O DIREITO À REVISÃO DAS DECISÕES AUTOMATIZADAS DE RECONHECIMENTO FACIAL E O PRINCÍPIO ANTROPOCÊNTRICO

THE RIGHT TO REVIEW AUTOMATED DECISIONS OF FACIAL RECOGNITION AND THE ANTHROPOCENTRIC PRINCIPLE

Caio Sperandeo de Macedo

Doutorado em Filosofia do Direito pela Pontifícia Universidade Católica de São Paulo, PUC/SP (2014), Brasil, Mestrado em Direito do Estado pela Pontifícia Universidade Católica de São Paulo (2005) Professor Permanente da Pós-graduação do Programa de Mestrado "strictu sensu" em Direito da Sociedade da Informação, do Centro Universitário das Faculdades Metropolitanas Unidas-UniFMU/SP.
E-mail: caio.csm@terra.com.br

Recebido em: 20/10/2022
Aprovado em: 09/11/2023

RESUMO: Analisar a proteção de dados pessoais, inclusive nos meios digitais erigido a condição de direito fundamental na Constituição da República Federativa do Brasil de 1988 e minudenciado pela Lei nº13.709/2018. Reconhecer as externalidades da economia digital e que o uso das tecnologias de inteligência artificial(IA) para captura de dados biométricos para reconhecimento automatizado de características humanas para fins de segurança pública e persecução penal em espaços públicos implicam em restrições às liberdades, à autodeterminação informacional e à privacidade do cidadão em um cenário de assimetria informacional. A complexidade do tema referente a proteção de dados pessoais sensíveis e os elevados riscos de utilização destas novas tecnologias, que apresentam reconhecidos vieses discriminatórios, exige além de legislação que especifique as hipóteses de sua aplicação, estudos de impacto prévio e salvaguardas para a defesa de direitos, como a inafastável possibilidade de revisão humana das decisões automatizadas enquanto postulado ético ligado à dignidade humana. A pesquisa fez uso do método dedutivo e se embasou na revisão bibliográfica de doutrina nacional e estrangeira, além da análise comparativa da legislação nacional com as diretrizes da legislação europeia de proteção de dados – Regulamento (UE) n.º2016/679.

Palavras-chave: Algoritmos de inteligência artificial. assimetria informativa. direito fundamental. proteção de dados pessoais.

ABSTRACT: To analyze the protection of personal data, including in digital media, established as a fundamental right in the Constitution of the Federative Republic of Brazil of 1988 and detailed by Law No. 13,709/2018. Recognize the externalities of the digital economy and that the use of artificial intelligence (AI) technologies to capture biometric data for automated recognition of human characteristics for the purposes of public safety and criminal prosecution in public spaces, imply restrictions on freedoms, informational self-determination and citizen privacy in a scenario of information asymmetry. The complexity of the issue of protection of sensitive personal data and

the high risks of using these new technologies, which have recognized discriminatory biases, require, in addition to legislation that specifies the hypotheses of their application, prior impact studies and safeguards for the defense of rights, as the inescapable possibility of human review of automated decisions, as an ethical postulate linked to human dignity. The research made use of the deductive method and was based on the literature review of national and foreign doctrine, in addition to the comparative analysis of national legislation with the guidelines of European data protection legislation - Regulation (EU) No. 2016/679.

Keywords: Artificial intelligence algorithms; informational asymmetry; fundamental right; personal data protection.

SUMÁRIO: Introdução. 1 Revoluções industriais e cidades inteligentes. 2 Câmeras de reconhecimento facial – contexto cidades inteligentes. 2.1 Reconhecimento facial e decisões automatizadas adotadas por algorítmo de *machine learning*. 3 Anomia normativa referente às decisões automatizadas adotadas para as hipóteses do art. 4, III, letras a, b, c, d, da LGPD. 4. A Emenda Constitucional Nº115/2022, de 11/02/2022, introduz novo direito fundamental às cláusulas pétreas? 5 Contaminação das liberdades pelas novas tecnologias. 6 Decisões automatizadas e Direito a não discriminação. 7 Princípio antropocêntrico à intervenção humana sobre decisões automatizadas conduzidas inteiramente por máquina. Considerações. Referência.

INTRODUÇÃO

O presente trabalho tem por escopo analisar criticamente o regramento normativo em nosso país referente à proteção de dados pessoais, inclusive nos meios digitais, e compará-lo com as disposições da União Europeia a respeito do tema, destacar os riscos socias decorrentes da aplicação das tecnologias de Inteligência artificial em ambientes públicos, notadamente em caso de utilização dados biométricos para fins de segurança pública e atividades de investigação e repressão de infrações Penais. Referendar a necessidade de se prever em lei a revisão humana das decisões automatizadas como imperativo ético para exercício do Direito a não discriminação.

Assim, na primeira seção estabelecer uma linha cronológica genérica para contextualizar os períodos históricos e avanços tecnológicos respectivos conforme as Revoluções Industriais consideradas na modernidade e pós-modernidade até o surgimento da economia digital ou atual Sociedade de Dados(*Data Driven Economy*[1]) ou ainda por outro enfoque como Capitalismo de Vigilância (ZUBOFF, 2019).

Na segunda seção, comentar o funcionamento das cidades inteligentes (*smart cities)* e de grandes adensamentos urbanos, emergindo as novas tecnologias e especialmente a Tecnologia de Reconhecimento Facial (TrF) como uma alterativa sedutora para o exercício de poder de polícia mais efetivo. Problematizar os riscos ínsitos à liberdade e à privacidade dos cidadãos diante do potencial caráter discriminatório (*machine bias*) perpetrado pelos algoritmos de inteligência artificial (IA) que se utilizam de tratamento automatizado dados biométricos, considerados dados pessoais sensíveis.

Em séquito, estabelecer a premissa de que os algoritmos de inteligência artificial utilizados para o reconhecimento facial em verdade não adotam uma decisão, do azo que não possuem livre arbítrio para agir com independência, ao operar de forma condicionada e baseado nos dados de treinamento com os quais seu sistema foi valorado pelo programador.

Na terceira seção, comentar sobre a anomia normativa referente a decisões automatizadas a serem adotadas nos conteúdos previstos pelo art. 4, III, letras a, b, c, d, da LGPD, destacando as

[1] Disponível em: https://www.intereconomics.eu/contents/year/2019/number/4/article/data-driven-economy-challenges-and-opportunities.html. Acesso em 15.fev.2022

hipóteses das letras "a"(segurança pública) e "d"(atividades de investigação e repressão infrações Penais), ligadas mais diretamente ao uso das tecnologias de reconhecimento facial para locais públicos, que permanecem sujeitas a futura legislação, e que deverão enquanto não sobrevier a lei própria, ser equacionadas subsidiariamente pela Lei nº13.709/2018.

Referendar a insegurança jurídica da sociedade, pois embora existam projetos legislativos em discussão atualmente no Senado Federal, verifica-se que o Poder Público está antecipadamente a implementar a franca expansão dos usos das tecnologias que utilizam algoritmos de inteligência artificial para reconhecimento automatizado de características humanas, sem que estejam asseguradas previamente salvaguardas específicas em norma legal, a fim de proteger as liberdades e direitos dos cidadãos.

Na quarta seção, declinar sobre a constitucionalização da proteção de dados pessoais, inclusive nos meios digitais (conforme EC-nº115/2022), elevando o direito à proteção de dados pessoais a condição de direito fundamental (Art. 5º, inciso LXXIX, CF/88).

Na quinta seção, comentar a ideia de contaminação das liberdades pelas novas tecnologias, como a tecnologia de inteligência artificial para reconhecimento facial e enaltecer o princípio da precaução como vetor a guiar os debates legislativos concernente ao tema, que deve ter por escopo o bem-estar social, para que que o resultado do tratamento de dados pessoais seja o menos gravoso para resguardar os direitos dos cidadãos.

Na sexta seção, estabelecer a necessidade de se prever em legislação a possibilidade de revisão humana das decisões automatizadas como imperativo ético para a ampla defesa do Direito a não discriminação (Art. 6º da LGPD) e possibilitar a apreciação por pessoa natural sobre o desfecho de um processo decisório conduzido inteiramente por máquina.

E na sétima e última seção objetiva reconhecer a aplicação do princípio antropocêntrico a legitimar a intervenção humana sobre decisões automatizadas conduzidas inteiramente por máquinas como corolário do art. 5º, inciso LXXIX (proteção de dados pessoais), e inciso LV (ampla defesa), quando envolver a proteção de dados pessoais sensíveis, sob pena de se compactuar com a erosão da autodeterminação e da dignidade da pessoa humana.

Justifica-se a pertinência temática em face de seu pleno desenvolvimento junto à realidade social e jurídica brasileira e mundial, para compreender a ubiquidade da Economia de Dados(*Data Driven Economy*) que se utiliza massivamente de dados pessoais como ativo estratégico para as mais diversas finalidades(por exemplo, para segurança pública e atividades de investigação e repressão infrações Penais), operando muitas vezes em evidente ofensa à proteção de dados pessoais, à autodeterminação informativa e ao direito à privacidade dos cidadãos, não nos olvidando de reiterar o caráter discriminatório dos algoritmos de inteligência artificial.

A metodologia utilizada na elaboração do artigo foi uma pesquisa jurídico-dogmática com raciocínio dedutivo e técnica de pesquisa legislativa e bibliográfica, partindo-se do texto normativo da Lei nº13.709/2018(Lei Geral Proteção Dados), engrandecida pela Emenda Constitucional nº115/2022 e demais vetores axiológicos constitucionais, além da análise comparativa de previsões da *General Data Protection Regulation*(Regulamento (UE) n.º2016/679), norma comunitária europeia que serviu de inspiração para a LGPD, para concluir que se faz imprescindível reconhecer valores éticos imanentes que inviabilizam que decisões automatizadas de alto risco social, produzidas por sistemas de inteligência artificial com viés discriminatório possam prejudicar a vida das pessoas, sem que lhes seja garantido em seu direito à ampla defesa a participação humana no processo revisional.

1 REVOLUÇÕES INDUSTRIAIS E CIDADES INTELIGENTES (*smart cities*)

Pode-se dizer que a Primeira Revolução Industrial teria surgida na metade do século XVIII (1760 – 1840) e foi possibilitada basicamente pela máquina a vapor para mecanizar a produção; que a Segunda, no século XIX (1850-1945) envolveu predominantemente o desenvolvimento de

indústrias química, elétrica, de petróleo e aço, além do progresso dos meios de transporte e comunicação; a Terceira no século XX(1950 – 2010) fora marcada pela substituição gradual da mecânica analógica pela digital, pelo utilização de microcomputadores e criação da internet (1969) e o incremento da tecnologia da informação e da comunicação.

Atualmente, no primeiro quarto do Século XXI, a Quarta Revolução Industrial (SCHAWAB, 2016, prefácio e I capítulo)[2], nominada como Revolução 4.0 – teria como marco temporal inicial ano de 2011 e se consubstancia na confluência de todas as tecnologias no estado da arte existentes e que efetivamente estão transformando a sociedade mundial em um novo panorama envolvendo a robótica, uso de inteligência artificial nos mais diversos usos como os algoritmos que geram decisões automatizadas, tecnologia de reconhecimento facial (TrF), agentes artificiais-*Bots,* Internet das coisas (Iot); Tecnologia 5G, desenvolvimento de computadores quânticos; coleta massiva e armazenamento de dados pessoais para predições políticas públicas (fins estatísticos; demográficos) etc..

Por corolário do paradigma da economia digital inserido com a Quarta Revolução, surge concomitantemente o conceito de Cidades inteligentes - *smart cities*, que incorporam aos centros urbanos o uso integrado destas novas tecnologias à infraestrutura baseada lato sensu em TIC´s, com a modernização dos mecanismos de atuação e estratégias para melhorar a eficiência da administração pública e de serviços urbanos de forma célere, econômica e sustentável, no intuito almejado de valorizar a qualidade de vida (JOÃO, SOUZA e SERRALVO, p.4, 2019).

Soluções tecnológicas integradas (interconexão de bens e serviços) passam a ser adotadas pela administração pública e iniciativa privada para superar desafios de planejamento e gestão decorrentes de urbanização nas grandes cidades com relação a infraestrutura e as políticas públicas em setores estratégicos para o desenvolvimento como, por exemplo: o fornecimento de energia; logística de transportes, iluminação pública, prestação de serviços de saúde, cadastros para tutela de aposentados e pensionistas em sistema de previdência ("prova de vida"), na análise de credito, segurança pública, persecução criminal, etc.

Enfim, aludidas soluções integradas têm por escopo superar com a utilização das novas tecnologias digitais óbices técnicas e conjunturais para fornecer serviços mais eficientes decorrente do contínuo adensamento urbano e incremento econômico.

E por outra perspectiva, a utilização deste aparato tecnológico -que pressupõe coleta e tratamento massivo de dados pessoais para treinamento, análises estatísticas e predições comportamentais pelos algoritmos de inteligência artificial(IA), resta implicada a diminuição da liberdade(de expressão, de informação, de comunicação, de opinião) e da privacidade(intimidade, honra, imagem) do cidadão, nisso incluídos ofensa ao seu direito fundamental à autodeterminação informativa(ADI 6389-STF) e à proteção de seus dados pessoais, inclusive nos meios digitais (EC-nº115/2022).

Não nos olvidando sobre o potencial caráter discriminatório (*machine bias*) que pode ser perpetrado pelos algoritmos de inteligência artificial (IA) decorrente de decisões baseadas unicamente em tratamento automatizado de dados e consequente lesão a direitos.

A fim de conciliar as externalidades negativas envolvendo restrições de direitos em decorrência da nova ordem socioeconômica e o desenvolvimento tecnológico ínsito, entende-se que o assunto enfocado deve ser regulado por legislação específica, compatível com o que dispõem os princípios do art.6º e incisos I a X, da LGPD(Lei nº13.709/2018) e deverá ser interpretado

[2] Após a internet e a internet móvel terem dado a largada para a terceira revolução industrial, as tecnologias de Inteligência Artificial (IA), direcionadas por big data, estão desencadeando uma quarta revolução industrial. (...): A convergência de IA e big data começou no início dos anos 2000. Quando o Google e o Baidu – os novos mecanismos de busca da época – passaram a utilizar sistemas de recomendação para propagandas alimentados por IA, e descobriram que os resultados eram ainda melhores que o esperado. E quanto mais dados coletavam, melhores eram os resultados. Mas, naquele momento, ninguém percebeu que isso poderia ser aplicado também em outras áreas. Conforme Yang Qiang, entrevistado por Wang Cha. Disponível em: https://pt.unesco.org/courier/2018-3/quarta-revolucao. Acesso em 15.Fev.2022.

conjuntamente com os valores da Constituição Federal de 1988 e conteúdos axiológicos imanentes que auxiliem a efetividades de valores voltados para assegurar o exercício de direitos fundamentais e a dignidade da pessoa humana.

2 CAMERAS DE RECONHECIMENTO FACIAL – CONTESTO CIDADES INTELIGENTES (*smarts cities*)

Dentro do contexto do funcionamento das cidades inteligentes e de grandes adensamentos urbanos, a Tecnologia de Reconhecimento Facial (TrF) é apontada como alterativa sedutora para a proteção e expectativa de segurança da sociedade diante da ubiquidade e capilaridade de vigilância e de exercício de poder de polícia mais efetivo com diversos usos possíveis, como, por exemplo, na identificação de pessoas em aeroportos; de foragidos da justiça; procurar suspeitos em bases de dados; identificar vítimas de tráfico de seres humanos ou de exploração sexual; abuso de menores; na persecução penal, monitoramento eletrônico de condenados pelo sistema judiciário e outros.

Como é cediço, a LGPD(Lei Geral de Proteção de dados – 13.709/2018**)** considera como dado pessoal toda informação relacionada a pessoa natural identificada ou identificável (art. 5, I). E as Tecnologias de Reconhecimento Facial (TrF) ao *escannear*, medir, fotografar, capturar partes do corpo humano, formas e padrões de superfície (LEE-MORINSON, 2019), estão compreendidos dentro de dados pessoais sensíveis, enquanto dados biométricos (PUGLIESE, 2010), a rogo do art 5º, II, da LGPD, para exercer com grande probabilidade de acerto a tarefa de identificação de pessoas para finalidades ligadas predominantemente à segurança pública e atividades de investigação e repressão a infrações Penais.

Entre as diferenças básicas de arquitetura do sistema de funcionamento dos algoritmos, a doutrina faz referência a (i) Sistema *Analytics* – composto por dados já estruturados, onde algoritmos fazem previsões (relacionadas com a projeção de dados passados no futuro) sobre a análise de informações e cruzamentos conforme amostras prévias integrada por dados em que parâmetros são inseridos a priori. E o (ii) Sistema *Machine learning* – em que os algoritmos são capazes de predizer (trabalham com estimativas e probabilidades do que se espera acontecer no futuro se utilizando da matemática e da estatística) e generalizar padrões apreendidos a partir de um conjunto de dados utilizados para "treinar" seu sistema (WOLKART, 2019, p. 706).

Ao que nos interessa, na vertente dos algoritmos que utilizam a tecnologia de *machine learning* o sistema tem a capacidade de *aprender* em interação com ambiente externo no qual realiza as correlações estabelecidas em sua programação, para reconhecer padrões com base em dados não organizados como fotos, vídeos ou textos. A maioria dos *softwares* de identificação de reconhecimento facial funciona dentro do gênero *machine learning,* e depende de grande quantidade de dados disponíveis da rede virtual para calibrar suas inferências, espécie denominada *deep learning* (Pinto, 2019, p.45/46).

Em síntese, algoritmos de inteligência artificial para reconhecimento automatizado de características humanas em ambientes públicos, como o reconhecimento facial, possibilita a captura de imagem do cidadão, que será confrontando com banco de dados do *software* para verificar ou autenticar sua identidade. E tem escopo responder ao questionamento: A qual pessoa (identidade) pertence essa face coletada? [3].

2.1 Reconhecimento facial e decisões automatizadas adotadas por algoritmo de *machine learning*

[3] Recentemente, mafioso italiano (G. Gammino), foragido há 20 anos da justiça, foi preso na Espanha após aparecer e ser identificado no Google Maps, street view. Disponível: https://epocanegocios.globo.com/Mundo/noticia/2022/01/mafioso-italiano-foragido-e-preso-na-espanha-apos-aparecer-no-google-maps.html. Acesso em: 5 ja.2022.

Pode-se estabelecer para fins de melhor compreensão do processo que existem 6 (seis) etapas do percurso para que máquinas executem as *decisões* automatizadas para efetivar o reconhecimento facial, respectivamente: (i) a máquina coleta dados de imagens automaticamente por câmeras apontadas aos transeuntes em via pública (dados de entrada); (ii) o modelo analisa essas imagens comparando-as com imagens de seu banco de dados que foram previamente utilizados para treinar o sistema antes de colocá-lo para funcionar de forma institucionalizada (por exemplo, imagens disponíveis dos foragidos da justiça[4]), a fim de que faça a associação determinada como *correta* pelo programador; (iii) executado o cruzamento entre a imagem capturada e as existentes em seu banco de dados, se for encontrada uma relação coincidente, a máquina faz a predição e detecta que ali possivelmente está um foragido, com base na alta probabilidade de seu repertório; (iv) em seguida, a máquina *julga* e sinaliza o suspeito para o operador; (v) com base nessa operação adotar-se-á uma ação que pode ser humana ou automatizada para determinar a detenção do cidadão, que poderá estar correta ou incorreta; (vi) conforme o resultado do procedimento (correto ou incorreto), a depender de uma análise humana posterior dos acontecimentos, a máquina será realimentada (dados em feedback), para reforçar ou refutar aquele julgamento (REIS, 2021, p.85/86).

Como se depreende do acima exposto, em termos próprios a máquina em verdade não adota uma *decisão* vez que não tem possibilidade de escolher em função da própria convicção, não tem independência moral para agir de acordo com sua consciência ou *julgar* com esteio em valores éticos ou de equidade sobre qual seria a solução mais adequada para a situação enfrentada.

Vez que o algoritmo que comanda seu funcionamento é programado para lhe determinar qual será a decisão *correta* naquele contexto, já que opera de forma condicionada e conforme os dados de treinamento previamente inseridos no seu sistema, calibrado pelo interesse estabelecido pelo programador (REIS, 2021, p.84).

No mesmo sentido, apontam MARQUES e NUNES (2018), ao se referir as escolhas subjetivas e vieses ocultos inerentes a atuação do programador, desenvolvedor do algoritmo:

> Essas escolhas, portanto, fazem com que sempre haja pontos cegos nos algoritmos, os quais refletem os objetivos, prioridades e concepções de seu criador, de modo que os modelos são, a todo tempo, permeados pela subjetividade do sujeito que os desenvolve (MARQUES e NUNES, 2018, p. 4)

No caso de dados pessoais sensíveis, como o são os dados biométricos, o consentimento do titular para tal tratamento em tese deveria ser livre, informado e inequívoco e em vista de finalidade específica (5, XII LGPD), cônscio sobre quais procedimentos estão sendo aplicados, em respeito à autodeterminação informativa (art, 2, II) e aos seus direitos de personalidade. Ou seja, o consentimento específico representa a autonomia de atuação do titular e não autoriza o uso irrestrito para tratamento de seus dados seja por instituições públicas ou privadas.

Porém, o consentimento é relativizado quando o tratamento incidir nas exceções II, art. 11, LGPD (proteção da vida física do titular ou terceiro; aplicação politicas publicas previstas em lei; prevenir fraudes; cumprimento obrigação legal ou regulatória).

Outrossim, existem temas regulados subsidiariamente, no sentido de que a LGPD não se aplica ao tratamento dados pessoais para fins exclusivos de (i) segurança pública, (ii) defesa nacional, (iii) segurança do Estado e (iv) atividades de investigação e repressão infrações Penais (LGPD, art. 4, III, a, b, c, d), estando tais temas sujeitos a futura legislação (4, §1º), e que deverão enquanto não sobrevier a lei própria prever medidas proporcionais e necessárias ao interesse público, observado o devido processo legal e os princípios gerais de proteção (2 a 6º LGPD) e os direitos do titular (17 a 22 LGPD).

[4] Por exemplo: Disponível: https://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/programas-e-projetos-menu/foragidos-da-justica. Acesso em 11 mai.2022.

E que cabe à Autoridade Nacional de Proteção de Dados – ANPD a tarefa de regulamentar e fiscalizar, na falta de lei específica, tratamento de dados não sujeito inteiramente a LGPD, mediante opiniões técnicas ou recomendações e solicitar Relatórios de Impacto à Proteção Dados Pessoais-RIPDP (art. 4,§3º).

E aludido RIPDP -relatório pelo qual o controlador registra seu processo de tratamento de dados e as medidas para mitigar os riscos aos direitos dos titulares dos dados, embora importante, não teve seu procedimento previsto na LGPD e também deve ser objeto de legislação posterior.

Assim, enquanto a anomia normativa persistir (ausência de legislação especifica nas hipóteses referidas), tais temas ficam sujeitos aos elementos genéricos previsto art. 20, LGPD quanto a eventuais decisões automatizadas adotadas nas searas do art. 4, III, letras a, b, c, d, da LGPD.

3 ANOMIA NORMATIVA REFERENTES ÀS DECISÕES AUTOMATIZADAS ADOTADAS PARA AS HIPÓTESES ART. 4, III, letras a, b, c, d, da LGPD

Como preconizado, diante da ausência de legislação especifica nas hipóteses referidas, e nos atendo as hipóteses das letras "a"(segurança pública) e "d"(atividades de investigação e repressão infrações Penais), tais temas estão sujeitos a futura legislação (4, §1º), e que deverão enquanto não sobrevier a lei própria, prever medidas proporcionais e necessárias ao interesse público, observado o devido processo legal e os princípios gerais de proteção (2 a 6º LGPD) e os direitos do titular (17 a 22 LGPD).

É de se observar a insegurança jurídica da sociedade concernente à regulação da Inteligência Artificial -assunto cuja aplicação e usos estão diretamente ligado aos temas sujeitos a futura legislação- e que atualmente tramitam no Poder Legislativo, respectivamente, o Projeto de lei nº21/2021(Redação Final assinada pela Relatora, Dep. Luisa Canziani (PTB-PR), aprovado na Câmara[5] e entrado no Senado Federal, e o Projeto de Lei n°5051, de 2019 no Senado (autoria do Sen. Styvenson Valentim (PODEMOS/RN), tramitando no Senado[6] que buscam cada qual regulamentar e estabelecer os princípios para o uso da Inteligência Artificial no Brasil.

E no Poder Executivo, temos a Estratégia Brasileira de Inteligência Artificial - EBIA[7], documento do Governo Federal, de julho de 2021, que enaltece os sistemas de reconhecimento facial e de policiamento inteligente para seus usos, e estabelece dentre as ações estratégicas, a utilização ética para uso da IA; mecanismos para célere apuração de denúncias e reclamações sobre violações de direitos em decisões realizadas por sistemas de IA; análise de impacto nos casos de uso da IA que afetem diretamente o cidadão e demais elementos (p. 45) etc..

Contudo, ressalta-se que tais iniciativas (legislativa e administrativa, respectivamente) embora importantes, não possuem força cogente apta a preencher a lacuna no tocante a (i) segurança pública, (ii) defesa nacional, (iii) segurança do Estado e (iv) atividades de investigação e repressão infrações Penais (LGPD, art. 4, III, a, b, c, d).

E que atualmente, no que se refere à segurança pública (letra a), e atividades de investigação e repressão infrações penais (letra d), verifica-se a franca expansão da implantação de usos das tecnologias que utilizam algoritmos de inteligência artificial para reconhecimento automatizado de características humanas de Reconhecimento Facial apenas com amparo nas previsões gerais acima referidas da LGPD.

---

[5] Disponível:https://www.camara.leg.br/internet/ordemdodia/integras/2082600.htm. Acesso:13 mai. 2022.

[6] Embora ainda esteja em discussão inicial, o projeto de lei do Senado, diferentemente do oriundo da Câmara, prevê em seu art. 4º que: Os sistemas decisórios baseados em Inteligência Artificial serão, sempre, auxiliares à tomada de decisão humana. Disponível:https://www25.senado.leg.br/web/atividade/materias/-/materia/138790. Acesso: 13 mai. 2022.

[7] Disponível: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_documento_referencia_4-979_2021.pdf. Acesso em: 13 mai. 2022.

Conforme informações disponíveis de 2021, a Polícia Federal anunciou recentemente a implementação do sistema ABIS (Solução Automatizada de Identificação Biométrica), que realizará coleta, armazenamento e o cruzamento de dados da impressão digital e reconhecimento facial, a fim de permitir a identificação de indivíduos [8].

Tal sistema foi planejado para contemplar dados de 50,2 milhões de indivíduos, em 48 meses, sendo viável ampliação posterior que pode resultar em dados de até 200 milhões de pessoas. O sistema começa a operar com aproximadamente 22,2 milhões de dados. E os Estados da federação seguem na mesma senda e começam a adotar a mesma política de vigilância pelos instrumentos de inteligência artificial voltados para o reconhecimento facial [9].

Como se depreende, embora uso de inteligência artificial para reconhecimento automatizado de características humanas em espaços públicos, como o reconhecimento facial, estejam sendo amplamente implementados em todo o país, ainda não existe legislação compatível para regulamentar o mister ou definidos padrões técnicos (art, 46, §1º, LGPD) para sua utilização pela ANPD, considerando-se o alto risco de possível viés discriminatório.

Por outro vértice, impende referir que na Europa, cuja legislação protetiva de dados pessoais **(**2016/679 - Regulamento Geral de Proteção de Dados[10]) serviu como referência para a elaboração da nossa lei nº 13.853/19-LGPD, adota-se como regra geral a proibição de processamento automatizado(item, 26, Documento P9_TA(2021)0405)[11], tornando lícita sua utilização apenas nos casos expressamente elencados; e previsão que inclui de forma explícita os direitos à intervenção humana e a contestação de decisão automatizada como parte de salvaguardas mínimas nos casos em que as decisões automatizadas são permitidas (art. 22 da RGPD-decisões automatizadas caso a caso, incluindo criação de perfil).

E as autoridades responsáveis pela supervisão de aplicação das legislações de proteções de dados pessoais, respectivamente *European Data Protection Board e European Data Protection Supervisor*[12], se posicionaram em junho de 2021 pela proibição de utilização de algoritmos de inteligência artificial para reconhecimento automatizado de características humanas em ambientes públicos, como o reconhecimento facial, e também em qualquer contexto por seus elevados riscos, principalmente para minorias, conforme razões abaixo expostas:

> Levando em conta os riscos extremamente altos impostos por identificação biométrica remota de indivíduos em espaços públicos, a EDPB e a EDPS clamam por um banimento geral em qualquer uso de inteligência artificial para reconhecimento automatizado de características humanos em espaços públicos, como reconhecimento facial, padrão de caminhada, digitais, DNA, voz, digitação ou outros sinais biométricos ou comportamentais, em qualquer contexto.
> Similarmente, a EDPB e a EDPB recomendam o banimento[13] de sistemas de

[8] BRASIL. Ministério da Justiça e Segurança Pública. Polícia Federal implementa nova Solução Automatizada de Identificação Biométrica. 2021. Disponível em: https://www.gov.br/pf/ptbr/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-deidentificacao-biometrica. Acesso em: 10 mai. 2022

[9] Sob críticas por viés racial, reconhecimento facial chega a 20 estados. Folha de S. Paulo, 09 jul. 2021. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/07/sob-criticas-por-vies-racial-reconhecimento-facialchega-a-20-estados.shtml. Acesso em: 11 mai. 2022.

[10] Disponível: https://dsgvo-gesetz.de/art-22-dsgvo/. Acesso: 16 mai. 2022.

[11] Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais. Disponível: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html. Acesso. 17 mai. 2022.

[12] Disponível em: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en. Acesso em: 11 mai.2021.

[13] Outras países e localidades vem adotando o banimento do reconhecimento facial por órgãos públicos. Disponível em:https://olhardigital.com.br/2020/06/25/noticias/boston-proibe-uso-de-reconhecimento-facial-por-orgaos-publicos/. Acesso em 18 mai. 2022. No mesmo sentido: Disponível em: https://tab.uol.com.br/noticias/redacao/2020/01/16/cambridge-bane-reconhecimento-facial-entenda-por-que-temos-de-pensar-nisso.htm. Acesso em: 18 mai. 2022.

> inteligência artificial que utilizam biometria para caracterizar indivíduos em grupos baseados em etnicidade, gênero, orientação política ou sexual, ou quaisquer outros critérios em que a discriminação é proibida pelo Artigo 21 da Carta de Direitos Fundamentais. (tradução nossa)
> [...]

Portanto, a União Europeia baseada em uma interpretação precaucionaria entende atualmente que a tecnologia de identificação biométrica em espaços públicos apresenta elevados riscos e viola a essência de direitos fundamentais e das liberdades do cidadão em uma dimensão que esvazia o direito de estar anônimo nestes espaços socializantes contrariando os valores fundamentais da União Europeia, não se justificando (irrazoabilidade) tal intrusão nas liberdades por razões genéricas de segurança pública ou persecução criminal.

4 A EMENDA CONSTITUCIONAL Nº115/2022, de 11/02/2022, INTRODUZ NOVO DIREITO FUNDAMENTAL ÀS CLÁUSULAS PÉTREAS?

A publicação recente da Emenda Constitucional nº115/2022[14], reconheceu a necessidade de positivar a proteção de dados pessoais, inclusive nos meios digitais, com o *status* de direito fundamental, conjuntamente ao demais direitos previstos pelo Art. 5º da CF/1988. E uma vez reconhecido a proteção de dados pessoais como direito fundamental, necessário sejam compreendidos a tal *status* algumas características clássicas enaltecidas mais ou menos de forma unânime pela doutrina e que são incorporados ao arcabouço normativo da sociedade ao longo do seu desenvolvimento, respectivamente: a historicidade, inalienabilidade, irrenunciabilidade, imprescritibilidade, relatividade e universalidade.

Em linhas gerais, necessário referendar que a historicidade dos direitos fundamentais se relaciona com o fato de que eles não surgem ocasionalmente, são dinâmicos e em regra evoluem conforme o momento histórico e cultural, bem como decorrem de lutas políticas e conquistas sociais por novas liberdades; a inalienabilidade está relacionada à dignidade da pessoa humana, não podendo se transigir com os direitos fundamentais; a noção da irrenunciabilidade dos direitos fundamentais estabelece que, em regra, eles não podem ser renunciados pelo seu titular, vez que ostentam eficácia objetiva de modo proteger não apenas o sujeito, mas a toda coletividade; são imprescritíveis por que seu não exercício não acarreta a perda da exigibilidade pelo decurso do tempo; são relativos, vez que nenhum direito fundamental pode ser considerado absoluto devendo ser interpretado e aplicado conforme os limites fáticos e ponderado com demais valores constitucionais, notadamente outros direitos fundamentais; e ao derradeiro, são universais no sentido de que a titularidade é inerente a condição humana, estendendo seus atributos de forma irrestrita a todos os cidadãos tanto o exercício como a proteção dos direitos reconhecidos como fundamentais (MARCHINHACKIP, 2012,173-174).

No caso específico analisado, além da fundamentabilidade reconhecida pela EC nº115/2022, entende-se que o direito à proteção de dados pessoais passa a integrar as cláusulas pétreas (art 60, §4º, IV, CF/1988) e, portanto, estão imunes a qualquer supressão de seu predicado normativo, vez que seu conteúdo axiológico ressalta valores já protegidos pela Constituição Federal de 1988.

A ratificar tal entendimento de ficar a salvo de qualquer supressão posterior, confirma Gonet Branco[15] (BRANCO, 2017) sobre a possibilidade de declaração de novos direitos

[14] EMENDA CONSTITUCIONAL Nº 115/2022, de 11/02/2022(...)
Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:
"Art. 5º (...)
LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[15] Disponível em: https://enciclopediajuridica.pucsp.br/verbete/21/edicao-1/clausulas-petreas, Acesso em 15. Fev. 2022.

fundamentais via Emenda à Constituição de 1988 e aduz que a inclusão como cláusula pétrea poderá ou não ocorrer, conforme o caso:

> É dado também indagar se o direito fundamental criado pelo constituinte de reforma há de integrar o rol das cláusulas pétreas. Uma vez que a cláusula pétrea visa a proteger o núcleo essencial de direitos que o constituinte originário quis ver inabalado, um direito que não foi por ele levado em conta não cabe no conceito de cláusula pétrea.
> [...]
> Pode ocorrer, todavia, de uma emenda vir a acrescer o rol dos direitos fundamentais uma regra nova que explicite um direito fundamental implicitamente contido em disposição do constituinte originário. Nesse caso, a emenda não estará criando um novo direito, mas estará realçando um direito já existente, extraindo-o da regra mais ampla da Constituição originária. O problema da criação do direito não se põe nessa circunstância. A nova regra não poderá ser abolida, já que, se o for, o sentido da norma do constituinte originário sofrerá dano.

A rogo do colacionado, temos que o *status* de direito fundamental à proteção de dados pessoais, mormente dados sensíveis (como o são os dados biométricos utilizados em reconhecimento facial) se encontra protegida por cláusula pétrea e não poderá ser abolida ou sofrer retrocesso ainda que por nova Emenda Constitucional. E tal imutabilidade decorre da constatação de que seu conteúdo axiológico visa explicitar valores albergados pelo constituinte originário, notadamente as liberdades de expressão, de manifestação do pensamento, da informação, de comunicação e de opinião; bem como do direito à privacidade, inviolabilidade da intimidade, honra, e imagem das pessoas; direitos fundamentais enaltecidos no Art. 5º CF/1988.

Assim, estes direitos fundamentais primevos referidos acima foram engrandecidos pelo reconhecimento do direito à proteção de dados pessoais, inclusive nos meios digitais, como direito fundamental pelo poder constituinte derivado, vez que visam resguardar os dados sensíveis dos cidadãos diante de nova realidade socioeconômica da Economia de Dados(Data Driven Economy) ou ainda por outro enfoque, como Capitalismo de Vigilância (ZUBOFF, 2019), enquanto estado da arte do desenvolvimento tecnológico e econômico atual, que se baseia na coleta e utilização massiva de dados pessoais como um ativo independente e estratégico.

Por corolário, referenda-se que a partir da promulgação da Emenda Constitucional (ocorrida em 12/02/2022) o conteúdo normativo depreendido do direito fundamental a proteção de dados pessoais, inclusive nos meios digitais, também está apto a servir de parâmetro de controle de constitucionalidade de leis e normas infraconstitucionais incompatíveis, suscitados tanto pelo sistema difuso(via Recurso Extraordinário, 102, III, a, b, c, CF/88) quanto pelo concentrado(ação direta inconstitucionalidade, art. 102, I, a, CF/88), que deverão ser dirimidos pelo Supremo Tribunal Federal, caso provocado a decidir.

Complementarmente, cabe aduzir que a Emenda Constitucional Nº115/2022[16] ainda fixou a competência material para a União (art. 21, inciso XXVI) organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei; e também conferiu competência privativa para a União para legislar sobre proteção e tratamento de dados pessoais (Art. 22, inciso XXX), evitando-se a dispersão e falta de uniformidade na produção legislativa e aumentando a segurança jurídica

[16] EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022.
(...)
Art. 2º O caput do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI:
"Art. 21. (...)
XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei." (NR)
Art. 3º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:
"Art. 22. (...)
XXX - proteção e tratamento de dados pessoais.

com relação a proteção de dados pessoais, inclusive nos meios digitais.

O reconhecimento do direito a proteção de dados pessoais como direito fundamental, via Emenda Constitucional nº115/2022, engrandecendo posicionamento anterior do Supremo Tribunal Federal, no julgamento da ADI-STF nº6387[17], que reconheceu o direito à autodeterminação informativa, foi um passo essencial no processo de consolidação da proteção de dados pessoais em nosso país para fortalecer a resguardar as amplas previsões da LGPD, notadamente em um cenário de assimetria informacional entre os agentes de tratamento de dados (controlador e operador) e a pessoa natural, titular dos dados pessoais.

É cediço que a Lei Geral de Proteção de Dados, Lei nº13.709/2018, criada sob influência da RGPD ou GDPR-EU(Regulamento(UE) n.º2016/679), previu diversos elementos importantes, como por exemplo: seus princípios(art 1º); fundamentos(art 2º); o consentimento do titular(art. 7º); que o tratamento de dados pessoais deverão observar a boa-fé e demais princípios (art 6º, incisos de I a X); definir o legítimo interesse do controlador(art. 10); término do tratamento de dados (art. 15); tratamento de dados sensíveis (art. 17), direitos do titular de dados(art. 18); direito 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 (art. 20); tratamento de dados pelo poder público (art. 23); da responsabilidade e ressarcimento de danos (art 42) etc.

Porém, no contexto do reconhecimento do direito a proteção de dados pessoais elevado à categoria de direito fundamental pela Constituição Federal de 1988, parece-nos que a utilização dos dados biométricos, ínsitos na captura dos dados para o reconhecimento facial, carece de regulamentação específica para estabelecer formas mais restritivas de utilização de algoritmos de inteligência artificial para reconhecimento automatizado de características humanas em ambientes públicos, conforme os contextos a serem previstos, diante de seus elevados riscos, notadamente para minorias, e grupos sociais marginalizados, consoante posicionamento referendado pela EU e referido anteriormente.

5 CONTAMINAÇÃO DAS LIBERDADES PELAS NOVAS TECNOLOGIAS

De forma reflexiva, pode-se dizer que os direitos e liberdades de terceira dimensão ou geração, ligados ao valor da solidariedade, como a preservação do meio ambiente, direito à paz, qualidade de vida, a liberdade informática ou direitos no âmbito das Novas Tecnologias Informação e Comunicação-NTIC e outros, se apresentam como uma resposta ao chamado fenômeno da contaminação das liberdades, que consiste na degradação que está a acoimar os direitos fundamentais diante de determinados usos das novas tecnologias (LUÑO, 2012, p.56).

Aduz Perez Luño, com relação a tais direitos de 3ª dimensão que se faz necessário reconhecer a todos os cidadãos a legitimação para se defender de violações a bens coletivos ou interesses difusos que, por sua própria natureza, não podem ser protegidos apenas pela ótica de lesão individualizada, exigindo-se, portanto, uma mudança dos instrumentos jurídicos aptos a proteção da sociedade, superando a concepção de tutela de um processo judicial individual (LUÑO, 1991, p 215).

[17] ADI 6387 MC-REF/DF- Trecho destacado da Ementa(07/05/2020): [...] "1.Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art.5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos."[...]. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso: 25.Fev.2022.

Em alusão ao Relatório de Impacto à Proteção de Dados (RIPD) da nossa LGPD[18], relata-nos Maria Cecilia Oliveira Gomes (GOMES, 2019, p. 176) que sua origem remonta ao revogado Privacy Impact Assessment (PIA) da Diretiva 95/46/EC, e que este instrumento se converteu no atual DPIA(Data Protection Impact Assessment), relatório mandatório para processamento de dados que possam gerar altos riscos aos direitos e liberdades pessoas naturais, conforme Regulamento 216/679 e General Data Protection Regulation, art. 35[19].

Denota-se que desde a origem que aludidos relatórios de impacto à proteção de dados pessoais tanto aqui como na Europa decorrem de uma perspectiva acautelatória, confirmada pelo nosso art. 6, inciso VIII da LGPD, que estabelece o princípio da prevenção no tratamento de dados com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Na mesma linha, aprofundando o caráter acautelatório, Isadora Leardini Vidolin (VIDOLIN, 2021), ao comentar o tema, entende o risco como a eventualidade de sofrer um dano e alerta para a necessidade de aplicação também do princípio da precaução diante do fenômeno da coleta indiscriminada de dados pessoais e da vigilância que a Inteligência Artificial proporciona.

É possível vislumbrar a aplicação pratica do princípio da precaução na atuação da Autoridade de proteção dados (no caso brasileiro, art 55-A da LGPD, Autoridade Nacional de Proteção de Dados), o qual deve predizer suas convicções e orientações de caráter regulatório e técnico conforme apurar os estudos de avaliação e precificação de altos riscos de impacto na privacidade e proteção de dados. E a LGPD ainda prevê em seu Art. 55-J, em especial, que a ANPD tenha dentre outras, a atribuição de: "Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei".

Parece-nos que o princípio da precaução embora não previsto expressamente na LGPD, permeia indelevelmente a avaliação e precificação de riscos que possam implicar impacto na privacidade e proteção de dados pessoais, consoante a elaboração técnica do RIPD e na atuação regulatória da Autoridade Nacional de Proteção de Dados, notadamente para os casos de utilização de dados biométricos para fins de reconhecimento facial.

Pois, para os usos em que a inteligência artificial pode ser potencialmente lesiva, como a tecnologia de reconhecimento facial, o princípio da precaução permite que a regulação envidada seja aplicada visando o bem-estar social a fim de que o resultado do tratamento de dados seja o menos gravoso para a sociedade (MULHOLLAND, 2020, p. 18).

Conforme aduz Cavoukian (2010) com relação as tecnologias da informação, a privacidade deve se tornar parte integrante da organização, prioridades, processos de design e operações de planejamento e como objetivo principal do processo de construção de *software* e as cautelas devem ser consideradas durante o todo o ciclo de vida do sistema *(Privacy by design).*

Depreende-se que a sociedade deve avançar do conceito de autodeterminação informacional (*informational self-determination)* para a direção de arquitetura de precaução de danos (*informational – induced-harms)*, onde embora nem todos os dados podem ser considerados pessoais, todo processamento automatizado de informações deve desencadear pelo menos uma obrigação de avaliar efetivamente os impactos pretendidos e incidentais prováveis de processamento de dados sobre a vida das pessoas (PURTOVA, 2018).

[18] LGPD, Art. 5, XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

[19] GDPR, art. 35. 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação

6 DECISÕES AUTOMATIZADAS E DIREITO A NÃO DISCRIMINAÇÃO

É cediço que o Art. 6º da LGPD prevê que as atividades de tratamento de dados pessoais deverão observar a boa-fé e demais princípios inseridos, com destaque para o inciso IX, que busca garantir a não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Não obstante a previsão legal, decisões automatizadas decorrentes de padrões sociais discriminatórios (machine Bias) podem ser replicados aos algoritmos e prejudicar grupos vulneráveis. Como exemplo paradigmático, o caso da Rekognition(serviço reconhecimento facial da Amazon)[20] apresentou viés(Bias) racista, ao discriminar o gênero feminino e etnia de mulheres negras. No mesmo sentido o Twitter foi acusado adotar algoritmo discriminatório em postagens de fotos em que pessoas negras tendiam a ser minimizadas no *feed* da rede social (MONTEIRO, 2020, p.13).

O exercício do direito à revisão humana na valoração dessas decisões enviesadas é fundamental para restaurar os direitos violados, nisso inclui o art. 18, III, LGPD, que prevê o direito de correção ou direito de retificação de informações errôneas a respeito do titular de dados, como podem ocorrer com dados coletados em massa do ambiente digital levando-se em conta apenas o Internet Protocol (IP) ligado ao titular, que pode não ser o usuário exclusivo do endereço ou ser objeto de fraude.

E o art. 20 da LGPD, que garante que 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 [21].

É importante dirimir que sistemas de auxilio de decisão, que se utilizam de insumos tecnológicos automatizados para amparar tomada decisão por responsável Humano, desde que este efetue trabalho cognitivo adicional, não atrai a aplicação do art. 20, não ensejando portando direito a revisão da decisão.

É de se observar que a Perfilização ou *Profiling*, entendido como a síntese de hábitos, preferencias pessoais e outros registro de vida da pessoa, pressupondo que a pessoa tomará decisões com base em padrão predefinido (DONEDA, 2006, p. 14/15) também restou prevista na parte final do caput do art. 20, comportando igualmente direito a revisão decisões automatizadas com base em tratamento dados pessoais. Exemplo desta hipótese legal é a de Empresas de análise de credito que praticam operações automatizadas para classificar indivíduos conforme critérios eleitos como: capacidade de pagamento, o local onde fazem compras, o endereço de residência etc., violando sua privacidade e possivelmente restringindo indevidamente acesso a credito, oportunidades de emprego etc.

Assim, em síntese, o direito à revisão das decisões automatizadas tem por escopo permitir alterar/retificar o desfecho de um processo decisório conduzido inteiramente por máquina maculado por viés discriminatório; não se olvide que os preconceitos socioculturais que vicejam na sociedade acabam sendo replicados para a relação homem-máquina estabelecida na gênese entre o programador e o algoritmo por ele desenvolvido(O'NEIL, 2016).

---

[20] Disponível em: https://exame.com/tecnologia/impreciso-com-negros-sistema-de-reconhecimento-facial-da-amazon-e-suspenso/. Acesso em:15 mai. 2022.

[21] Art. 20, da LGPD ainda prevê o Direito à explicação em seu parágrafo 1º, e o parágrafo 2º, possibilidade de a ANPD auditar o tratamento de dados por informações negadas pelo controlador. [...]:

§1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Contudo, o direito à revisão das decisões automatizadas atualmente na lei não exige que a decisão revisora seja objeto de intervenção humana[22]. A previsão de que a revisão deveria ser feita por "pessoa natural" foi suprimida do §3º, art. 20, da LGPD (redação original), conforme Mensagem 288/2019 e Veto Presidencial não derrubado pelo Congresso Nacional, sob os fundamentos de que: (i) revisão humana torna inviável negócios em que a conformidade seria muito onerosa; (ii) revisão humana impactaria análise de credito em novos modelos de negócio pelas Instituições Financeiras.

Pela vigente legislação brasileira da LPGD o direito a revisão das decisões automatizadas não condiciona que a decisão revisora seja objeto de intervenção humana; ou seja, a revisão em tese pode também ser automatizada, porém, nesta hipótese, parece-nos que estaria a deslegitimar o devido processo legal administrativo [23] e o direito a proteção de dados pessoais do ofendido e demais direitos ínsitos.

7 PRINCÍPIO ANTROPOCÊNTRICO À INTERVENÇÃO HUMANA SOBRE DECISÕES AUTOMATIZADAS CONDUZIDAS INTEIRAMENTE POR MÁQUINA

Não obstante a supressão do §3º, art 20 LGPD do texto legal vigente, que garantia expressamente que a revisão da decisão fosse procedida por "pessoa natural", os valores constitucionais imanentes do art. 5º, inciso LXXIX [24] (proteção de dados pessoais), e inciso LV (ampla defesa, em processo judicial ou administrativo) combinados garantem suporte normativo a fazer prevalecer os direitos fundamentais referidos e exigem de forma implícita o direito à participação humana sobre decisões automatizadas produzidas inteiramente por máquinas quando envolver a proteção de dados pessoais, sob pena de se compactuar com a erosão da autodeterminação e da dignidade humana.

É paradigmático referendar que a União Europeia, através da Resolução P9_TA(2021)0405, em seu considerando letra "E"[25], estabelece o que ora se denomina de princípio antropocêntrico por entender que as tecnologias de inteligência artificial(IA) devem ser desenvolvidas e aplicadas de forma que o homem seja o centro das ações, cujas criações são colocadas a seu serviço; em síntese, feitas para a respeitar a condição humana e os direitos fundamentais.

E como sustentamos em linhas anteriores, os sistemas de inteligência artificial no estado da arte do desenvolvimento tecnológico não adotam uma *decisão* vez que não tem condições de dirimir em função da própria convicção (livre arbítrio) ou *julgar* os nuances das relações sociais e ponderar com esteio em valores éticos ou senso de justiça para adotar a solução mais adequada ao

---

[22] De forma diversa, o ART.20 da RGPD-EU, tem como regra geral a proibição do processamento de decisões automatizadas. E considera lícito no art.22(2) sua utilização apenas nas hipóteses elencadas e inclui de forma explicita os direitos à intervenção humana e a contestação a decisão automatizada como parte de salvaguardas em que a decisões automatizadas são permitidas.

[23] Constituição Federal 1988.

art. 5º, inciso LV, disciplina que "aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, como os meios e recursos a ela inerentes."

[24] EMENDA CONSTITUCIONAL Nº 115/2022, de 11/02/2022(...)

Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:

"Art. 5º (...)

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais

[25] Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais.

[...]

Letra "E". Considerando que a tecnologia de IA deve ser desenvolvida de forma antropocêntrica, ser digna de confiança pública e estar sempre ao serviço dos seres humanos; considerando que os sistemas de IA devem garantir que são concebidos de modo a que possam ser sempre desligados por um operador humano; Disponível: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html. Acesso. 17 mai. 2022

caso concreto.

O algoritmo que comanda o funcionamento dos mecanismos de inteligência artificial é refém da programação que lhe determina qual será a decisão *correta* de forma condicionada e adstrita a amostragem dos dados de treinamento e de dados externos a que teve acesso, que foram valorados pelo programador de seu sistema operacional (MARQUES e NUNES, 2018).

Além do que, referidas *decisões* automatizadas são valoradas por critérios não transparentes a cargo do programador e possivelmente produzidas em contextos sociais discriminatórios (*machine Bias*) e replicadas como *corretas* para o caso sob análise.

Na opinião de O'Neil(O'NEIL, 2016, p. 14) a chamada opacidade do sistema permite que os algoritmos de Inteligência Artificial operem sem transparência, sendo cognoscível apenas por especialistas e programadores computacionais. Assim, se não houver previsão legal específica de revisão humana, as *decisões* automatizadas dos algoritmos dificilmente serão submetidas a escrutínio de pessoa natural (*accountability)*, salvo quando constatado o prejuízo pelo próprio prejudicado na esfera judicial, perpetuando os vieses discriminatórios pela realimentação do sistema (*feed back*) com potencial difuso de produzir dano.

Ao se aventar que as revisões sejam procedidas apenas por sistemas autônomos, restaria prejudicada outrossim o disposto no artigo 20 da LINDB[26], que procura assegurar a transparência e participação popular nas decisões administrativas e ofensa ao Decreto 10.472/20, art. 2º inciso IV[27], que estabelece que compete a ANPD: (in verbis) "fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso".

Quanto as características do processo administrativo ou judicial, aplicáveis que devem ser igualmente aplicadas ao processo de revisão humana de decisões automatizadas, o Ministro Gilmar Mendes, no julgamento do Mandado de Segurança perante o Supremo Tribunal Federal (STF, MS 24.268/MG, rel. Min. Ellen Gracie, j. 17.09.2004 [28]) elucida os desdobramentos da garantia do art. 5º, LV, da CF/88, que englobam dentre outras considerações, que o administrado exercite direitos, dentre eles:

> [...]
> Direito de ver seus argumentos considerados (*Recht auf Beruckichtigung*), que exige do julgador a capacidade, apreensão e isenção de ânimo (*Aufnahmefähiggkeit und Aufnahmebereitschaft*) para contemplar as razões apresentadas [...].
> Sobre o direito de ver os seus argumentos contemplados pelo órgão julgador (*Recht auf Berückichtigung*), que corresponde, obviamente, ao dever do juiz ou da Administração de a eles conferir atenção (*Beachtenspflicht*), pode-se afirmar que envolve não só o dever de tomar conhecimento (*kenntnissnahmepflicht*), como também o de considerar, séria e detidamente, as razões apresentadas (*Erwägungspflicht*) [...]

Portanto, ao se desconsiderar o princípio antropocêntrico e permitir a revisão da *decisão* automatizada por outra decisão revisora automatizada, a nova *decisão* tem razoável possibilidade de estar igualmente enviesada posto que fora igualmente valorada por critérios estabelecidos pelo programador do algoritmo revisor, que ademais pode também ter sido alimentado com dados discriminatórios (machine Bias).

Assim, vislumbra-se que a exigência substantiva do art. 5, LV (em processo administrativo ou judicial), da CF/88 de que o julgador/revisor do caso tenha a capacidade, apreensão e isenção de ânimo, bem como de que leve em consideração séria e detidamente os argumentos ventilados pelo prejudicado, simplesmente não podem ser exigidos para decisões automatizadas produzidas por algoritmos de tecnologia

[26]DECRETO-LEI Nº 4.657, DE 4 DE SETEMBRO DE 1942. Disponivel: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso:17 mai 2020.
Decreto 10.474/20. ANEXO I, [...]; Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Acesso em: 19. Mai. 2022.
[28] Disponível: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=86111. Acesso: 13 Mai. 2022.

de inteligência artificial, vez que a avaliação da adequação das predições, juízo de ponderação e senso de equidade para adaptar a regra à situação do caso se caracterizam como faculdades humanas.

Estar-se-ia a ferir considerações elementares de dignidade da pessoa humana em caso de decisões automatizadas que comportem elevados riscos sociais, como as que podem implicar na detenção injusta decorrente de captura de dados biométricos para o reconhecimento facial de cidadãos, ainda que para fins de segurança pública e persecução penal.

Mormente por que as *decisõe*s automatizadas incorretas no ambiente digital podem impactar parcela significativa da população, dar ensejo à estigmatização das pessoas e outras consequências deletérias para os grupos sociais que venham a ser vítimas de eventual viés algorítmico de gênero (feminino), de etnia (mulheres negras), de classe social [29].

Além destas considerações, há uma importante função preventiva na revisão de decisões automatizadas com participação de pessoa humana ainda na esfera administrativa, especialmente quando a revisão tem por escopo frear a continuidade da lesão (por exemplo: restrição a acesso a tratamento saúde; negativa de fornecimento de medicamentos pelo SUS etc), já que se revela mais célere, econômico e razoável ao lesado se socorrer pela via administrativa do que a uma demanda judicial (assegurado no art. 22 LGPD), estar sujeito aos custos da demanda e a produção de provas em que a opacidade dos algoritmos de inteligência artificial dificultarão de sobremaneira a defesa de seu direito.

CONSIDERAÇÕES

A economia digital ao se utilizar do aparato tecnológico disponível no estado da arte promove a coleta e tratamento massivo de dados implicando na diminuição das liberdades (de expressão, de informação, de comunicação, de opinião) e da privacidade(intimidade, honra, imagem etc) do cidadão, bem como ofensa ao direito fundamental à proteção de dados pessoais e a autodeterminação informativa, com potencial caráter discriminatório decorrente no tratamento de dados pessoais sensíveis.

O direito fundamental à proteção de dados pessoais, inclusive nos meios digitais, introduzido pela Emenda Constitucional nº115/2022 à Constituição Federal de 1988, passa a integrar as cláusulas pétreas e, portanto, estão imunes a qualquer retrocesso de seu predicado normativo, além de servir de parâmetro de controle de constitucionalidade.

Compete a ANPD, a rogo da LGPD(46, §1º) estabelecer padrões técnicos mínimos, para que agentes de tratamento de dados públicos e privados compatibilizem soluções técnicas aos objetivos definidos pela entidade reguladora, voltados ao interesse da sociedade, notadamente garantir liberdade aos cidadãos e privacidade de seus dados pessoais sensíveis.

Os valores constitucionais imanentes do art. 5º, inciso LXXIX (proteção de dados pessoais, inclusive meios digitais), e inciso LV (ampla defesa, em processo judicial ou administrativo) garantem a prevalência dos direitos fundamentais e exigem o direito à participação humana sobre decisões automatizadas produzidas inteiramente por máquinas quando envolver tratamento de dados pessoais sensíveis, como os que envolvem a biometria para reconhecimento facial, sob pena de se compactuar com a erosão da autodeterminação, restrição de direitos e ofensa à dignidade humana(art, 1, III).

Como imperativo ético a tecnologia de IA deve ser desenvolvida respeitando-se o princípio antropocêntrico, revelando-se insustentável que a revisão de decisões automatizadas que lesem direitos e prejudiquem a vida das pessoas não seja acompanhada por pessoa humana natural, vez que as tecnologias de inteligência artificial não possuem habilidades para avaliar a adequação das predições, bem como senso de equidade ou juízo de ponderação para adaptar a regra

[29] Inúmeros casos têm sido relatados globalmente sobre erro de identificação, alguns com danos relevantes como o recente caso no Rio de Janeiro (julho/2019): uma mulher foi detida por engano em Copacabana e levada à delegacia do bairro, após as câmeras de reconhecimento facial darem positivo. Disponível: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 14 mai. 2022.

preexistente à situação do caso concreto, vez que opera por critérios não transparentes e valorados conforme interesse do programador e sujeitas a vieses discriminatórios.

A determinação em quais hipóteses a revisão da decisão automatizada pode ou não ser feita sem a percepção e cognição humanas devem ser reguladas de forma restritiva e tipificadas expressamente em lei, avaliando-se a pertinência da aplicação e os riscos envolvidos, devendo-se de em qualquer hipótese resguardar a dignidade humana do contexto de automação.

Diante da contaminação das liberdades pelas novas tecnologias, a sociedade deve avançar do conceito de autodeterminação informacional para a de arquitetura de precaução de danos, vez que todo processamento automatizado de dados pessoais deve desencadear ao menos a obrigação de se avaliar mediante relatórios próprios os impactos pretendidos e incidentais prováveis de processamento de dados sobre a vida das pessoas.

REFERÊNCIAS

ANSA BRASIL Agencia italiana de notícias. Disponível em: https://epocanegocios.globo.com/Mundo/noticia/2022/01/mafioso-italiano-foragido-e-preso-na-espanha-apos-aparecer-no-google-maps.html. Acesso em: 5 ja.2022.

BRANCO, Paulo Gustavo Gonet. Cláusulas pétreas. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/21/edicao-1/clausulas-petreas. Acesso: 16.Fev.2022.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em Fev. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 10 Fev. 2022.

BRASIL. Ministério da Justiça e Segurança Pública. Polícia Federal implementa nova Solução Automatizada de Identificação Biométrica. 2021. Disponível em: https://www.gov.br/pf/ptbr/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-deidentificacao-biometrica. Acesso em: 10 mai. 2022.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. Estratégia Brasileira de Inteligência Artificial -EBIA. Junho 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_documento_referencia_4-979_2021.pdf. Acesso em: 13 mai. 2022.

CÂMARA DOS DEPUTADOS. Ordem do dia. Disponível em: https://www.camara.leg.br/internet/ordemdodia/integras/2082600.htm. Acesso:13 mai. 2022.

CAMARGO, Solano de. As sanções da LGPD e o Inferno de Dante. Revista do Advogado, nº144, nov. 2019.

CAVOUKIAN, Ann. Privacy by Design - The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. 2010. Disponível:

https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/; Acesso: 17 mai. 2022.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DECRETO-LEI Nº 4.657, DE 4 DE SETEMBRO DE 1942. Disponivel: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm. Acesso:17 mai 2020.

CONSELHO EUROPEU DE PROTEÇÃO DE DADOS (EDPB). EDPB e EDPS pedem a proibição do uso de IA para reconhecimento automatizado de recursos humanos em espaços acessíveis ao público e alguns outros usos de IA que podem levar a discriminação injusta. Disponível em: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en. Acesso em: 11 mai.2022.

DAMASCENO, Victor. FERNANDES, Samuel. Sobre críticas por viés racial reconhecimento facial chega a 20 estados. Folha de São Paulo. https://www1.folha.uol.com.br/cotidiano/2021/07/sob-criticas-por-vies-racial-reconhecimento-facialchega-a-20-estados.shtml. Acesso em: 11 mai. 2022.

GLOBO.COM,-G1 Rio. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. Publicado em 11 de julho de 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 14 mai. 2022.

GOMES, Maria Cecilia Oliveira. Relatório de impacto à proteção de dados pessoais. Revista do Advogado, nº144, nov. 2019.

JOÃO, Belmiro do Nascimento. SOUZA, João Crisomar e SERRALVO, Antonio Francisco Lobo. Revisão sistemática de cidades inteligentes e internet das coisas como tópico de pesquisa. Cad. EBAPE.BR 17 (4) • Oct-Dec 2019.

LEE-MORRISON. Lila. Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face. Transcript Verlag, 2019. Ebook. Disponível em: https://www.transcriptverlag.de/978-3-8376-4846-1/portraits-of-automated-facial-recognition/. Acesso: 18 jan. 2022.

LOUREIRO, Rodrigo. Impreciso com negros, reconhecimento facial da Amazon é suspenso. Exame, publicada 11 de junho de 2020. Disponível em https://exame.com/tecnologia/impreciso-com-negros-sistema-de-reconhecimento-facial-da-amazon-e-suspenso/. Acesso em:15 mai. 2022.

LUÑO, Antonio-Henrique Perez. Perspectivas e Tendências Atuais do Estado Constitucional. Trad. José Luiz de Morais e Valéria Ribas do Nascimento. Porto Alegre, Ed. Livraria do Advogado, 2012.

LUÑO, Antonio-Henrique Perez. Generaciones de derechos humanos. In: Revista del Centro de Estudos Constitucionales, nº10, Sept, 1991.

MARCHINHACKI, Romualdo Paulo. Direitos Fundamentais: Aspectos Gerais e Históricos.

Revista da Unifebe (Online) 2012; 11 (dez):166-179. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/42974490/artigo017-with-cover-page-v2.pdf?Expires=1645447449&Signature=Yv1je47vSK6bwsR2zVRYnicPrXoVx4ySQ7HUFOT49pn5gMIr2YUM69YSxB4AgYAummUgL4cLVEWNwZg1cpaDo3yQnOyTsdzjHtzRVPyfxQEY6R-iWGf9~QUP7eu7yY3M5DVz3UFk8mdYZ~gDUwGKm4lthb2-vX76zczZm1GLlvhBxOf~FVOzQHnZWeqtVHPV668Il6QHl8jBtnKpogZbSpKWlAwJXvmizawW563u1hkIxVBEuHlPXnKMqFx5TSoFfXEoVOgIJQRoUV6QalKBA6R2lXBrIFfFLzlWOHEon3eX8amsOK-8BEb0ddPq7nJVDsQDhUhBzLfxPEiSoqgs-g__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso: 21. Fev. 2022.

MARQUES, Ana Luiza Pinto Coelho. NUNES, Dierle. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. Revista de Processo | vol. 285/2018 | p. 421 - 447 | Nov / 2018. Disponível: https://www.academia.edu/38112588/Intelig%C3%AAncia_artificial_e_direito_processual_vieses_algor%C3%ADtmicos_e_os_ricos_de_atribui%C3%A7%C3%A3o_de_fun%C3%A7%C3%A3o_decis%C3%B3ria_%C3%A0s_m%C3%A1quinas?from=cover_page. Acesso: 14 mai. 2022.

MINISTÉRIO PÚLBICO DO DISTRITO FEDERAL E TERRITÓRIOS. Foragidos da Justiça. Disponível em: https://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/programas-e-projetos-menu/foragidos-da-justica. Acesso em 11 mai.2022

MULHOLLAND, Caitlin. Inteligência Artificial e Regulação: Breves Apontamentos sobre equidade, responsabilidade e transparência. Cultura, educação e tecnologias em debate/Org. de Fernando Almeida; Gustavo Torrezan; Luciana Lima; Rosana Elisa Catelli; Realização PUC-SP; Cetic.br; NIC.br; CGI.br; Serviço Social do Comércio.– São Paulo: Sesc São Paulo, 2019. – 58 p. il. Disponível: https://webcache.googleusercontent.com/search?q=cache:ZzSpzr2g6U4J:https://centrodepesquisaeformacao.sescsp.org.br/uploads/BibliotecaTable/9c7154528b820891e2a3c20a3a49bca9/339/1605117675184351722 1.pdf+&cd=2&hl=pt-BR&ct=clnk&gl=br. Acesso: 16 mai. 2022.

O'NEIL, Cathy. Weapons of math destruction: How Big Data increases inequality democracy. New York. Crown Publisher, 2016.

ORNELAS MONTEIRO, G. (2021). Instrumentos de reconhecimento facial e os contornos da lei geral de proteção de dados ante a privacidade nas cidades (in)inteligentes. Revista De Direito E Atualidades, 1(1). Disponível em: https://www.portaldeperiodicos.idp.edu.br/rda/article/view/5220. Acesso em: 18 mai. 2022.

PARLAMENTO EUROPEU E DO CONSELHO. Regulamento Geral de Proteção de Dados EU - 2016/679. Disponível: https://dsgvo-gesetz.de/art-22-dsgvo/. Acesso: 16 mai. 2022.

PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões - Por uma necessária accountability. RIL Brasília a. 57 n. 225 p. 43-60 jan./mar. 2020. Disponível em: https://www12.senado.leg.br/ril/edicoes/57/225/ril_v57_n225_p43.pdf. Acesso: 10. Mai. 2022.

POLLO, Luiza. Cidade-berço do MIT bane reconhecimento facial; decisão tem peso simbólico. TAB-UOL, publicado em 16 de Janeiro de 2020. Disponível em; https://tab.uol.com.br/noticias/redacao/2020/01/16/cambridge-bane-reconhecimento-facial-

entenda-por-que-temos-de-pensar-nisso.htm. Acesso em: 18 mai. 2022.

PUGLIESE, Joseph. Biometrics: Bodies, Technologies, Biopolitics. New York: Routledge, 2010.

PURTOVA, Nadezhda.The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology Volume 10, 2018.Disponível: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176. Acesso: 16 mai. 2022.

QUIANG, Yang. A quarta revolução. Correio da UNESCO. Muitas vozes, um mundo. E-ISSN-2179-8818. Disponível em:https://pt.unesco.org/courier/2018-3/quarta-revolucao. Acesso em 15. Fev. 2022.

REIS, Nazareno César Moreira. Decisões automatizadas, revisão humana e direito à proteção de dados: uma análise à luz da Lei Geral de Proteção de Dados Pessoais. 2021. 157 f. Dissertação (Mestrado em Direito Constitucional) Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2021. Disponível em: https://repositorio.idp.edu.br//handle/123456789/3357. Acesso em: 7 jan. 2022.

Resolução do Parlamento Europeu, de 6 de outubro de 2021, a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais. Disponível: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html. Acesso. 17 mai. 2022.

ROLFINI, Fabiana. Boston proíbe uso de reconhecimento facial por órgãos públicos. Publicado em 25 junho de 2020, em Olhar Digital. Disponível em: https://olhardigital.com.br/2020/06/25/noticias/boston-proibe-uso-de-reconhecimento-facial-por-orgaos-publicos/. Acesso em 18 mai. 2022.

SCHAWAB, Klaus. A Quarta Revolução Industrial. Tradução: Daniel Moreira Miranda. 2016. Ed. Jair Lot Vieira e Maira Lot Vieira Micales.

SENADO FEDERAL. Projeto de Lei n° 5051, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/138790. Acesso: 13 mai. 2022.

SMICHOWSKI, Bruno Carballa. ENGELS, Barbara. HAUCAP, Justus. OLK, Christopher. SPIEKERMANN, Markus. GRAFENSTEIN, Max von. WERNICK, Alina. Data-Driven Economy: Challenges and Opportunities. Volume 54, 2019 · Number 4 · p. 200. Intereconomics Review of European Economic Policy. Disponível em: https://www.intereconomics.eu/contents/year/2019/number/4/article/data-driven-economy-challenges-and-opportunities.html. Acesso em 15.fev.2022.

SUPREMO TRIBUNAL FEDERAL- STF, MS 24.268/MG, rel. Min. Ellen Gracie, j. 17.09.2004. Disponível: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=86111. Acesso: 13 mai. 2022.

VIDOLIN, Isadora Leardini. Princípio da Precaução: Do Direito Ambiental à Proteção de Dados e Inteligência Artificial, Revista Percurso, v. 1, n. 38, 2021. Disponível: http://revista.unicuritiba.edu.br/index.php/percurso/article/view/5429. Acesso: 20. Fev. 2022.

WOLKART, Erik Navarro. Análise econômica do processo civil: como a economia, o direito e a psicologia podem vencer a tragédia da justiça. São Paulo: Revista dos Tribunais, 2019. Apresentada originalmente como tese de doutorado, Universidade do Estado do Rio de Janeiro, 2018.

ZUBOFF, Shoshana, The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power. 2019, Nova York, Public Affairs.