personalidade para os robôs inteligentes não lhe parece a melhor saída, uma vez que surgiria o embate quanto à gerência do patrimônio do robô, afirmando que se mostra mais eficiente a criação de um novo tipo de cobertura securitária do que a de uma nova categoria de pessoas jurídicas⁷¹.

João Sérgio dos Santos Soares, por sua vez, realiza uma ponderação acerca dos dispositivos legais previstos em nossa legislação nacional aptos a auxiliar o debate no tocante à responsabilidade civil dos robôs inteligentes. O escritor faz menção ao art. 927, parágrafo único, e art. 931, ambos do Código Civil que, uma vez cumulados, denota que os empresários individuais e empresas terão a obrigação de reparar, independentemente de culpa (tratando-se, portanto, de responsabilidade objetiva), os danos causados pelos produtos postos em circulação. Ao fim de seu artigo, assevera o autor que não obstante a criação de um seguro para os danos causados pela IA seja uma solução eficiente, a discussão acerca da atribuição da personalidade aos sistemas contempla, ainda, eventuais direitos que se efetivem (direitos de imagem, direitos do autor, propriedade intelectual e *et cetera*)⁷².

Percebe-se, diante disso, uma tendência de que os riscos cibernéticos gradativamente se tornem mais frequentes. Nesse sentido, o relatório realizado no ano de 2023 pela seguradora Allianz deu conta de que tais riscos, pelo segundo ano seguido, são considerados como os mais importantes atualmente, sendo que foi elencado pelo *Allianz Risk Barometer* (Barômetro de Risco da Allianz) por mais de um terço de todos os entrevistados como a principal preocupação dos entrevistados neste ano. Dentre os riscos cibernéticos citados, como o aumento dos ataques de *ransomware*, a interrupção decorrente de falhas nas cadeias de plataformas de serviços de tecnologia e o aumento dos ataques de *malware*, o vazamento de dados foi considerado, por 53% dos entrevistados, como o mais preocupante⁷³.

Em face do apresentado acima, imprescindível é a análise dos possíveis agentes a serem responsabilizados por eventuais danos causados a IA. Para além disso e com o objetivo de prevenir o vazamento desses dados e resguardar os direitos dos usuários, o exame da ética-jurídica da aplicação da IA no manuseio de dados pessoais se mostra pertinente.

5. OS LIMITES ÉTICOS DA APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO MANUSEIO DE DADOS PESSOAIS

Diante de um contexto global de crescentes discussões sobre a governança da IA, foi lançado um projeto de lei para um marco legal da Inteligência Artificial (PL 2.338/2023). O

⁷¹ SOUZA, Carlos Affonso. O debate sobre personalidade jurídica para robôs. In: JOTA, [s.l.], 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-debate-sobre-personalidade-juridica-para-robos-10102017>. Acesso em: 27 maio 2023.

⁷² PEREIRA, João Sérgio dos Santos Soares. E-personality aos robôs dotados de inteligência artificial: uma terceira via de personalidade? Utopia ou Realidade? – A necessidade de discutir a interação entre seres humanos e robôs. *Revista de Direito e as Novas Tecnologias*, São Paulo, v. 7, 2020, p. 8 - 9. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em: <https://revistadotribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b00000188975bca442ffe9bbd&docguid=Ic014af30a48811ea9c19bc57168f93fc&hitguid=Ic014af30a48811ea9c19bc57168f93fc&spos=2&epos=2&td=4&context=181&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 26 maio 2023.

⁷³ ALLIANZ. *Allianz Risk Barometer: Identifying the major business risks for 2023*. [S.l.]: Allianz Global Corporate & Specialty, 2023. Disponível em: <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf>. Acesso em: 08 jun. 2023.

mencionado projeto determina, já em seus artigos iniciais, as diretrizes a serem respeitadas pela inteligência artificial, preceituando que deverá observar a boa-fé e, dentre outros princípios elencados no art. 3º, a confiabilidade e robustez dos sistemas de IA e segurança da informação.

Nesse cenário, ganha destaque a matéria da ética de dados (*Data ethics*). Esse estudo pode ser definido como o ramo da ética que estuda e avalia problemas morais relacionados a dados e algoritmos, com a finalidade de formular e apoiar soluções moralmente corretas⁷⁴. A ética dos dados estuda o modelo de estruturação dos algoritmos de modo a proteger os indivíduos do mal uso da IA.

Em 1942, o escritor e bioquímico Isaac Asimov apresentou uma proposta de investigação com as três leis da robótica: A primeira refere que um robô não pode ferir um ser humano ou permitir que seja prejudicado; a segunda estabelece que os robôs deverão obedecer as regras estipuladas por seres humanos, salvo se as primeiras ordens conflitarem com a primeira lei; a terceira, por sua vez, determina que um robô deve proteger sua própria existência, caso essa proteção não entre em conflito com a primeira e segunda lei⁷⁵.

Percebe-se, portanto, que o ramo de estudo ético-jurídico da aplicação da IA no manuseio de dados vislumbra a IA como um objeto a ser conduzido pela racionalidade humana e em prol da vontade humana. Disso decorre que a ética da IA encontra respaldo no manuseio consciente dos dados pessoais.

À vista disso, no ano de 2021, a Organização das Nações Unidas para a Educação, Ciência e a Cultura (UNESCO) criou a Recomendação sobre a Ética da Inteligência Artificial⁷⁶, que determinou, em seu item 34, que os sistemas algorítmicos exigem uma avaliação adequada de impacto na privacidade, que inclui a consideração social e ética de sua utilização. A Recomendação dispôs, ainda, um tópico detalhado acerca da política de dados, que estipulou o desenvolvimento de estratégias de governança de dados que garantam adequação dos processos de coleta e armazenamento desses dados como uma obrigação aos Estados-membros.

Nesse cenário, destaca-se a matéria de *compliance* digital, o “atuar em conformidade”⁷⁷. A LGPD cuidou da matéria entre os artigos 50 e 51⁷⁸, transformando a governança de dados como uma faculdade do agente. Em seguida, o Decreto-Lei nº 10.046, de 07 de outubro de 2019⁷⁹, previu, em seu artigo 3º, as diretrizes das operações de tratamento de dados pelo Poder

⁷⁴ FLORIDI, Luciano; TADDEO, Mariarosaria. Introduction: What is data ethics? **Philosophical Transactions: Mathematical, Physical and Engineering Sciences**, [s.l.], v. 374, nº 2083, p. 1 – 5, 2016. Disponível em: <https://www.jstor.org/stable/26115816>. Acesso em: 27 maio 2023.

⁷⁵ ASIMOV, Isaac. **Eu, Robô**. Tradução por Luiz Horácio da Matta, 9. ed. Rio de Janeiro: Editora Expressão e Cultura, 1975, p. 7.

⁷⁶ ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. **Recomendação sobre a Ética da Inteligência Artificial**. [S.l.]: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_por. Acesso em: 29 maio 2023.

⁷⁷ MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Compliance digital e responsabilidade civil na Lei Geral de Proteção de dados. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson. **Responsabilidade civil e novas tecnologias**. São Paulo: Editora Foco, 2020, pp. 482 – 530.

⁷⁸ Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

⁷⁹ BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm#:~:text=DECRETO%20N%2010.046%2C%20DE%209%20DE%20OUTUB

Público. Nesse seguimento, insta observar o regulamento de aplicação de sanções administrativas publicada pela Agência Nacional de Proteção de Dados na data de 27 de fevereiro de 2023, que se tornou uma ferramenta importante para reconduzir o agente de tratamento de dados pessoais à conformidade com a LGPD.

Patrícia Peck Pinheiro sustenta que o investimento em tecnologia e pessoas não é suficiente, sendo que as empresas devem passar por um planejamento estratégico que integre as áreas de organização e fomenta a mudança de comportamento com relação ao tema de segurança dos dados, governança e *compliance*⁸⁰. Explica a autora que o gerenciamento de riscos deve passar por etapas bastante delimitadas, que visem a prevenção de crimes cibernéticos, são elas:

[...] a) adequação à legislação vigente aplicável em toda a cadeia do negócio; b) revisão de contratos com fornecedores, parceiros, colaboradores e clientes; c) elaboração de novas minutas de contratos que tratem adequadamente das responsabilidades das partes quanto aos riscos digitais envolvidos, incluindo aplicação de cláusulas ou acordos de nível de serviço (SLA) e Plano de Continuidade (PCN); d) implantação de políticas de segurança para o uso das ferramentas tecnológicas no trabalho; e) conscientização para construção de cultura interna na empresa de segurança da informação e proteção dos ativos intangíveis⁸¹.

Nicholas Kluge Corrêa, Nythamar Fernandes de Oliveira e Diogo Fernando Massmann por sua vez, asseveram que, não obstante a importância do estabelecimento de diretrizes éticas, existem questionamentos acerca da sua eficiência de governança, advertindo, ao fim, a indispensabilidade da regulação legal do tema, argumentando que “as justificativas para os projetos de lei em nosso País seriam várias, oscilando desde a preocupação emergente quanto à convivência humana com entes autônomos e inteligentes até questões de segurança jurídica [...]”⁸².

Diante do que foi discorrido nesse tópico, conclui-se que a despeito da previsão de inúmeras diretrizes éticas, bem como a importância conferida à estipulação de sanções aos agentes que não atuarem em conformidade com a proteção de dados, a matéria relacionada à IA ainda guarda determinadas nuances, cujas resoluções poderiam se valer da criação de uma regulamentação específica da IA, tendo como símbolo inicial o Marco legal para a Inteligência Artificial, apresentado ao Senado Federal pelo presidente da Casa, Rodrigo Pacheco, no dia 03 de maio de 2023.

Tal necessidade se verifica, principalmente, pelo reconhecimento da proteção de dados pessoais como direito fundamental pela Constituição Federal de 1988⁸³, fato que, de acordo

RO%20DE%202019&text=Dispõe%20sobre%20a%20governança%20no,Central%20de%20Governança%20de%20Dados. Acesso em: 08 jun. 2023.

⁸⁰ PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2021. *E-book*. ISBN 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 08 jun. 2023. p. 175 – 177.

⁸¹ PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2021. *E-book*. ISBN 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 08 jun. 2023. p. 176.

⁸² CORRÊA, Nicholas Kluge; OLIVEIRA, Nythamar Fernandes de; MASSMANN, Diogo Fernando. **Sobre a eficiência da ética como ferramenta de governança da inteligência artificial**. Porto Alegre: Veritas, 2022, p. 7 - 10. Disponível em: <https://revistaseletronicas.pucrs.br/ojs/index.php/veritas/issue/view/1523>. Acesso em: 28 maio 2023.

⁸³ Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022).

com Eduardo Carlos Bianca Bittar, Gabrielle Bezerra Sales Sarlet e Ingo Wolfgang Sarlet⁸⁴, demandou uma governança algorítmica transparente, que envolva uma permanente análise dos impactos e dos riscos oriundos do manejo da IA.

6. CONSIDERAÇÕES FINAIS

O presente artigo buscou expor uma análise da aplicação da Inteligência Artificial no manuseio de dados pessoais. Para tanto, mostrou-se imprescindível o exame dos momentos históricos de maior importância no âmbito do tema da proteção de dados, oportunidade em que foi apresentada a evolução da noção de tutela da privacidade que, diante dos avanços tecnológicos, atraiu interesses alheios sob as informações pessoais dos indivíduos, acarretando na necessidade de uma regulação específica sobre o tema.

Conforme mencionado, diversas legislações nacionais dispuseram, anteriormente à promulgação da LGPD, conceitos que viriam a ser previstos na legislação nacional sobre dados. Esse é o caso, por exemplo, da mencionada Lei do Cadastro Positivo que previu a definição de informações sensíveis, atribuindo um enfoque e atenção maior para determinados dados, bem como do Marco Civil da Internet que representou, sem dúvidas, um avanço no que tange à regulação das relações em ambientes digitais. Contudo, a edição do Regulamento Geral de Proteção de Dados da União Europeia se mostrou como uma ocasião oportuna para que o legislador brasileiro progredisse com a redação da LGPD, promulgada no ano de 2018.

Nesse sentido, foram expostas as categorias de dados pessoais abarcados pela LGPD, quais sejam: os dados pessoais, os dados sensíveis e os dados anonimizados. Aqui, foi realizada importante diferenciação entre pessoa singular identificada e identificável, aumentando a gama de sujeitos cujos dados são protegidos pelo diploma legal. Tal exposição se mostrou relevante para a delimitação do enfoque do artigo, especificando exatamente o que se intenta referir quando da menção de “dados pessoais”.

Adentrando de maneira mais delimitada no tema do trabalho, foi realizada uma reflexão, no sentido de que se mostra imprescindível a análise da congruência entre os atuais ditames da IA com a LGPD. Tal discussão trouxe à tona os desafios de conciliação entre as ferramentas inteligentes e o manuseio de dados pessoais, que se demonstra principalmente pelas decisões tomadas pela IA, na medida em que não se consideram duas hipóteses: a incerteza acerca do sujeito que revisará uma decisão automatizada, no caso de o titular dos dados exigir seu direito à explicação, ou a recusa do controlador em fornecer informações solicitadas pelos titulares dos dados sob alguma justificativa que não se enquadra nas hipóteses do artigo.

Em seguida, direcionou-se o artigo para uma investigação quanto à aplicabilidade da IA como uma solução no vazamento de dados pessoais. Não obstante a existência de uma lacuna na doutrina e jurisprudência pátria sobre o tema, foi efetuado um exame em artigos periódicos estrangeiros referente à segurança cibernética. Constatou-se a existência de uma linha de estudos que congrega a IA com o instituto da cibersegurança. Depreende-se desses estudos que os sistemas automatizados se mostram plenamente capazes de sugerir e criar maneiras cada vez mais eficazes de prevenção ao vazamento de dados.

Com o objetivo de ilustrar de forma prática como se dá a interação da IA com o manuseio de dados pessoais foi realizado um recorte para a área dos seguros, oportunidade em que foi observado que as ferramentas inteligentes ganharam um espaço bastante relevante na etapa da mensuração dos riscos, na medida em que ampliaram os métodos de armazenamento e monitoramento dos dados pessoais dos segurados. A discussão acerca da efetividade de tais

⁸⁴ SARLET, Ingo Wolfgang.; SARLET, Gabrielle Bezerra Sales; BITTAR, Eduardo Carlos Bianca. **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital**. São Paulo: Editora Saraiva, 2022. *E-book*. ISBN 9786555599527. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555599527/>. Acesso em: 29 maio 2023. p. 13.

operações, na proporção dos riscos que representam, trouxe à tona o debate quanto à responsabilização por eventuais danos causados pelos sistemas dotados de IA.

Nesse cenário, foi apresentada a atribuição de uma personalidade para a IA a casos em que robôs tomem decisões autônomas ou interajam independentemente de intervenção humana como uma possível solução à controvérsia relacionada à responsabilização de um robô.

Foram colacionadas, no presente trabalho, duas visões. A primeira diz respeito à concepção de que a criação de um estatuto jurídico para robôs garantiria, sobretudo, os direitos intelectuais por eventuais criações dessas ferramentas inteligentes. A segunda dá conta que a criação de uma personalidade eletrônica não se mostra viável, na medida em que surgiriam dúvidas acerca de quem realizaria a gestão deste patrimônio, mostrando-se mais viável a criação de um seguro de responsabilidade civil.

Assim, passou-se à análise da conveniência da criação de um seguro de responsabilidade civil para danos causados pela IA. Foi apresentada, como uma alternativa, a obrigação do produtor de contratar um seguro para os robôs autônomos que produz, conforme disposto na Resolução do Parlamento Europeu, de 16 de fevereiro de 2017.

Ao fim do artigo foram analisados os limites éticos da aplicação da IA no manuseio de dados pessoais, que ganharam maior importância através da previsão pela Agência Nacional de Proteção de Dados de sanções administrativas para agentes que não atuem em conformidade com a LGPD. Foi mencionada, ainda, a existência de um campo de estudos, qual seja o da Ética de Dados, que vem ganhando maior atenção, na medida em que entende que as ferramentas inteligentes têm de ser adaptadas em prol da sociedade e devem passar pela averiguação humana.

Diante de todo o exposto, verifica-se que o presente trabalho não teve como objetivo exaurir o tema, mas tão somente auxiliar e incentivar o debate quanto aos desafios e benefícios da Inteligência Artificial na matéria de proteção de dados. Depreende-se, da leitura do artigo, que um recurso viável para a solução das controvérsias apresentadas é a tramitação do Projeto de Lei nº 21/2020 (Marco legal do desenvolvimento e uso da Inteligência Artificial), que estabelece princípios, fundamentos e diretrizes para um funcionamento efetivo e ético da inteligência artificial no Brasil.

REFERÊNCIAS

ALLIANZ. **Allianz Risk Barometer: Identifying the major business risks for 2023.** [S.l.]: Allianz Global Corporate & Specialty, 2023. Disponível em: <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf>. Acesso em 08 jun. 2023.

ASIMOV, Isaac. **Eu, Robô.** Tradução por Luiz Horácio da Matta, 9. ed. Rio de Janeiro: Editora Expressão e Cultura, 1975.

BRASIL. Casa Civil. **90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa.** Brasília: Casa Civil, 2022. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa>. Acesso em: 15 abr. 2023.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019.** Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm#:~:text=DECRETO%20N%2010.046%2C%20DE%209%2

ODE%20OUTUBRO%20DE%202019&text=Dispõe%20sobre%20a%20governança%20no,C
entral%20de%20Governança%20de%20Dados. Acesso em: 08 jun. 2023.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplimento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm. Acesso em: 15 abr. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 15 abr. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 15 abr. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Brasília, DF. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 02 abr. 2023.

BRASIL. Supremo Tribunal de Justiça (2ª Turma). **Agravo em Recurso Especial nº 2130619 SP 2022/0152262-2.** Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravada: Maria Edite de Souza. Relator: Ministro Francisco Falcão. Brasília. Data do julgamento: 07 de março de 2023. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp>. Acesso em: 14 maio 2023.

BRASIL. Tribunal de Justiça do Estado de Minas Gerais (16ª Câmara Cível). **Agravo de Instrumento nº 10000205976319001/MG.** Agravante: Facebook Servicos Online do Brasil LTDA. Agravado: Drogeria E Perfumaria Dornela LTDA. Relator: Marcos Henrique Caldeira Brant. Data de julgamento: 23/06/2021. Disponível em: https://www5.tjmg.jus.br/jurisprudencia/pesquisaNumeroCNJEspelhoAcordao.do;jsessionId=9A36C660515962DF443E4192600B539E.juri_node2?numeroRegistro=1&totalLinhas=1&linhasPorPagina=10&numeroUnico=1.0000.20.597631-9%2F001&pesquisaNumeroCNJ=Pesquisar. Acesso em: 14 maio 2023.

CAMARGO, Everson da Silva; CASSOL, Jessica. A inteligência artificial e o processo de seleção: entre a discriminação e o direito à explicação. *In*: FINCATO, Denise Pires; WUNSCH, Guilherme (Coord.). **Redes de tecnologia e relações de trabalho.** Porto Alegre: Lex/ASRDT, 2022.

CARVALHO, André Carlos Ponce de Leon Ferreira de. **Inteligência Artificial: riscos, benefícios e uso responsável.** São Paulo: Universidade de São Paulo, Instituto de Ciências Matemáticas e de Computação, 2021. Disponível em: <https://doi.org/10.1590/s0103-4014.2021.35101.003>. Acesso em: 20 maio 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução N° 332 de 21/08/2020**: Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Brasília, DF, 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em 23 abr. 2023.

CORRÊA, Nicholas Kluge; OLIVEIRA, Nythamar Fernandes de; MASSMANN, Diogo Fernando. **Sobre a eficiência da ética como ferramenta de governança da inteligência artificial**. Porto Alegre: Veritas, 2022. Disponível em: <https://revistaseletronicas.pucrs.br/ojs/index.php/veritas/issue/view/1523>. Acesso em: 28 maio 2023.

DINIZ, Bruno. **O Fenômeno Fintech**. Rio de Janeiro: Editora Alta Books, 2020. *E-book*. ISBN 9788550815459. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788550815459/>. Acesso em: 29 maio 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: Fundamentos da Lei Geral de Proteção de Dados. *E-book*. 2. ed. São Paulo: Thomson Reuters, 2020.

DONEDA, Danilo. Fundamentos teóricos e históricos da proteção de dados pessoais. *In*: BIONI, Bruno; MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (Coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. *E-book*. ISBN 9788530992200. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 02 abr. 2023.

FLORIDI, Luciano; TADDEO, Mariarosaria. Introduction: What is data ethics? **Philosophical Transactions: Mathematical, Physical and Engineering Sciences**, [s.l.], v. 374, n. 2083, 2016. Disponível em: <https://www.jstor.org/stable/26115816>. Acesso em: 27 maio 2023.

HARADA, Eduardo. Fail épico: sistema do Google identifica pessoas negras como gorilas, **Tecmundo**, [s.l.], jul. 2015. Disponível em: <https://www.tecmundo.com.br/google-fotos/82458-polemica-sistema-google-fotos-identifica-pessoas-negras-gorilas.htm>. Acesso em: 09 jun. 2023.

HOFFMANN-RIEM, Wolfgang. Big data e Inteligência Artificial: desafios para o direito. Tradução por: Gabriella Bezerra Sales Sarlet e Carlos Alberto Molinaro. **Revista de Estudos Institucionais**, [s.l.], v. 6, n. 2, maio/ago.2020. DOI: 10.21783/rei.v6i2.484. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/484>. Acesso em: 22 abr. 2023.

IBM SECURITY. **Relatório de custo da violação de dados em 2022**. São Paulo: ITM Brasil Ltda, 2022.

LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil – RBDCivil**, [s.l.], v. 26, out./dez. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584>. Acesso em: 22 abr. 2023.

LINDOSO, Maria Cristine Branco. Igualdade por design: novas formas de pensar o fim da discriminação por algoritmos e data mining. **Revista de Direito e as Novas Tecnologias**, São Paulo, n. 13, ano IV, 2021. Acesso mediante assinatura da Base Revista dos Tribunais. Disponível

em: <https://revistadotribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b000001889c4d5e6366b5cf2a&docguid=I6fd33110533011ecbc698533b2d39e4e&hitguid=I6fd33110533011ecbc698533b2d39e4e&spos=1&epos=1&td=1&context=12&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 23 abr. 2023.

LUTZKY, Daniela Courtes. **A reparação de danos imateriais como direito fundamental**. Porto Alegre: Livraria do Advogado Editora Ltda, 2012.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Compliance digital e responsabilidade civil na Lei Geral de Proteção de dados. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson. **Responsabilidade civil e novas tecnologias**. São Paulo: Editora Foco, 2020.

MEDON, Filipe. Tendências para a responsabilidade civil da Inteligência Artificial na Europa: a participação humana ressaltada. *In*: MIGALHAS, [s.l.], 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/335801/tendencias-para-a-responsabilidade-civil-da-inteligencia-artificial-na-europa--a-participacao-humana-ressaltada>. Acesso em: 27 maio 2023.

MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados do mundo. *In*: MIGALHAS, [s.l.], 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo>. Acesso em: 23 abr. 2023.

MIRAGEM, Bruno; PETERSEN, Luíza. **Direito dos Seguros**. Porto Alegre: Grupo GEN, 2022. *E-book*. ISBN 9786559645435. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559645435/>. Acesso em: 29 maio 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA. **Recomendação sobre a Ética da Inteligência Artificial**. [S.l.]: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_por. Acesso em 29 maio 2023.

PEREIRA, João Sérgio dos Santos Soares. E-personality aos robôs dotados de inteligência artificial: uma terceira via de personalidade? Utopia ou Realidade? – A necessidade de discutir a interação entre seres humanos e robôs. **Revista de Direito e as Novas Tecnologias**, São Paulo, v.7, 2020. Acesso mediante assinatura da Base Revista dos Tribunais. Disponível em: <https://revistadotribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b00000188975bca442ffe9bbd&docguid=Ic014af30a48811ea9c19bc57168f93fc&hitguid=Ic014af30a48811ea9c19bc57168f93fc&spos=2&epos=2&td=4&context=181&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 26 maio 2023.

PHILMLEE, Don. Practice Innovations: Fighting back fast – Artificial Intelligence Comes to Cybersecurity. *In*: THOMSON REUTERS. [**homepage**], 2020. Disponível em: <https://www.thomsonreuters.com/en-us/posts/legal/practice-innovations-january-ai-cybersecurity/>. Acesso em 02 jun. 2023.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2021. *E-book*. ISBN 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 08 jun. 2023.

PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da Inteligência Artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, [s.l.], v. 7, n. 3, 2017. Disponível em: <https://doi.org/10.5102/rbpp.v7i3.4951> . Acesso em: 22 abr. 2023.

REIS, Nazareno César Moreira; FURTADO, Gabriel Rocha. Decisões automatizadas: definição, benefícios e riscos. **Civilistica.com**, Rio de Janeiro, v. 11, n. 2, 2022. Disponível em: <http://civilistica.com/decisoes-automatizadas/>. Acesso em: 21 maio 2023.

RIPERT, Georges. **Aspectos Jurídicos do Capitalismo Moderno**. São Paulo: Red Livros, 2002.

RIVELLI, Fabio. O projeto “AI for Humanity” a estratégia francesa. *In*: MIGALHAS, [s.l.], 2021. Disponível em: <https://www.migalhas.com.br/coluna/ia-em-movimento/376364/o-projeto-ai-for-humanity-a-estrategia-francesa>. Acesso em: 20 maio 2023.

SARLET, Ingo Wolfgang.; SARLET, Gabrielle Bezerra Sales; BITTAR, Eduardo Carlos Bianca. **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital**. São Paulo: Editora Saraiva, 2022. *E-book*. ISBN 9786555599527. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555599527/>. Acesso em: 29 maio 2023.

SCHREIBER, Anderson. **Direitos da personalidade**. 2. ed. São Paulo: Editora Atlas S/A, 2013.

SCHWAB, Klaus. The Fourth Industrial Revolution - FOREWORD. **Journal of International Affairs Editorial Board**, Nova Iorque, v. 72, n. 1, 2018. Disponível em: <https://www.jstor.org/stable/26588338>. Acesso em: 15 abr. 2023.

SÊMOLA, Marcos. Vazamento de informações. *In*: PINHEIRO, Patricia Peck. **Segurança Digital – Proteção de Dados nas Empresas**. Rio de Janeiro: Grupo GEN, 2020. *E-book*. ISBN 9788597026405. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026405/>. Acesso em: 21 maio 2023.

SILVA, Anthony Charles de Novaes da; OLIVO, Carlos Augusto Acosta. O futuro é hoje: o impacto da tecnologia nos seguros. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 15, ano 5, abr.-jun. 2022. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em: <https://revistadotribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b000001889759c2bd7c539beb&docguid=I689d3f70e3be11ec8b36b35cb5d3a37f&hitguid=I689d3f70e3be11ec8b36b35cb5d3a37f&spos=3&epos=3&td=3&context=147&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1>. Acesso em: 29 maio 2023.

SOARES, Marcos José Porto. Impacto da evolução tecnológica no reconhecimento de novos direitos: proteção dos dados pessoais e uso adequado da inteligência artificial. **Revista de**

Direito e as Novas Tecnologias, São Paulo, v. 15, ano 5, abr.-jun. 2022. Acesso mediante assinatura da base Revista dos Tribunais. Disponível em: <https://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2022-9795>. Acesso em: 22 abr. 2023.

SOUZA, Carlos Affonso. O debate sobre personalidade jurídica para robôs. *In*: JOTA, [s.l.], 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-debate-sobre-personalidade-juridica-para-robos-10102017>. Acesso em: 27 maio 2023.

TEFFÉ, Chiari Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro v.9, n.1, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em: 15 abr. 2023.

TORRES, Alisson B.; RENDÓN, Fredy F.; GUTIÉRREZ, Juan F. Revisión de las técnicas de inteligência artificial aplicadas en seguridad informática. **Revista Ontare**, [s.l.], v. 8, 2020. Disponível em: <https://doi.org/10.21158/23823399.v7.n0.2019.2612>. Acesso em: 21 maio 2023.

UNIÃO EUROPEIA. Parlamento Europeu. **Parlamento na vanguarda das normas europeias sobre inteligência artificial**. [S.l.], 2020. Disponível em: <https://www.europarl.europa.eu/news/pt/press-room/20201016IPR89544/parlamento-na-vanguarda-das-normas-europeias-sobre-inteligencia-artificial>. Acesso em: 27 maio 2023.

UNIÃO EUROPEIA. Regulamento (UE) n° 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretriz 95/46/CE. **Jornal Oficial da União Europeia**, Estrasburgo, 04 maio 2016. Disponível em: <https://gdpr-info.eu/>. Acesso em: 15 abr. 2023.

UNIÃO EUROPEIA. Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)). **Jornal Oficial da União Europeia**, [s.l.], 2017. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52017IP0051>. Acesso em: 28 maio 2023.

VAZ, Caroline. Revisitando a Responsabilidade Civil: aspectos relevantes da antiguidade à contemporaneidade pandêmica. **Revista do Ministério Público do RS**, Porto Alegre, n. 87, jan. 2020 – jun. 2020. Disponível em: <https://www.revistadomprs.org.br/index.php/amprs/article/view/190/80>. Acesso em: 29 maio 2023.

VITALIS, André. **Informartique, pouvoir et libertés**. Paris: Econômica, 1981.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The right to privacy. **Harvard Law Review**, Boston, vol. 4, n. 5, 1890. Disponível em: <https://www.jstor.org/stable/1321160>. Acesso em: 25 mar. 2023.

YASAR, Kinza. Wearable technology. TECHTARGET, [homepage], [s.l.], 2022. Disponível em: <https://www.techtargget.com/searchmobilecomputing/definition/wearable->

technology#:~:text=Wearable%20technology%20is%20any%20kind, clothing%20or%20elements%20of%20clothing. Acesso em: 29 maio 2023.