REVISTA MULTIDISCIPLINAR
ISSN 1809-1628
HUMANIDADES E TECNOLOGIAS (FINOM)
FACULDADE DO NOROESTE DE MINAS

INTELIGÊNCIA ARTIFICIAL E PROTEÇÃO DE DADOS: SOBRE A AUDODETERMINAÇÃO INFORMATIVA E A MANIPULAÇÃO INFORMACIONAL POR *MACHINE LEARNING*

ARTIFICIAL INTELLIGENCE AND DATA PROTECTION: ABOUT INFORMATIVE AUDODETERMINATION AND INFORMATIONAL MANIPULATION BY MACHINE LEARNING

Bruna Pinotti Garcia Oliveira[1]

Resumo: A proteção de dados vem sendo regulamentada no campo do direito internacional dos direitos humanos e, em meio aos debates que cercam este objeto regulatório, surgem discussões a respeito dos limites jurídicos da inteligência artificial. Neste sentido, a inteligência artificial se realiza por meio de *softwares* programados com algoritmos de aprendizado – a denominada tecnologia de *machine learning* – e da alimentação destes com dados. Com o objetivo de apresentar o estado da arte deste debate, este artigo se desenvolve pelo método doutrinário-analítico, partindo do estudo da economia de dados e da autodeterminação informacional enquanto pressupostos condutores, passando pela compreensão da relação entre inteligência artificial e proteção de dados e finalizando com o estudo do cenário regulatório no direito internacional dos direitos humanos.

Palavras-chave: Direito eletrônico; direito internacional dos direitos humanos; tecnologia da informação; proteção de dados; inteligência artificial.

Abstract: Data protection has been regulated in the field of international human rights law and, in the midst of debates surrounding this regulatory object, discussions have arisen regarding the legal limits of artificial intelligence. In this sense, an artificial intelligence performs by means of software programmed with learning algorithms - called machine learning - and with the feeding of this with data. In order to present the state of the art of this debate, this article develops by the doctrinal-analytical method, starting from the study of data economics and informational self-determination as guiding assumptions, going through the understanding of the relationship between artificial intelligence and data protection and ending with the study of the regulatory scenario in international human rights law.

[1] Doutora em Direito pela Universidade de Brasília (UnB). Mestre-bolsista (CAPES/PROSUP) em Direito pelo UNIVEM. Professora adjunta da Universidade Federal da Goiás – Unidade Acadêmica Especial de Ciências Sociais Aplicadas (UFG-UAECSA). Professora de cursos preparatórios para concursos e pós-graduação. Advogada e consultora jurídica, inscrita na OAB/GO sob o nº 48.875. E-mail: brunapinotti@ufg.br

Recebido em 10/06/2020
Aprovado em 15/07/2020

Key Words: Electronic law; international human rights law; technology of information; data protection; artificial intelligence.

INTRODUÇÃO

A preocupação com a inteligência artificial parecia algo mais ficcional do que real por muitos anos. É fácil recordar os filmes e livros que descreviam robôs que se assemelhavam à figura humana e os conflitos éticos que se desenhavam neste cenário. Atualmente, a inteligência artificial faz parte do cotidiano, mas não propriamente da forma como se idealizou nas obras de ficção. Não surgiram os robôs humanoides, mas foram criados *softwares* com capacidade de aprender a partir dos dados que são nele inseridos. Estes *softwares* são movidos por algoritmos inteligentes, capazes de se reinventarem e aprenderem a partir do comportamento humano – a tecnologia se denomina *machine learning*, do inglês, "aprendizado de máquina".

O objetivo geral deste artigo é apresentar o estado da arte do tema inteligência artificial no contexto das regulamentações de proteção de dados, especialmente no campo do direito internacional dos direitos humanos. A pesquisa se desenvolve com procedimentos técnicos bibliográfico e documental e utilizando um método doutrinário-analítico.

Neste sentido, parte-se de uma contextualização teórica do leitor quanto ao cenário do uso e da monetização de dados pessoais, desenhando uma proteção normativa em relação aos mesmos. Após aborda-se a relação entre inteligência artificial e proteção de dados, tanto observando os dados como a força-motriz que viabiliza a inteligência artificial, quanto destacando a proteção de dados como instrumento para a imposição de limites éticos e jurídicos aos recursos da inteligência artificial. Ao final, desenha-se o cenário da proteção de dados e da inteligência artificial no campo do direito internacional dos direitos humanos, desde o sistema da ONU até os sistemas regionais americano, africano e europeu.

1 ECONOMIA DE DADOS E AUTODETERMINAÇÃO INFORMATIVA

O dado reflete o estado primitivo da informação, no sentido de que um dado digital, por si só, não agrega conhecimento. Os dados são fatos brutos que ao serem processados e organizados podem se converter em algo inteligível, fornecendo uma informação[2]. Existe uma relação direta entre dado e informação, a partir do momento em que a segunda é um reflexo do

[2] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense/GEN, 2019, p. 36-37.

processamento do primeiro. Quando se está diante da regulação da proteção de dados, na verdade, se está falando da proteção da informação. Por isso, diante de dados desprotegidos, abre-se brecha para a manipulação de informação, em especial pelos algoritmos inteligentes.

Na economia de dados, a informação desperta um interesse econômico, permitindo que aquele que adquiriu o dado tenha informações do perfil de consumo do utilizador de uma plataforma e as utilize para direcionar um padrão de comportamento. A propósito, estas plataformas usualmente não cobram valores dos usuários e funcionam com base no *zero-price advertisement business model*, onde um negócio toma a aparência de gratuito, mas esconde os sujeitos necessários para a sua operacionalização, os quais compõem uma intrincada rede de atores comprometida a atuar em colaboração para a entrega de publicidade direcionada pelos padrões comportamentais dos usuários e gerada a partir de algoritmos de aprendizado – na prática, há uma troca dos dados pessoais pelo serviço ou produto, ou seja, o consumidor paga com seus dados pelo que é aparentemente oferecido gratuitamente nas plataformas[3].

> O mercado de dados em geral cresce a partir da difusão de visões como a de que o modelo de negócios é justo, já que os usuários receberiam contrapartidas adequadas pelos seus dados, ou mesmo necessário, dado que haveria um verdadeiro *trade off* entre inovação e privacidade, de maneira que a violação desta última seria o preço a pagar ou o mal necessário para o progresso tecnológico e os novos ser viços que daí decorrem. Até a forma como a questão é apresentada já reflete a perspectiva utilitarista que permeia a análise, pois se parte da premissa de que, em nome da inovação, é justificável o sacrifício de direitos fundamentais elementares. O excesso de otimismo das próprias pessoas em relação a muitos dos modelos de negócios da economia digital e os benefícios diretos que eles lhes proporcionam, aliado às próprias dificuldades de compreensão dos seus efetivos impactos, são também fatores que criam ônus adicionais para os reguladores que, premidos entre a assimetria informacional e os benefícios das inovações, muitas vezes, não sabem o que fazer para conter esse processo e proteger minimamente os cidadãos. Foi esse o cenário que possibilitou que vários desses negócios evoluíssem em um ambiente no qual o suposto vácuo regulatório fosse convenientemente preenchido pela autorregulação criada pelos agentes em seu próprio benefício[4].

Não obstante, a informação extraída dos dados pode despertar outros interesses para além do econômico, como os políticos. Recentemente, o escândalo envolvendo a Cambridge Analytica, uma empresa privada de análise de dados e comunicação estratégica, e o Facebook

[3] Ibid., p. 26-33.
[4] FRAZÃO, Ana. **Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 23-52, p. 30-31.

trouxe à tona as possibilidades multifacetadas da manipulação dos dados em prol de uma determinada pauta, minando o poder de decisão individual por meio do controle e da manipulação da informação[5]. A verificação de padrões comportamentais de usuários no que se refere às suas opiniões políticas, econômicas e religiosas para conduzir o discurso político de um ou outro candidato rumo à vitória nas eleições demonstra que sem a proteção de dados o risco de abuso do poder econômico é pequeno se comparado a outros riscos que estão em jogo com a manipulação informacional, como o risco ao processo democrático.

Para controle destes riscos, parece que não basta garantir ao utilizador das plataformas o conhecimento de que seus dados estão sujeitos a coleta, armazenamento e compartilhamento, nem permitir que ele conheça os dados a seu respeito que estão armazenados – o que se denomina "Direito de Saber". É preciso ir além, permitindo que o usuário de fato decida a respeito dos dados de que é titular, exercendo o "Direito de Decidir".

O "Direito de Decidir" consiste na possibilidade de deliberar a respeito da utilização dos dados e, ao fazê-lo, garantir que a informação chegue sem manipulação pelas plataformas utilizadas, viabilizando a formação da opinião sem influências indevidas e permitindo que se tome uma decisão apenas pelo exercício da autonomia individual, não pela condução do padrão comportamental por intermédio da inteligência artificial. Considerando que a autodeterminação é um ato ou efeito de decidir por si, tem-se que a autodeterminação informativa corresponde aos aspectos decisórios no exercício da autonomia individual em relação à informação.

Essencialmente, a autodeterminação informacional é vista como um aspecto inerente ao direito de personalidade. Em 1983, a Suprema Corte alemã reconheceu explicitamente este direito como uma expressão do direito fundamental ao livre desenvolvimento da personalidade. A base de tal direito não está somente na Constituição alemã, mas repousa no direito internacional dos direitos humanos e, especialmente, no artigo 22 da Declaração Universal dos Direitos Humanos de 1948, segundo o qual toda pessoa tem direito ao livre desenvolvimento de sua personalidade, e no Pacto Internacional dos Direitos Econômicos, Sociais e Culturais, que garante o direito à educação e à participação na esfera pública[6].

A decisão do Tribunal Alemão se referiu à "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" (1977), julgando-a inconstitucional e radicalizando o conceito

[5] SILVEIRA, Alessandra; FROUFE, Pedro. **Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos**. UNIO – EU Law Journal, v. 4, n. 2, jul. 2018, p. 4-20, p. 12.

[6] BELLI, Luca. **Network Self-Determination and the Positive Externalities of Community Networks**. In: Community Networks: the Internet by the People, for the People. Rio de Janeiro: FGV Direito Rio, 2017, p. 35-64.

de livre controle do indivíduo sobre o fluxo de suas informações. A sentença reconheceu a existência de um direito à "autodeterminação informativa" e colocou o indivíduo como protagonista do processo de tratamento de seus dados. De tal modo, haveria um núcleo essencial inerente à proteção de dados, consistente na autodeterminação informativa, o qual não poderia ser violado pelo legislador na elaboração de outras normas[7].

A lei determinava a realização de um censo que deveria se finalizar em 1983, sobrevindo em 1982 a sua regulamentação, onde se fixava um rol de 160 perguntas a serem respondidas pelos recenseados que posteriormente seriam submetidas a tratamento informatizado, impondo multa a quem se recusasse a responder as perguntas. A preocupação que surgiu era de que o governo poderia se valer dos dados para realizar um controle capilar das atividades e da condição pessoal dos cidadãos[8].

A sentença da Corte reconheceu a necessidade de se observar o princípio da finalidade na coleta de dados pessoais e desmistificou a noção de que o tratamento de certos tipos de dados pessoais seria irrelevante para a privacidade, de modo que reconheceu que um dado aparentemente insignificante, conforme a finalidade para o qual foi coletado, poderia ser utilizado indevidamente. Não obstante, conceituou a autodeterminação informativa como o direito dos indivíduos de "decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados"[9].

> A Corte afirmou que o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação de modo a formar um retrato completo da pessoa, sem a sua participação ou conhecimento. Nesse contexto, argumentou que a Constituição alemã protege o indivíduo contra o indevido tratamento de dados pessoais, por meio do direito fundamental ao livre desenvolvimento da personalidade, segundo o qual o indivíduo tem o poder para determinar o fluxo de suas informações na sociedade[10].

A partir da sentença, foi aprovada na Alemanha uma nova lei corrigindo os pontos contestados, promulgada em 1985 para um censo realizado em 1987, no qual os dados para fins estatísticos passaram a ser separados das informações individuais, o cidadão passou a ser

[7] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental**. Brasília: IDP, 2019. (Edição do Kindle), p. 520-550.
[8] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2019. (E-book), p. RB-2.8.
[9] Ibid., p. RB-2.8.
[10] MENDES, Op. Cit., p. 544.

informado cuidadosamente a respeito das finalidades da coleta das informações, foi vetada a transferência de dados pessoais entre autoridades federais e regionais. Até hoje, o direito à autodeterminação informativa orienta a proteção de dados pessoais na Alemanha e exerce grande influência em países do sistema jurídico romano-germânico[11]. Exemplo disso é o próprio Brasil, que reconheceu como um de seus fundamentos na Lei Geral de Proteção de Dados a autodeterminação informativa, conforme artigo 2º, II[12].

Logo, desde a década de 1980, o direito à autodeterminação informacional tem sido como pedra de toque da proteção de dados pessoais, inclusive sendo assim reconhecido pela Suprema Corte alemã – o poder do indivíduo de deliberar sobre a divulgação de seus dados pessoais, escolhendo a quem serão divulgados e com quais finalidades pode ser usado. A transformação dos modos de coleta e processamento de dados pessoais com a informatização se apresenta como um desafio ao direito à autodeterminação informacional[13].

Os dados são a fonte da maioria dos serviços prestados pela internet e, de tal modo, parece ser cada dia mais distante uma separação entre a proteção de dados e o acesso à internet, por diversos motivos: primeiramente, devido à estrutura da economia de dados, que atribui valor ao dado e, ofertando serviços aparentemente gratuitos, é por meio dele remunerado; em segundo lugar, porque muitos usuários não têm noção do valor de seus dados pessoais e não estão cientes das implicações da coleta e do processamento de seus dados[14].

Com efeito, a autodeterminação informacional é um direito multifacetado que traduz o atual estágio do direito de informação, como se pretende delinear daqui em diante. Há que se destacar concepções mais restritas do direito à autodeterminação informacional, como detalhou Bruno Ricardo Bioni[15] em dissertação apresentada à Universidade de São Paulo – segundo estas, a autodeterminação informacional se centra no consentimento informado, o qual é a técnica que viabiliza que o indivíduo autodetermine suas informações pessoais. Acredita-se que, de fato, o consentimento informado é um aspecto essencial da autodeterminação informacional, mas que outras nuances detectadas nas normativas de proteção de dados também se relacionam a ela, notadamente as que se referem ao poder do indivíduo de deliberar a respeito

[11] DONEDA, Op. Cit., p. RB-2.8.
[12] BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei n. 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: 12 fev. 2020.
[13] BELLI, Op. Cit., p. 42-46.
[14] Ibid., p. 42-46.
[15] BIONI, Op. Cit., p. XXV-XXVII.

de seus dados, como é o caso das que se voltam diretamente à manipulação informacional, atentando de forma direta contra a autodeterminação pelo uso de algoritmos inteligentes.

2 INTELIGÊNCIA ARTIFICIAL, *MACHINE LEARNING* E PROTEÇÃO DE DADOS

Os debates mais recentes a respeito da autodeterminação informacional na internet centram-se na preocupação com a credibilidade da informação que chega aos usuários, a partir do momento em que a coleta de dados permite a manipulação dos mesmos por intermédio do controle dos fluxos informacionais e contra a neutralidade de rede, como ocorre devido ao uso de algoritmos, que são procedimentos eletrônicos que permitem filtrar a partir dos dados da rede os conteúdos direcionáveis a um usuário.

O professor de ciências da computação Pedro Domingos[16], na obra "O Algoritmo Mestre", descreve a evolução dos algoritmos para adotarem a configuração atual, denominada de *machine learning* ou algoritmo de aprendizado. Basicamente, nas origens dos sistemas de computação, os algoritmos precisavam ser programados para desempenharem determinada tarefa e deviam ser descritos minunciosamente. Com o *Big Data*, tornou-se possível que o algoritmo desenvolvesse a si mesmo, dispensando programação específica e, na verdade, o próprio *Big Data* ganhou valor e utilidade por conta dos algoritmos. Noutras palavras, o algoritmo de aprendizado – que opera de forma predominante na rede mundial de computadores e na Web 2.0 – descobrem tudo sozinhos e programam a si mesmos a partir dos dados que estão disponíveis on-line. Paulatinamente, o *machine learning*, a tecnologia que constrói a si mesma, está recriando a ciência, a tecnologia, os negócios, a política e a guerra.

> Vivemos na era dos algoritmos. Há apenas uma ou duas gerações, a simples menção da palavra algoritmo não significava nada para a maioria das pessoas. Atualmente, os algoritmos integram tudo que se faz no mundo civilizado. Eles fazem parte da trama que compõe nossa vida diária. Não estão apenas nos celulares ou laptops, mas nos carros, em nossa casa, nos utensílios domésticos e em brinquedos. [...] Um algoritmo é uma sequência de instruções que informa ao computador o que ele deve fazer. Os computadores são compostos por bilhões de minúsculas chaves chamadas transistores, e os algoritmos ligam e desligam essas chaves bilhões de vezes por segundo. [...] Todo algoritmo tem uma entrada e uma saída: os dados entram no computador, o algoritmo faz o que precisa com eles, e um resultado é produzido. O *machine learning* faz o contrário: entram os dados e o resultado desejado, e é produzido o algoritmo que transforma um no outro. Os algoritmos de aprendizado – também conhecidos como aprendizes – são aqueles que criam outros

[16] DOMINGOS, Pedro. **O Algoritmo Mestre: como a busca pelo algoritmo de *machine learning* definitivo recriará nosso mundo**. São Paulo: Novatec, 2017, p. 130-180. (Edição do Kindle)

> algoritmos. Com o *machine learning*, os computadores escrevem seus próprios programas, logo não precisamos mais fazê-lo[17].

A aprendizagem de máquina ou *machine learning* gera o aperfeiçoamento dos algoritmos por inteligência artificial, de forma obscura. Os algoritmos aprendem com seus próprios erros e se aprimoram e, "como não é possível entender completamente esse processo, diante da sua complexidade e multiplicidade de passos ou etapas, fala-se até mesmo na chamada 'eficácia irracional dos dados'"[18].

Existem diferentes tipos de algoritmos de aprendizagem, mas Pedro Domingos[19] acredita que é possível a criação de um algoritmo mestre, que substitua os diferentes tipos de algoritmos e possa derivar todo o conhecimento existente no mundo, presente, futuro e passado. Este algoritmo mestre ainda está distante da realidade, mas os algoritmos de aprendizado estão cada vez mais avançados. Essencialmente, estes algoritmos de *machine learning* trabalham com o reconhecimento e a modelagem de padrões, compondo uma subárea da inteligência artificial.

Em tal cenário, os algoritmos de aprendizagem processam os dados de cada usuário da internet e direcionam suas escolhas – seja para apresentar interesses de compra ou para sugerir músicas e filmes que seriam interessantes, ou mesmo para apontar vínculos de amizades e relacionamentos que parecem adequados. A escolha última é individual, mas 99,9% do que ocorreu antes das opções de escolha serem apresentadas foi feito por algoritmos. Na prática, a sensação de escolha corresponde a 0,1% do processo de decisão[20].

Sendo assim, parece razoável a preocupação de que o tratamento de dados corrompa com as características essenciais da informação, a integridade e a exatidão. Em razão disso, as normativas que endereçam a proteção de dados incorporam princípios sobre a preservação da informação íntegra e exata, como se denota no preâmbulo do RGPD, em seu § 49, tal como do artigo 5º da norma, que enuncia os princípios que devem reger a proteção de dados, dentre eles a exatidão (artigo 5º, § 1º, "d") e a integridade (artigo 5º, § 1º, "f"). Neste sentido, os dados devem ser "exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora" – nos termos do princípio da exatidão – e "tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as

[17] Ibid., p. 316-405.
[18] FRAZÃO, Op. Cit., p. 39.
[19] DOMINGOS, Op. Cit., p. 180-500.
[20] Ibid., p. 510-520.

medidas técnicas ou organizativas adequadas" – nos moldes do princípio da integridade[21]. No Brasil, o artigo 6º, V, LGPD traz o princípio da qualidade dos dados, segundo o qual deve ser conferida "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento"[22].

Não obstante, o RGPD reflete no seu preâmbulo uma preocupação geral com o uso da manipulação algorítmica para fins discriminatórios, considerando a possibilidade de que o tratamento automatizado de dados para a definição de perfis de usuários ocorra de forma discriminatória ou de maneira a sujeitar o ser humano unicamente à decisão de uma máquina:

> 71. O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrônica ou práticas de recrutamento eletrônico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança[23].

A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os

[21] UE – UNIÃO EUROPEIA. **RGPD – Regulamento Geral de Proteção de Dados**. Regulamento n. 679/2016. Disponível em: https://eur-lex.europa.eu/. Acesso em: 13 fev. 2020.
[22] BRASIL, LGPD, 2018, Op. Cit.
[23] UE, RGPD, 2016, Op. Cit.

dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos.

Basicamente, os algoritmos permitem que seja definido um perfil do usuário, tanto que esta técnica de criar um arcabouço de dados que definam aspectos do usuário é conhecido como *profiling*. São acuradas as preocupações de que o *profiling* se torne uma forma de selecionar e discriminar usuários, conforme exposto por Mendes[24], Frazão[25] e Doneda[26]. De acordo com o que descreve o último destes autores, o *profiling* cria uma espécie de "avatar", ou seja, de representação virtual de um usuário, com o auxílio de métodos estatísticos e de técnicas de inteligência artificial. Tal perfil é composto por aspectos que cada vez mais são o principal fator levado em conta na avaliação de uma concessão de crédito, na aprovação de um plano de saúde, na obtenção de um emprego, na passagem pela migração em um país estrangeiro, entre tantos outros casos[27].

> Um perfil assim obtido pode se transformar numa verdadeira representação virtual da pessoa, e pode ser o seu único aspecto visível a outros sujeitos que com ela terão algum tipo de interação. Este perfil estaria, em diversas circunstâncias, fadado a confundir-se com a própria pessoa. A partir do momento em que um perfil eletrônico é a única parte da personalidade de uma pessoa visível a outrem, as técnicas de previsão de padrões de comportamento podem levar a uma diminuição de sua esfera de liberdade, visto que vários entes com os quais ela se relaciona partem do pressuposto que ela adotaria um comportamento predefinido, tendo como consequência uma potencial diminuição de sua liberdade de escolha visto que muitas de suas possibilidades podem ser pré-formatadas em função destas ilações[28].

Notoriamente, o *profiling* se aproveita e se baseia nos chamados dados sensíveis, que são "determinados tipos de informação que, caso sejam conhecidas e submetidas a tratamento,

[24] MENDES, Op. Cit.
[25] FRAZÃO, Op. Cit., p. 32.
[26] DONEDA, Op. Cit., p. RB-1.1.
[27] Ibid., p. RB-1.1.
[28] Ibid., p. RB-2.6.

podem se prestar a uma potencial utilização discriminatória", sendo que "entre estes dados, tidos como sensíveis, estariam as informações sobre raça, credo político ou religioso, opções sexuais, histórico médico ou dados genéticos de um indivíduo"[29]. Fato é que informações oriundas de bases de dados podem ser extraídas e utilizadas de forma discriminatória, o que justifica "tutela mais rígida em caso de tratamento de dados sensíveis e de situações potencialmente discriminatórias"[30]. Por isso, a decisão e definição de perfis automatizada baseada em categorias especiais de dados sensíveis só deverá ser permitida em condições específicas, conforme reforça Frazão[31]:

> Os algoritmos estão hoje sendo programados para a extração de padrões e inferências a partir dos quais serão tomadas, de forma automatizada, decisões sobre questões objetivas, mas que estão atreladas a importantes dados sensíveis, assim como decisões sobre questões subjetivas e que envolvem complexos juízos de valor, tais como (i) avaliar as características, a personalidade, as inclinações e as propensões de uma pessoa, inclusive no que diz respeito à sua orientação sexual; (ii) analisar o estado de ânimo ou de atenção de uma pessoa; (iii) identificar estados emocionais, pensamentos, intenções e mesmo mentiras; (iv) detectar a capacidade e a habilidade para determinados empregos ou funções; (v) analisar a propensão à criminalidade; (vi) antever sinais de doenças, inclusive depressão, episódios de mania e outros distúrbios, mesmo antes da manifestação de qualquer sintoma.

Há limites ao *machine learning*, de tal modo que se sustenta a afirmação de Silveira e Froufe[32] no sentido de que "a aprendizagem automática não passa de uma tecnologia – e, portanto, o que importa é o que decidimos fazer com ela e como regular a sua utilização". Entretanto, parece haver um abismo entre o reconhecimento da necessidade de regular a manipulação algorítmica da informação e o encontro de uma solução regulatória adequada que preserve as características essenciais do ciberespaço. Em meio a posicionamentos que oscilam entre extremos, cabe lembrar que "a chave para manejar as consequências éticas e morais da tecnologia enquanto a alimentação da economia cresce é regular o uso da tecnologia sem banir ou restringir a sua criação"[33] (tradução nossa).

[29] Ibid., p. RB-2.3.
[30] MENDES, Op. Cit., p. 626.
[31] FRAZÃO, Op. Cit., p. 32.
[32] SILVEIRA; FROUFE, Op. Cit., p. 11.
[33] ABELSON, Hal; LEDEEN, Ken; LEWIS, Harry. **Blown to bits**: your life, liberty and happiness after the digital explosion. Crawfordsville (Indiana/USA): Addison-Wesley, 2008. No original: "The key to managing the ethical and moral consequences of technology while nourishing economic growth is to *regulate the use* of technology without *banning or restricting its creation*".

Por sua vez, episódios recentes mostram que as possibilidades de que a manipulação algorítmica afete de forma severa e direta direitos humanos são mais vastas que o imaginado, mesmo após a eclosão do caso Snowden. Prova disso está no caso da Cambridge Analytica, empresa especializada em tratamento de dados que trabalhou junto à campanha vitoriosa de Donald Trump à presidência dos Estados Unidos em 2016, tomando por base os dados dos usuários do Facebook para a definição de perfis políticos e a delimitação de público-alvo da campanha presidencial, a partir de onde deliberava, inclusive, a respeito dos rumores e das notícias falsas – as chamadas *fake news* – que gerariam resultados positivos à campanha.

Apesar do escândalo, até hoje, o Facebook é evasivo a respeito de sua relação com a Cambridge Analytica, que encerrou suas atividades. Nas audiências diante do Congresso Americano sobre o episódio, Mark Zuckerberg, CEO do Facebook, respondeu de forma genérica aos questionamentos que lhe foram direcionados e negou conhecimento a respeito da operacionalização da Cambridge Analytica, mas foi consistente na pauta de direitos e deveres dos usuários, afirmando que a privacidade é de responsabilidade de cada indivíduo e que, se uma pessoa insere informações na internet, deve ter ciência que serão utilizadas[34].

Há que se destacar que não foi a primeira vez que o *machine learning* foi utilizado para alcançar sucesso em campanhas presidenciais. Em 2012, o presidente Obama contratou Rayid Ghani, um especialista em *machine learning*, como cientista-chefe de sua campanha, que deu início ao que seria, até então, a maior operação de análise de dados da história da política[35]. O cerne do escândalo da Cambridge Analytica não parece estar no uso de algoritmo inteligente para a delimitação do perfil do eleitorado, mas sim nos limites do que pode ser feito com a informação obtida a partir dele e, especialmente, dos recursos que a internet possibilita para transformar a informação útil de um potencial eleitor num voto – claramente, as *fake news* ultrapassam todos estes limites e jamais se saberá ao certo o impacto que tiveram no processo democrático norte-americano nas eleições de 2016, ou mesmo no processo democrático de outros países nos anos que se seguiram. O que as *fake news* mostram é que o algoritmo não é capaz de processar se uma informação é ou não acurada, se deve ou não ser propagada, mas apenas de definir se aquela informação, verdadeira ou falsa, é interessante para o anunciante.

> O exemplo das notícias falsas é elucidativo. O algoritmo do Facebook tem por objetivo maximizar o envolvimento do internauta – quer que as pessoas leiam

[34] WATSON, Chloe. **The key moments from Mark Zuckerberg's testimony to Congress**. The Guardian, 11 abr. 2018. Disponível em: https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments. Acesso em: 18 fev. 2020.
[35] DOMINGOS, Op. Cit., p. 600.

> as *fake news* porque é assim que lhes pode mostrar mais anúncios. Não interessa ao algoritmo se as notícias são verdadeiras ou falsas, boas ou más. De resto, como as notícias falsas são as mais escandalosas, são também aquelas que mais chamam a atenção dos internautas. Em última análise, os algoritmos de aprendizagem são estúpidos – como explica Pedro Domingos – , pois falta-lhes, pelo menos por enquanto, senso comum e ética, que são características humanas, como também a empatia e a criatividade[36].

Com a internet, a informação perdeu uma de suas principais características, a autenticidade, inviabilizada tecnicamente pelo intenso e sem precedentes fluxo informacional. Contudo, para além da impossibilidade técnica, é preciso indicar que procedimentos de checagem podem conduzir a internet a uma burocracia irreversível, gerar censura e atentar contra o seu próprio propósito informacional. Neste cenário, o direito internacional dos direitos humanos pouco a pouco cria diretrizes para a proteção de dados no contexto da inteligência artificial.

3 INTELIGÊNCIA ARTIFICIAL E PROTEÇÃO DE DADOS NO DIREITO INTERNACIONAL DOS DIREITOS HUMANOS

Aos poucos, a **Organização das Nações Unidas – ONU** tem percebido que a questão dos dados não mais se relaciona apenas ao aspecto da privacidade, tal como vinha desenhando nas primeiras normas sobre proteção de dados, e que a internet impactou nos modos de vida social, não bastando garantir uma proteção passiva dos usuários da rede e apoiando o reconhecimento do direito de decidirem, na medida do possível, sobre seus dados. Neste sentido, destaca-se o Relatório sobre a Economia Digital de 2019, que reconheceu o valor econômico dos dados e os tratou como bem público a ser compartilhado por toda humanidade[37].

Na Resolução n. 32/13 do Conselho de Direitos Humanos sobre a "promoção, proteção e fruição de direitos humanos na *Internet*", muitas afirmações se direcionam para além da necessidade de proteção dos dados mediante segurança digital como corolário do direito à privacidade, por exemplo, abordando que a permanência da internet como global, aberta e interoperável, essencial não apenas à privacidade, mas também à liberdade[38].

[36] SILVEIRA; FROUFE, Op. Cit., p. 12.
[37] ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Digital Economy Report 2019: Overview**. Geneva: United Nations, 2019. Disponível em: https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf. Acesso em: 08 fev. 2020, p. 1-12.
[38] Id., Conselho de Direitos Humanos. **The promotion, protection and enjoyment of human rights on the Internet**. Resolução n. 32/13 do Conselho de Direitos Humanos, 18 de julho de 2016. Disponível em: http://search.un.org/. Acesso em: 25 ago. 2018.

Especificamente sobre a autodeterminação informacional, a ONU não fez menção expressa, mas é importante salientar que ela reconheceu a existência de um direito de autodeterminação individual, que deriva do direito à autodeterminação dos povos. Neste sentido, a Assembleia Geral tem emitido declarações sobre a realização universal do direito dos povos à autodeterminação, a última delas publicada em 21 de janeiro de 2020[39]. Já os elementos deste direito à autodeterminação informacional têm se desenhado no sistema internacional de proteção aos direitos humanos, dentre eles o direito à não manipulação da informação.

A propósito, na Resolução n. 73/179, adotada em 17 de dezembro de 2018 pela Assembleia Geral da ONU sobre "o direito à privacidade na era digital", última de uma série de resoluções sobre a temática tanto da Assembleia Geral quanto do Conselho de Direitos Humanos, refletindo o ideário das Relatorias sobre o Direito à Privacidade e sobre a Liberdade de Opinião e de Expressão, assevera-se a importância dos direitos à privacidade e ao acesso à informação no contexto das TICs e expressa-se preocupação especial com relação aos elementos do direito à autodeterminação informacional, ainda no preâmbulo:

> Expressando preocupação de que os indivíduos geralmente *não fornecem e/ou não podem fornecer seu consentimento livre, explícito e informado* para a venda ou revenda múltipla de seus dados pessoais, uma vez que a coleta, o processamento, o uso, o armazenamento e o compartilhamento de dados pessoais, incluindo dados confidenciais, aumentou significativamente na era digital;
> Observando com preocupação que a *delimitação de perfil digital, as tecnologias automatizadas de tomada de decisão e de algoritmos de aprendizado*, às vezes referidas como inteligência artificial, sem salvaguardas adequadas, podem levar a decisões com potencial de afetar o gozo dos direitos humanos, incluindo direitos econômicos, sociais e culturais, e reconhecendo a *necessidade de aplicar o direito internacional de direitos humanos no desenho, na avaliação e na regulamentação dessas práticas;*
> Enfatizando que a vigilância ilegal ou arbitrária e/ou a intercepção de comunicações, bem como a coleta ilegal ou arbitrária de dados pessoais, como atos altamente intrusivos, violam o direito à privacidade, podem interferir no direito à liberdade de expressão e contradizer os princípios de uma sociedade democrática, inclusive quando realizada de maneira extraterritorial ou em massa;
> Reconhecendo que os mesmos direitos que as pessoas têm off-line também devem ser protegidos on-line, incluindo o direito à privacidade; [...]
> Expressando *preocupação com a disseminação da desinformação e propaganda*, inclusive na internet, que pode ser projetada e implementada de modo a *enganar, violar os direitos humanos*, incluindo o direito à privacidade e à liberdade de expressão, e incitar a violência, o ódio, a discriminação ou a

[39] Id. **Right of peoples to self-determination**. Resolução adotada pela Assembleia Geral em 18 de dezembro de 2019. Disponível em: https://documents-dds-ny.un.org/. Acesso em: 18 fev. 2020.

> hostilidade, e enfatiza a importante contribuição dos jornalistas para combater essa tendência; [...][40] (Tradução e grifos nossos)

A manifestação da ONU vem centrada no direito à privacidade, mas traz dois dos elementos que representam o atual momento do direito de informação: primeiro, menciona-se a necessidade do consentimento livre, explícito e informado do titular dos dados; após, manifesta-se a preocupação com a integridade e a veracidade informacional, afirmando limites da manipulação algorítmica e destacando uma preocupação com a propagação de informação falsa.

Também no cenário internacional, destacam-se movimentos da União Internacional das Telecomunicações – UIT, agência especializada da ONU, e da Cúpula Mundial sobre a Sociedade da Informação, iniciativa intermediada pela UIT com participação de diversos atores, públicos e privados (modelo *multistakeholder*). A Cúpula deliberou pela constituição do Fórum sobre Governança na Internet – IGF[41], evento periódico no âmbito do qual se elaborou a Carta de Direitos Humanos e Princípios para a Internet, cuja primeira versão foi lançada em 2010, com o propósito de construir uma sociedade da informação centrada na pessoa humana, com respeito aos direitos tradicionalmente reconhecidos na Declaração Universal dos Direitos Humanos, englobando aspectos relacionados à proteção de dados e à inteligência artificial.

---

[40] Id. **The right to privacy in the digital age**. Resolução adotada pela Assembleia Geral em 17 de dezembro de 2018. Disponível em: https://documents-dds-ny.un.org/. Acesso em: 18 fev. 2020. No original: "Expressing concern that individuals often do not and/or cannot provide their free, explicit and informed consent to the sale or multiple resale of their personal data, as the collecting, processing, use, storage and sharing of personal data, including sensitive data, have increased significantly in the digital age;
Noting with concern that profiling, automated decision-making and machine learning technologies, sometimes referred to as artificial intelligence, without proper safeguards, may lead to decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights, and recognizing the need to apply international human rights law in the design, evaluation and regulation of these practices;
Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale;
Recognizing that the same rights that people have offline must also be protected online, including the right to privacy; [...]
Expressing concern about the spread of disinformation and propaganda, including on the Internet, which can be designed and implemented so as to mislead, to violate human rights, including the right to privacy and to freedom of expression, and to incite violence, hatred, discrimination or hostility, and emphasizes the important contribution of journalists in countering this trend; [...]".

[41] Thiago Luís Santos Sombra (**Direito à privacidade e proteção de dados no ciberespaço: a *accountability* como fundamento da *lex privacy***. 2019. 219 f. Tese (Doutorado em Direito) – Universidade de Brasília, Brasília, 2019, p. 40) aponta que o IGF, apesar de ter se tornado uma arena de expressiva troca de experiências entre os *stakeholders*, não tem influenciado com efetividade os atores estatais, de modo que os Estados têm optado por restringir a regulação privada ao conferir efeitos extraterritoriais às suas leis ou adotar mecanismos de *data localization* com o intuito de assegurar que empresas estejam ao alcance das autoridades estatais de fiscalização e controle.

A Carta aborda no oitavo ponto o "direito à privacidade na internet", garantindo-se a toda pessoa o direito de proteção à sua privacidade e aos seus dados pessoais; a clareza nas políticas e configurações de privacidade para que a pessoa possa se proteger de violações a seus direitos; a proteção da personalidade virtual (relacionada com prerrogativas de apagamento e esquecimento que surgem nas normas de proteção de dados); direito ao anonimato e à criptografia; proteção contra a vigilância e contra a difamação. Ainda, a Carta endereça no ponto nove o "direito à proteção de dados digitais", assegurando universalmente a proteção de dados pessoais coletados e tratados; a fixação de obrigações aos coletores de dados; o "direito de acessar, recuperar e excluir os dados pessoais recolhidos sobre si"; a limitação ao uso de dados pessoais (temporal, contra perda e destruição, estrita necessidade); e o monitoramento por órgãos independentes de proteção[42]. Embora a Carta não enderece o tema da inteligência artificial de forma específica, traz a preocupação com a preservação da integridade dos dados pessoais e com o direito individual de consentir com o uso destes dados.

Por seu turno, no sistema interamericano de direitos humanos, centrado na **Organização dos Estados Americanos – OEA**, os trabalhos específicos sobre a temática dos direitos humanos eletrônicos e da proteção de dados são os realizados no âmbito da Relatoria para a Liberdade de Expressão, vinculada à Comissão Interamericana de Direitos Humanos, que toma como linha permanente de atuação a relação entre liberdade de expressão e internet.

Dentre os documentos que a Relatoria elaborou desde que começou a atuar neste campo, o principal foi publicado em 2013 com o título "Liberdade de Expressão e Internet", no qual traz uma asserção muito relevante acerca do direito informacional e do direito de proteção de dados: "os Estados estão obrigados a proibir o uso dos dados pessoais para fins contrários aos tratados de direitos humanos e a estabelecer os direitos de informação, correção e – caso seja necessário e proporcional – eliminação de dados, bem como a criar mecanismos de supervisão efetivos". Na sequência, afirma-se que deve ser garantido a todos o "direito de verificar se há dados pessoais seus armazenados em arquivos eletrônicos de dados, e, em caso afirmativo, de obter informações inteligíveis sobre quais são esses dados e com que objetivo eles foram armazenados[43].

De forma paralela, a Relatoria Especial sobre Direitos Econômicos, Sociais e Culturais, também vinculada à Comissão Interamericana de Direitos Humanos, emitiu em 2019

[42] Ibid.
[43] OEA – ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Comissão Interamericana de Direitos Humanos. Relatoria Especial para a Liberdade de Expressão. **Liberdade de Expressão e Internet**. Washington: OEA, 2013.

o "Informe Empresas e Direitos Humanos: estandartes interamericanos", onde se endereça de forma específica as empresas no âmbito de tecnologias de informação e comunicação. São feitas críticas à vigilância em massa e ao armazenamento indiscriminado de dados, que podem comprometer a fruição de direitos humanos na rede, o que é especialmente grave devido à posição de vulnerabilidade que ocupa o usuário. O Informe segue destacando as possibilidades de que o mau uso de *big data* gerem violações de direitos humanos, especialmente referentes à privacidade, à proteção de dados pessoais, à preservação do anonimato, à não discriminação algorítmica; tal como os problemas que envolvem as práticas de *profiling*, como a abertura a decisões puramente automatizadas e discriminatórias, e de manipulação dos resultados nos mecanismos de busca, influenciando no poder de decisão do usuário. Sendo assim, destaca a necessidade dos Estados promoverem tratados bilaterais com estas empresas atuantes na internet com o propósito de forçá-las a cumprir os padrões de direitos humanos on-line[44].

Ainda tomando em conta os sistemas regionais de proteção aos direitos humanos, em 2014, os membros da **União Africana** aprovaram um tratado internacional sobre proteção de dados dentre os organismos de proteção do direito internacional dos direitos humanos, a Convenção da União Africana sobre Cibersegurança e Proteção dos Dados Pessoais[45].

A Convenção fixa no artigo 13 os princípios de base que regem o processamento dos dados pessoais, justificando-se a menção do: princípio 1, do consentimento e da legitimidade do processamento de dados pessoais, de onde se extrai que somente é legítimo o processamento de dados cujo titular deu consentimento; princípio 2, da legalidade e da lealdade no processamento de dados pessoais, que deve ocorrer de forma lícita, justa e não fraudulenta, o que obsta a manipulação algorítmica de dados com propósito ilícito ou desonesto; princípio 4, da exatidão dos dados pessoais, obrigando a manutenção dos dados atualizados e compatíveis com a realidade; princípio 5, da transparência no processamento dos dados pessoais, devendo ser informado o titular dos dados acerca da forma como estes são tratados. Ainda, destaca-se no artigo 14 o princípio da proibição da coleta de determinados dados sensíveis, como os que revelam origem racial, étnica ou regional, filiação, ideologia, políticas, crenças religiosas ou convicções filosóficas, filiação sindical, vida sexual, informação genética ou estado de saúde[46].

[44] Id. Comissão Interamericana de Direitos Humanos. Relatoria Especial sobre Direitos Econômicos, Sociais e Culturais. **Informe sobre Empresas y Derechos Humanos: Estándares Interamericanos**. Washington: OEA, 2019.

[45] O documento ainda não conta com ratificações suficientes para entrar em vigor, mas prova que o sistema africano está atento à questão dos dados e da necessidade de protegê-los.

[46] UNIÃO AFRICANA. **Convenção da União Africana sobre Cibersegurança e Proteção dos Dados Pessoais**. Malabo, 27 jun. 2014. Disponível em: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Acesso em: 20 fev. 2020.

Finalizando a abordagem dos sistemas regionais, o **Conselho da Europa** se encontra em estágio avançado em suas normativas sobre a proteção de dados e a inteligência artificial. O vasto arcabouço normativo e jurisprudencial que cerca não apenas o Conselho da Europa, como também a União Europeia, notoriamente vanguardista e com maior impacto normativo que as demais normas de direito internacional dos direitos humanos, colocam o sistema europeu numa posição dianteira para a determinação dos estandartes a respeito da proteção do direito à informação e da autodeterminação informacional.

Dentre os diversos órgãos do Conselho da Europa que estão comprometidos com a pauta da proteção do direito informacional na internet, destaca-se o Comitê *ad hoc* sobre Inteligência Artificial, que se concentra em discussões sobre *machine learning* e proteção contra manipulação algorítmica e sobre os benefícios e riscos do avanço da Inteligência Artificial. Não há, em outros órgãos do sistema de proteção dos direitos humanos, uma discussão tão específica e avançada quanto esta.

Quanto aos documentos que podem ser apontados no âmbito do Conselho estão as Recomendações e Declarações do Comitê de Ministros no campo da mídia e da sociedade da informação[47] e o Guia para Direitos Humanos dos Utilizadores de Internet que é uma ferramenta para a compreensão dos direitos humanos na rede e seus limites[48]. Acerca da proteção de dados, o Guia destaca pontos que merecem atenção, fixando que toda pessoa:

> Tem o direito ao respeito pela sua vida privada e familiar na internet, o qual passa pela proteção dos seus dados pessoais e pelo respeito pela confidencialidade da sua correspondência e comunicações. Isto significa que: 1. Deve estar ciente de que, ao utilizar a internet, os seus dados pessoais são regularmente tratados. Isto acontece quando utiliza serviços como navegadores, correio eletrônico, mensagens instantâneas, voz por protocolos de internet, redes sociais, motores de pesquisa e serviços de armazenamento de dados na nuvem; 2. As autoridades públicas e as empresas privadas são obrigadas a respeitar regras e procedimentos específicos quando tratam os seus dados pessoais; 3. Os seus dados pessoais só devem ser tratados nas situações previstas na lei ou com o seu consentimento. Deve receber informação indicando quais os dados pessoais tratados e/ou transmitidos a terceiros, quando, por quem e para que fim. De um modo geral, deve poder controlar os seus dados pessoais (verificar a sua exatidão, solicitar a sua

[47] CONSELHO DA EUROPA. **Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society**. Estrasburgo, julho de 2015. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44. Acesso em: 25 ago. 2018.

[48] Id. **Guia dos Direitos Humanos para os Utilizadores de Internet**. Recomendação do Comitê de Ministros CM/Rec(2014)6, de 16 de abril de 2014. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a0532. Acesso em: 25 ago. 2018.

> correção ou supressão ou pedir a sua conservação por mais tempo do que o necessário); 4. Não pode ser objeto de medidas de vigilância geral ou interceptação. Nas circunstâncias excecionais previstas na lei, por exemplo, numa investigação criminal, pode ocorrer uma ingerência na sua privacidade através do acesso aos seus dados pessoais. Neste contexto, deve ser-lhe facultada informação acessível, clara e precisa sobre a lei ou política aplicável e sobre os seus direitos; [...][49].

Por seu turno, o Conselho da Europa, em parceria com a União Europeia, lançou um documento que sintetiza todos os debates acerca da proteção de dados no âmbito europeu. O documento contextualiza as normativas de proteção de dados europeias, tal como adota uma padronização terminológica. Ainda, discrimina os princípios que devem reger a proteção de dados – legalidade, lealdade e transparência; limitação de propósito; minimização da coleta; precisão; limitação ao armazenamento; segurança informacional e responsabilidade[50].

Além de delimitar a estrutura de proteção de dados europeia, o documento também aborda os direitos dos sujeitos titulares de dados, assim enumerados: informação; retificação; esquecimento; restrição do processamento; portabilidade de dados; não sujeição a decisões exclusivamente automatizadas. No encerramento do documento, abordam-se os novos desafios para a proteção de dados, entre eles o de compreensão sobre *big data*, algoritmos e inteligência artificial, que impactam diretamente nos direitos dos usuários da rede[51].

A preocupação com a questão da inteligência artificial também se reflete em outros documentos, como o Guia do Conselho da Europa sobre Inteligência Artificial e Proteção de Dados, lançado em novembro de 2019. O Conselho aponta que, de forma geral, tem utilizado uma técnica analógica, denominada *principles-based approach*, para compreender a aplicação dos direitos humanos fundamentais no contexto da inteligência artificial, que tem como atuais pontos de pressão o *big data* e o *machine learning*, mas que tende a se desenvolver para rumos cada vez mais complexos e desafiadores[52]. O documento chama atenção ao reconhecer que a autodeterminação informacional não pode ser vista apenas sob o foco do consentimento informado, em especial diante do complexo cenário evolutivo dos dados digitais:

[49] Ibid.
[50] Id. **Handbook on European data protection law**. Luxembourg: European Union Agency for Fundamental Rights and Council of Europe, 2018. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf. Acesso em: 20 fev. 2020.
[51] Ibid.
[52] Id. **Artificial Intelligence and data protection**. Council of Europe, november 2019. Disponível em: https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7. Acesso em: 20 fev. 2020.

> Os juristas abordaram essas questões destacando o papel da transparência, da avaliação de riscos e de formas de consentimento mais flexíveis, como consentimento amplo ou dinâmico. Embora nenhuma dessas soluções forneça uma resposta definitiva ao problema do consentimento individual, em certos contextos essas soluções, sozinhas ou combinadas, podem reforçar a autodeterminação. Além disso, a noção de autodeterminação não é limitada por um dado caso de processamento de dados. Ele pode ser usada em um sentido amplo para se referir à liberdade de escolha sobre o uso da IA e o direito a uma versão não inteligente dos dispositivos e serviços equipados com IA[53]. (Tradução nossa)

O documento prega uma abordagem de precaução no processo de coleta e armazenamento de dados, o que envolve especialmente a consideração dos riscos de impactos adversos devido à descontextualização de dados e de modelos algorítmicos. De tal modo, a vigilância algorítmica exige a responsabilidade e o controle de todos os atores que operam com dados, pois estes são obrigados a atender parâmetros de proteção aos direitos humanos[54].

Não obstante, o documento aprofunda a estrita relação entre proteção de dados e inteligência artificial, uma vez que as aplicações que se baseiam em inteligência artificial precisam da alimentação por dados para se operacionalizarem[55]. Além disso, destaca a evolução da temática da inteligência artificial no contexto da proteção de dados, pontuando a importância dos direitos humanos para o estabelecimento de limites éticos ao desenvolvimento tecnológico:

> Na última década, a crescente disponibilidade banda larga para transferência e armazenamento de dados e para recursos computacionais - por meio do novo paradigma da computação em nuvem - e a progressiva difusão de dados de grande parte de nossa vida e ambiente criaram um contexto completamente novo. Isso levou a uma ruptura na inteligência artificial, permitindo novas formas de gerenciamento de dados a extraírem mais informações e criarem novos conhecimentos. *Big Data* e *Machine Learning* representam os produtos mais recentes desse processo de desenvolvimento. [...] Um desenvolvimento de tecnologia orientada para os direitos humanos pode aumentar os custos e forçar os desenvolvedores e as empresas a ampliarem o atual tempo de inserção no mercado, pois o impacto de produtos e serviços nos direitos individuais e na sociedade deve ser avaliado com antecedência. Ao mesmo tempo, a médio e longo prazo, essa abordagem reduzirá custos e aumentará a eficiência. Além disso, as empresas e a sociedade estão maduras o suficiente para ver a responsabilidade em relação aos indivíduos e à sociedade como o principal objetivo no desenvolvimento da IA. [...] O desenvolvimento de IA

[53] Ibid. No original: "Legal scholars have addressed these issues by highlighting the role of transparency, risk assessment and more flexible forms of consent, such as broad consent or dynamic consent. Although none of these solutions provides a definitive answer to the problem of individual consent, in certain contexts these solutions, alone or combined, may reinforce self-determination. Moreover, the notion of self-determination is not circumscribed by a given case of data processing. It can be used in a broad sense to refer to freedom of choice over the use of AI and the right to a non-smart version of AI-equipped devices and services".
[54] Ibid.
[55] Ibid.

> centrada em dados deve, portanto, basear-se nos princípios da Convenção 108 como base para uma sociedade digital florescente[56]. (tradução nossa)

Sendo assim, o documento que tem servido de base no direito internacional dos direitos humanos para a disciplina da proteção de dados no contexto da inteligência artificial é a Convenção Europeia sobre a Proteção de Dados Pessoais (Convenção n. 108), datada de 1981 e modernizada em 2018, quando passou a ser denominada Convenção Europeia para a Proteção de Indivíduos com relação ao Processamento de Dados Pessoais (Convenção n. 108+). É interessante notar que, mesmo sendo um documento de uma organização regional europeia, se permitiu a abertura à assinatura por um país latino-americano, o Uruguai, em 2013[57].

O capítulo II da Convenção n. 108+ aborda os princípios básicos para a proteção de dados, dentre eles o de exigência de consentimento livre, específico, informado e inequívoco e o de transparência em todo o processo de coleta, armazenamento e transferência de dados (artigos 5º e 8º). Por seu turno, o artigo 9º sintetiza os direitos do titular de dados:

> Artigo 9º - Direitos do titular dos dados
> 1. Todo indivíduo tem direito:
> a. *não estar sujeito a uma decisão que o afete significativamente, com base apenas no processamento automatizado de dados,* sem que suas opiniões sejam levadas em consideração;
> b. obter, mediante solicitação, a intervalos razoáveis e sem demora ou despesa excessiva, a confirmação do processamento de dados pessoais relacionados a ele, a comunicação de forma inteligível dos dados processados, todas as informações disponíveis sobre sua origem, sobre o período de preservação, bem como qualquer outra informação que o responsável pelo tratamento seja obrigado a fornecer, a fim de garantir a transparência do processamento nos termos do artigo 8º.
> c. obter, mediante solicitação, conhecimento do raciocínio subjacente ao processamento de dados onde os resultados desse processamento sejam aplicados a ele;

[56] Ibid. No original: "Over the past decade, the increasing availability of bandwidth for data transfer, data storage and computational resources – through the new paradigm of cloud computing – and the progressive datafication of large part of our life and environment have created a completely new context. This has led to a breakthrough in AI, enabling new forms of data management to extract more information and create new knowledge. Big Data analytics and Machine Learning represent the most recent products of this development process. [...] A human rights-oriented development of technology might increase costs and force developers and business to slow their current time-to-market, as the impact of products and services on individual rights and society have to be assessed in advance. At the same time, in the medium to long-term, this approach will reduce costs and increase efficiency. Moreover, businesses and society are mature enough to view responsibility towards individuals and society as the primary goal in AI development. [...] Data-centric AI development should therefore be based on the principles of Convention 108 as the foundations for a flourishing digital society".

[57] Id. **Convention for the Protection of Individuals with Regard to the Processing of Personal Data**. Adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 20 fev. 2020.

> d. objetar a qualquer momento, por motivos relacionados à sua situação, ao tratamento de dados pessoais a seu respeito, a menos que o responsável pelo tratamento demonstre motivos legítimos para o tratamento que anulem seus interesses ou direitos e liberdades fundamentais;
> e. obter, mediante solicitação, gratuitamente e sem demora excessiva, retificação ou apagamento, conforme o caso, de tais dados, se estes estiverem sendo ou tiverem sido processados de maneira contrária às disposições da presente Convenção;
> f. ter um remédio nos termos do artigo 12, caso seus direitos sob esta Convenção tenham sido violados;
> g. beneficiar, independentemente de sua nacionalidade ou residência, da assistência de uma autoridade supervisora na acepção do artigo 15, no exercício de seus direitos ao abrigo da presente Convenção.
> 2. O parágrafo 1.a *não se aplica se a decisão for autorizada por uma lei à qual o responsável pelo tratamento está sujeito e que também estabelece medidas adequadas para salvaguardar os direitos, liberdades e interesses legítimos do titular dos dados*[58]. (Tradução nossa)

Com efeito, ainda que a Convenção n. 108+ não enderece terminologicamente a inteligência artificial, mostra uma preocupação bastante clara com a tomada de decisões a partir de algoritmos de aprendizado, servindo a proteção de dados como instrumento para assegurar que o *machine learning* não mine a autodeterminação individual e não se preste à reverberação de propósitos discriminatórios. Neste cenário, em meio aos sistemas atuantes no campo do direito internacional dos direitos humanos, o europeu tem se mostrado particularmente avançado e, ao que tudo indica, será a principal influência para futuros avanços no âmbito internacional, que ainda dá passos curtos e titubeantes rumo ao reconhecimento da importância da proteção de dados para a limitação do infinito potencial da inteligência artificial.

CONCLUSÃO

[58] Ibid. No original: "Article 9 – Rights of the data subject. 1. Every individual shall have a right: a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration; b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1; c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her; d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms; e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention; f. to have a remedy under Article 12 where his or her rights under this Convention have been violated; g. to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention. 2. Paragraph 1.a shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests".

As novas estruturas do modelo capitalista, erigindo um capitalismo informacional, coloca o dado como o objeto das transações entre poder público e privado, tal como entre agentes privados. O dado tem um valor e é tratado como mercadoria, uma vez que permitem ao adquirente que conheça a respeito do público de seu interesse, direcionando desejos de consumo e decisões de vida. Os algoritmos, alimentados pelos dados, conduzem o usuário da internet a uma falsa sensação de escolha, enquanto na prática condicionam seu comportamento. Numa velocidade sem precedentes, a humanidade vê sua forma de consumir e de gastar transformar-se. Simultaneamente, surgem novas formas de relacionamento e máquinas que aprendem conduzem comportamentos humanos diversos, inclusive afetivos, a partir do tratamento dos dados que alimentam os aplicativos deste nicho.

Vale destacar também que os dados revolucionaram a forma de se fazer política. Algoritmos inteligentes eram utilizados como instrumentos para a definição de público eleitoral antes mesmo do caso Snowden e ainda o são. O *machine learning* direciona notícias e publicidades que interessam a cada indivíduo, mas lhe falta a ética para questionar aspectos como autenticidade e razoabilidade – uma notícia é uma notícia, não importa se verdadeira ou falsa; uma publicidade é uma oferta de produto ou serviço, não importa se cumpre o prometido. Talvez as coisas já fossem assim no passado e talvez toda eleição que já ocorreu tenha sido em alguma medida cercada por "*fake news*". Contudo, a internet potencializou as possibilidades de manipulação do processo democrático.

Com efeito, a proteção de dados se mostra como o único instrumento capaz de impor limitações ao que a inteligência artificial, por intermédio do *machine learning*, tem potencial de fazer, podendo conduzir o comportamento humano e minar a autodeterminação individual. A proteção de dados pode impedir que os indivíduos se sujeitem a decisões totalmente automatizadas (e potencialmente discriminatórias) e que seus dados sejam indevidamente utilizados para a manipulação de seu poder decisório individual. Logo, a proteção de dados viabiliza a autodeterminação informativa e limita a inteligência artificial, o que justifica sua importância exponencial no campo do direito internacional dos direitos humanos.

REFERÊNCIAS

ABELSON, Hal; LEDEEN, Ken; LEWIS, Harry. **Blown to bits**: your life, liberty and happiness after the digital explosion. Crawfordsville (Indiana/USA): Addison-Wesley, 2008.

BELLI, Luca. **Network Self-Determination and the Positive Externalities of Community Networks**. In: Community Networks: the Internet by the People, for the People. Rio de Janeiro: FGV Direito Rio, 2017, p. 35-64.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense/GEN, 2019.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei n. 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: 12 fev. 2020.

CONSELHO DA EUROPA. **Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society**. Estrasburgo, julho de 2015. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44. Acesso em: 25 ago. 2018.

CONSELHO DA EUROPA. **Guia dos Direitos Humanos para os Utilizadores de Internet**. Recomendação do Comitê de Ministros CM/Rec(2014)6, de 16 de abril de 2014. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a0532. Acesso em: 25 ago. 2018.

CONSELHO DA EUROPA. **Handbook on European data protection law**. Luxembourg: European Union Agency for Fundamental Rights and Council of Europe, 2018. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf. Acesso em: 20 fev. 2020.

CONSELHO DA EUROPA. **Artificial Intelligence and data protection**. Council of Europe, november 2019. Disponível em: https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7. Acesso em: 20 fev. 2020.

CONSELHO DA EUROPA. **Convention for the Protection of Individuals with Regard to the Processing of Personal Data**. Adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 20 fev. 2020.

DOMINGOS, Pedro. **O Algoritmo Mestre: como a busca pelo algoritmo de *machine learning* definitivo recriará nosso mundo**. São Paulo: Novatec, 2017, p. 130-180. (Edição do Kindle)

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2019. (E-book)

FRAZÃO, Ana. **Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Revista dos Tribunais, 2019. p. 23-52.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental**. Brasília: IDP, 2019. (Edição do Kindle)

OEA – ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Comissão Interamericana de Direitos Humanos. Relatoria Especial para a Liberdade de Expressão. **Liberdade de Expressão e Internet**. Washington: OEA, 2013.

OEA – ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Comissão Interamericana de Direitos Humanos. Relatoria Especial sobre Direitos Econômicos, Sociais e Culturais. **Informe sobre Empresas y Derechos Humanos: Estándares Interamericanos**. Washington: OEA, 2019.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Digital Economy Report 2019: Overview**. Geneva: United Nations, 2019. Disponível em: https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf. Acesso em: 08 fev. 2020.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Conselho de Direitos Humanos. **The promotion, protection and enjoyment of human rights on the Internet**. Resolução n. 32/13 do Conselho de Direitos Humanos, 18 de julho de 2016. Disponível em: http://search.un.org/. Acesso em: 25 ago. 2018.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Right of peoples to self-determination**. Resolução adotada pela Assembleia Geral em 18 de dezembro de 2019. Disponível em: https://documents-dds-ny.un.org/. Acesso em: 18 fev. 2020.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **The right to privacy in the digital age**. Resolução adotada pela Assembleia Geral em 17 de dezembro de 2018. Disponível em: https://documents-dds-ny.un.org/. Acesso em: 18 fev. 2020.

SILVEIRA, Alessandra; FROUFE, Pedro. **Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos**. UNIO – EU Law Journal, v. 4, n. 2, jul. 2018, p. 4-20.

SOMBRA, Thiago Luís Santos. **Direito à privacidade e proteção de dados no ciberespaço: a *accountability* como fundamento da *lex privacy***. 2019. 219 f. Tese (Doutorado em Direito) – Universidade de Brasília, Brasília, 2019.

UE – UNIÃO EUROPEIA. **RGPD – Regulamento Geral de Proteção de Dados**. Regulamento n. 679/2016. Disponível em: https://eur-lex.europa.eu/. Acesso em: 13 fev. 2020.

UNIÃO AFRICANA. **Convenção da União Africana sobre Cibersegurança e Proteção dos Dados Pessoais**. Malabo, 27 jun. 2014. Disponível em: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Acesso em: 20 fev. 2020.

WATSON, Chloe. **The key moments from Mark Zuckerberg's testimony to Congress**. The Guardian, 11 abr. 2018. Disponível em: https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments. Acesso em: 18 fev. 2020.