



**Universidade de Brasília – UnB
Faculdade de Direito**

GABRIEL PINHEIRO BELEZA

**A PROTEÇÃO E O TRATAMENTO DE DADOS PESSOAIS POR
SISTEMAS DE IA: UMA POSSIBILIDADE DE APLICAÇÃO
ANALÓGICA DA LEI 13.709/18?**

*Protection and processing of personal data by AI systems: a possibility of analogue application of law
13.709/18?*

Brasília
2021

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

**A PROTEÇÃO E O TRATAMENTO DE DADOS PESSOAIS POR
SISTEMAS DE IA: UMA POSSIBILIDADE DE APLICAÇÃO
ANALÓGICA DA LEI 13.709/18?**

Autor: Gabriel Pinheiro Beleza

Orientador: Prof. Dr. Henrique Araújo Costa

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel, no Programa de ou Graduação da Faculdade de Direito da Universidade de Brasília.

Brasília, 17 de maio de 2021.

FOLHA DE APROVAÇÃO

GABRIEL PINHEIRO BELEZA

A proteção e o tratamento de dados pessoais por sistemas de IA: uma possibilidade de aplicação analógica da Lei 13.709/18?

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel no Programa de Graduação da Faculdade de Direito da Universidade de Brasília.

Aprovada em: 17 de maio de 2021.

BANCA EXAMINADORA

Prof. Dr. Henrique Araújo Costa
(Orientador – Presidente)

Prof. Dr. Bruno Freire de Carvalho Calabrich
(Membro)

Profa. Dra. Fernanda de Carvalho Lage
(Membro)

Profa. Fernanda Potiguara Carvalho
(Suplente)

Agradecimentos

Agradeço, primeiramente, meus pais, pelo amor e confiança que sempre depositaram em mim. Seu apoio foi e sempre será fundamental, e todas as minhas conquistas só se concretizaram pois vocês sempre estiveram aqui para me mostrar que eram e são possíveis.

Obrigado aos amigos que me acompanham e caminham ao meu lado desde os tempos de colégio e aos novos amigos feitos na Faculdade. Vocês são como uma segunda família para mim.

Obrigado, Universidade de Brasília, por me fazer enxergar o quão plural nossa sociedade é e me ensinar a respeitar cada uma dessas diferenças.

Obrigado a todos os professores pelos ensinamentos que, em sua maioria, ultrapassam os limites da sala de aula.

"Se vi mais longe foi por estar sobre os ombros de gigantes"

FICHA CATALOGRÁFICA

BELEZA, Gabriel Pinheiro. A proteção e o tratamento de dados pessoais por sistemas de IA: uma possibilidade de aplicação analógica da Lei 13.709/18? / Gabriel PINHEIRO BELEZA; orientador Henrique DE ARAÚJO COSTA. -- Brasília, 2021. 44 p.

Monografia (Graduação - Direito) -- Universidade de Brasília, 2021.

1. Inteligência Artificial. 2. Dados Pessoais . 3. Tratamento de Dados. 4. LGPD. 5. Analogia. I. COSTA, Henrique Araújo, orient.

PB428p

REFERÊNCIA BIBLIOGRÁFICA

BELEZA, G. P.. (2021). A proteção e o tratamento de dados pessoais por sistemas de IA: uma possibilidade de aplicação analógica da Lei 13.709/18?. Monografia apresentada como requisito parcial à obtenção do grau de Bacharel no Programa de Graduação da Faculdade de Direito da Universidade de Brasília, Brasília, DF.

Sumário

A proteção e o tratamento de dados pessoais por sistemas de IA: uma possibilidade de aplicação analógica da Lei 13.709/18?

1. INTRODUÇÃO	10
1.1 Apresentação do Estudo	10
1.2 Justificativa da Pesquisa	18
1.3 Problema de pesquisa e hipótese	20
1.4 Limitações do Estudo	21
2. DESENVOLVIMENTO	22
2.1 Por que é necessário regular o tratamento de dados por IAs?	22
2.2 As legislações internacionais sobre proteção e tratamento de dados pessoais e utilização de IAs	18
2.3 As legislações europeias sobre proteção e tratamento de dados pessoais e utilização de IAs	20
2.4 As leis brasileiras sobre proteção e tratamento de dados pessoais e utilização de IAs	32
2.5 É possível uma aplicação analógica da LGPD a sistemas de IA? Como deve ser feita?	36
3. CONCLUSÃO	38
REFERÊNCIAS BIBLIOGRÁFICAS	40

Resumo

Os avanços tecnológicos das últimas décadas possibilitaram o surgimento dos chamados sistemas de Inteligência Artificial - IA. Para que seu desenvolvimento e funcionamento seja possível, IAs se utilizam de grandes quantidades de dados (muitas vezes pessoais), tratando-os de acordo com o objetivo específico para que esse sistema foi desenvolvido. Ainda que possua inúmeros benefícios e um infinito número de aplicações possíveis, o tratamento de dados não está isento de risco, e suas consequências já podem ser observadas. Cientes desse risco, a maior parte dos países desenvolvidos busca incorporar a suas legislações normas capazes de ofertar um grau mínimo de segurança jurídica a essa atividade. Apesar de estarem buscando ensejar um grau mínimo de proteção aos dados pessoais e a seu tratamento, as legislações existentes sobre o tema estão desconsiderando quanto essas temáticas estão associadas a IAs ou necessitam destes sistemas para seu funcionamento. Por isto, este trabalho se dedica a analisar a possibilidade de uma aplicação analógica da Lei 13.709/18 (Lei Geral de Proteção de Dados - LGPD) às IAs, visando a assegurar que esses sistemas observarão as normas de proteção e tratamento de dados pessoais vigentes.

Palavras-chaves: Inteligência Artificial; Dados Pessoais; Tratamento de dados; LGPD; Analogia;

Abstract

The technological advances of the last decades have made possible the appearance of the so-called Artificial Intelligence systems - AI. For their development and operation to be possible, AIs use large amounts of data (often personal), treating them according to the specific objective for which this system was developed. Although it has numerous benefits and an infinite number of possible applications, data processing consequences can already be seen. Aware of this risk, most developed countries seek to incorporate into their legislation standards capable of offering a minimum degree of legal certainty to this activity. Although they are seeking to provide a minimum degree of protection to personal data and its treatment, the existing laws on the subject are disregarding the extent to which these themes are associated with IAs or need these systems for their functioning. For this reason, this work is dedicated to analyzing the possibility of an analogous application of Law 13.709/18 (General Data Protection Law - GDPL) to IAs, aiming to ensure that these systems observe and will observe the rules for the protection and treatment of personal data in force.

Keywords: Artificial Intelligence; Personal Data; Data Treatment; GDPL; Analogy;

Lista de Siglas e Abreviaturas

<i>CC</i>	<i>Computação Cognitiva</i>
<i>DL</i>	<i>Deep Learning</i>
<i>IA</i>	<i>Inteligência Artificial</i>
<i>LGPD</i>	<i>Lei Geral de Proteção de Dados</i>
<i>ML</i>	<i>Machine Learning</i>
<i>PE</i>	<i>Parlamento Europeu</i>
<i>OECD</i>	<i>The Organisation for Economic Co-operation and Development</i>
<i>RGPD</i>	<i>Regulamento Geral sobre a Proteção de Dados</i>
<i>UE</i>	<i>União Europeia</i>

A proteção e o tratamento de dados pessoais por sistemas de IA: uma possibilidade de aplicação analógica da Lei 13.709/18?

1. INTRODUÇÃO

1.1 Apresentação do Estudo

Considerando os impactos jurídicos decorrentes da utilização de inteligências artificiais (IAs), esta pesquisa analisa como o tratamento de dados poderia ser regulamentado por esses sistemas, de forma que sejam observadas as disposições contidas na Lei 13.709/18 (Lei Geral de Proteção de Dados - LGPD) brasileira. As perguntas que se pretende responder são: apesar de não ter sido desenvolvida com essa finalidade (de regulamentar IAs), a LGPD poderia ser aplicada analogicamente a esses sistemas? Qual a justificativa para realizar essa aplicação?

No capítulo introdutório, são abordados conceitos básicos fundamentais para o desenvolvimento do estudo, quais sejam: I) Dados; II) Inteligência Artificial; III) LGPD; IV) Analogia. Têm-se também os tópicos de Justificativa da Pesquisa (1.2), Problema de pesquisa e Hipótese (1.3) e Limitações do Estudo (1.4).

O segundo capítulo, referente ao desenvolvimento do presente estudo, foi dividido em quatro tópicos:

2.1: dedica-se a expor a necessidade de regulação sobre o tema e possíveis problemas já observados no tratamento de dados pessoais por sistemas de IA. São apresentados, também, dois casos exemplificativos em que esse tratamento gerou violações a direitos fundamentais;

2.2: apresenta como as temáticas de proteção e tratamento de dados e a utilização de IAs são encaradas internacionalmente e analisa a existência de tratados ou normas internacionais sobre o assunto;

2.3: analisa como o ordenamento europeu enfrenta as questões de proteção e tratamento de dados pessoais e a utilização de IA atualmente;

2.4: analisa como o ordenamento brasileiro enfrenta as questões de proteção e tratamento de dados pessoais e a utilização de IA atualmente. Também examina propriamente a possibilidade de aplicação analógica da LGPD aos sistemas de IA;

O terceiro capítulo dedica-se à apresentação dos resultados obtidos.

Em consonância com o que é explicado no tópico 1.2, a escolha das normas europeias como referencial não foi aleatória e se baseou em dois motivos. O primeiro é a eficácia dessas normas, que são consideradas por especialistas como as mais avançadas do mundo; o segundo é a semelhança entre as legislações brasileira e europeia em relação ao tema, o que não é coincidência. Conforme evidenciado nos tópicos 2.3 e 2.4, a LGPD foi diretamente inspirada no RGPD europeu.

1.1.1 O que são dados

Com o advento dos sistemas computacionais e sua posterior popularização, a informação tomou um lugar de protagonismo na sociedade moderna. Por consequência, quase não há grupo ou setor da sociedade que não utilize sistemas computacionais em suas atividades.

A implementação de sistemas computacionais e eletrônicos exige, em seu funcionamento, quantidades massivas de informações — os chamados dados. O dicionário Houaiss define o substantivo dados como “informação relativa a um indivíduo, capaz de identificá-lo; informação capaz de ser processada por um computador”.

Ainda que usualmente doutrina e a legislação tratem os conceitos de dados e de informação como sinônimos, alguns autores defendem a existência de uma diferenciação conceitual, pois entendem que o termo "dados" refere-se a uma “pré-informação”, anterior à sua interpretação e/ou transmissão ao interlocutor, enquanto o termo ‘informação’ propriamente dito faz alusão a um conhecimento de conteúdo depurado, refinado (WIENER,

1954, p. 17, apud DONEDA, 2020, p. 3485/9487, livro eletrônico). Para os fins deste estudo, o termo 'dados', sempre que utilizado, estará se referindo aos dados coletados e utilizados por dispositivos eletrônicos durante seu funcionamento (tais como os dados pessoais, dados pessoais sensíveis etc.), enquanto o termo informação será utilizado em seu sentido literal.

Um dado pode fazer referência a qualquer tipo de conteúdo, existindo por si só. Quando uma informação faz referência a uma pessoa, ela deixa de ser uma mera informação, adentrando uma nova categoria e se tornando uma informação pessoal. Pesquisadores do ramo da Teoria Jurídica da Informação, tais como Pierre Catala, sustentam que, a partir do momento que um dado pode fazer ou faz referência a uma pessoa, a uma característica pessoal e/ou às suas ações, esse torna-se uma informação pessoal.

O fato de um dado fazer referência a uma pessoa, por si só, não é suficiente para considerá-lo como sendo pessoal. Seguindo a linha defendida por Catala, Danilo Doneda entende que, além de referir-se a um indivíduo, dados pessoais devem revelar suas características e ações, como nome civil, perfil de consumo, opiniões que manifesta, domicílio etc. Sobre o assunto, o autor explana:

É importante estabelecer este vínculo objetivo, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre esta pessoa, por exemplo, a princípio não possuem este vínculo objetivo; também a produção intelectual de uma pessoa, em si considerada, não é per se informação pessoal (embora o fato de sua autoria o seja). (DONEDA, 2020).

Dados pessoais também podem ser utilizados como um meio de representação da pessoa ou de sua personalidade perante a coletividade. Na sociedade da informação¹ em que vivemos, um indivíduo pode, por exemplo, ter sua orientação religiosa revelada ou ser identificado em um determinado vínculo/relacionamento (seja afetivo, trabalhista, crédito etc.) apenas através dos dados pessoais que coloca a disposição (DONEDA, 2020; SCHERTEL, 2019).

¹ Termo cunhado pelo sociólogo Daniel Bell em sua obra "*O advento da sociedade pós-industrial*", de 1973;

Por outro lado, alguns dados podem ser anônimos. Um dado anônimo não é um dado vazio, sem informações ou com informações irrelevantes, mas sim aqueles que ou não podem ser diretamente vinculados a um único indivíduo ou armazenam informações referentes a grupos de indivíduos, de modo que nenhum deles possa ser identificado de forma personalíssima.

A LGPD traz, nos incisos de seu art. 5º, a conceituação de Dados Anônimos e Dados Pessoais, subdividindo este último em duas categorias: os Dados Pessoais e os Dados Pessoais Sensíveis. A grande maioria dos dados é armazenada nos chamados Bancos de Dados, que são locais para armazenamento de conjuntos massivos de informações, organizados em uma lógica pré-determinada (DONEDA, 2020).

Além disso, o aumento da capacidade de processamento das máquinas, somado à capacidade que dados pessoais têm em revelar informações das mais distintas naturezas, acabou viabilizando o que hoje é amplamente denominado tratamento de dados.

O tratamento de dados é a utilização de dados, pessoais ou anônimos, pelos mais diferentes setores da sociedade, privados ou públicos. Ele consiste em armazenar, processar, agrupar e combinar quantidades massivas de informações em um pequeno espaço de tempo e a custos baixíssimos, podendo ser aplicado a qualquer tipo de dados.

O tratamento de dados pessoais se tornou uma realidade no século XXI, e já ocorre de forma totalmente automatizada. Por isso quase não existem dados que não passem por algum tipo de tratamento, bem como operadores ou usuários de dispositivo eletrônico que não se beneficiem, direta ou indiretamente, dessa ação. O tratamento de dados, contudo, não está imune a riscos ou imbróglios, como apresentado no tópico 2.1.

1.1.2 O que é IA

Dentro do universo de novas tecnologias computacionais aplicadas, a Inteligência Artificial (IA) apresenta-se como uma das mais promissoras, encontrando-se empregada nas mais variadas atividades e dispositivos eletrônicos.

O termo Inteligência Artificial foi cunhado por John McCarthy em 1956 para remeter a “máquinas que conseguem realizar tarefas características da inteligência humana” (MARCONDES, 2017). Atualmente, a expressão é utilizada para se referir às mais diversas funções desempenhadas de forma independente por máquinas, ou seja, que não necessitam de constante intervenção humana.

A expressão Inteligência Artificial já é empregada para fazer alusão a “vários métodos, técnicas e práticas com algoritmos que tornam um *software* inteligente, como computação cognitiva, processamento de linguagem natural, *machine learning* e *deep learning*” (RIGUEIRA, 2017). A seguir, abordam-se, brevemente, as formas de funcionamento e particularidades de cada um dos sistemas operacionais mencionados por Marina Rigueira.

A grande maioria das IAs, senão todas, têm seu funcionamento baseado em algoritmos. De acordo com DOMINGOS (2017, p. 24, apud CALABRICH, 2020, p. 2-3), o algoritmo “é uma sequência de instruções que informa ao computador o que ele deve fazer. [...] Algoritmos programam voos e entregam mercadorias, calculam os lucros e mantêm registros”.

Bruno Calabrich ressalta, em seu artigo, que algoritmos já são capazes de realizar diagnósticos, julgamentos, classificações, e também podem ser utilizados como auxílio em processos de tomada de decisões e para traçar perfis pessoais, como os de consumo ou de crédito. Os algoritmos, portanto, são — neste contexto específico computacional — formas de tratamento e de utilização de dados pessoais com um objetivo específico, uma finalidade singular (independentemente do que é essa finalidade).

O *Machine Learning* (ML), ou Aprendizado de Máquinas, pode ser considerado como o “ponto de partida” de grande parte das IAs: consiste na utilização de algoritmos para captação de dados e, através da análise destes, na realização de previsões sobre possíveis cenários e/ou situações das mais diversas temáticas. O Aprendizado de Máquinas pode fazer uso de distintas metodologias e algoritmos (RIGUEIRA, 2017) e se manifesta como uma “alternativa metodológica para o enfrentamento de problemas de agrupamento (*clustering*), classificação, predição e inferência em grandes volumes de dados” (SILVA, 2018).

O *Deep Learning (DL)*, por sua vez, consiste em uma tentativa de “imitar” o cérebro humano e funciona através das chamadas redes neurais, responsáveis por interligar informações. Por meio de algoritmos, o *DL* é capaz de reconhecer padrões até então ocultos e até mesmo agrupar e classificar dados. Se antes as informações se encontravam meramente reunidas todas em um mesmo grande bloco — ex: informações sobre moradores de Brasília —, o *Deep Learning* pode ser utilizado para identificar qual a quantidade de moradores de uma determinada região, qual a renda média de cada bairro, para classificar os bairros em uma ordem decrescente de concentração de renda etc.

Parece não haver consenso quanto à definição formal da Computação Cognitiva (CC). De acordo com VARGA e ROTTA, a CC se apresenta como possível alternativa para “problemas complexos, dinâmicos, com certa dose de incerteza e ambiguidade” (2016, *TLCBRazil*, apud ATHENIENSE e RESENDE, 2017, p. 72). A empresa IBM, por exemplo, define que sistemas de CC são capazes de aprender com a linguagem natural e com textos, imagens e outros dados não estruturados que ainda não foram “transformados” para linguagem das máquinas.

Assistentes de voz presentes em smartphones, como o Google Voice e a SIRI, Chatbots, “ferramenta que atua como um atendente para entender e apresentar soluções para as demandas do usuário via chat” (MARTINS, 2017); veículos autônomos, como o Acura, desenvolvido pela Honda (HEAPS, 2017); e até mesmo a identificação facial em uma foto, citam-se, a título exemplificativo, os *softwares* utilizados pelas redes sociais *Facebook* e *Instagram*) são alguns exemplos da aplicação de IAs em atividades cotidianas.

Todos esses sistemas possuem três pontos em comum: 1) são alimentados com grandes quantidades de dados; 2) realizam, em/para seu funcionamento, o tratamento desses dados; 3) são embasados em algoritmos. Atingiu-se um patamar em que “a aplicação cotidiana da inteligência artificial pode ser usada tanto para previsões de fatos gerais sobre a economia, natureza ou política, como também para prever o comportamento individual” (DONEDA, SCHERTEL, SOUZA e ANDRADE, 2018).

Sistemas de IA, portanto, utilizam enormes quantidades de informações, e estas são constituídas majoritariamente (ou mesmo integralmente) de dados pessoais, sensíveis ou não. É necessário assegurar que dados coletados sejam tratados em conformidade com o preconizado na LGPD, e que o desenvolvimento desses sistemas esteja em consonância com a dignidade, os direitos e as liberdades dos indivíduos (GARCIA, 2019).

1.1.3 O que é a LGPD

A Lei Geral de Proteção de Dados foi a primeira lei no ordenamento brasileiro a dispor, de uma forma geral, sobre o tratamento de dados (SCHERTEL, 2019). Sancionada em agosto de 2018, a LGPD tem como objetivo assegurar que a utilização e o tratamento de dados - seja essa atividade realizada por entes públicos ou privados - se deem de forma transparente, de modo que seja possível evitar e combater irregularidades que podem surgir no processo de tratamento de informações.

A LGPD é considerada a primeira norma a efetivamente estabelecer um regime geral de proteção de dados no Brasil. Antes de sua edição, até existiam normas que dispunham sobre utilização e tratamento de dados; estas, contudo, estavam distribuídas de forma esparsa em legislações como o Código de Defesa do Consumidor e o Código Civil. Essa situação, além de gerar insegurança jurídica, não assegurava proteção satisfatória dos dados pessoais.

A lei em questão é altamente inspirada no Regulamento Geral para Proteção de Dados (RGPD ou Regulamento 2016/679) do Parlamento Europeu, contendo, inclusive, disposições semelhantes, a exemplo das referentes a tópicos como consentimento e tratamentos potencialmente discriminatórios de dados (CALABRICH, 2020, p. 5).

A LGPD traz, em seu corpo normativo, a conceituação dos principais termos e ações referentes aos dados pessoais e seu respectivo tratamento. São expostas, por exemplo, as diferenças entre dados pessoais e dados pessoais sensíveis, a definição de tratamento de dados, além de hipóteses em que a transferência internacional de dados pessoais é permitida.

Considerando que a citada norma já se encontra em vigor, ela será utilizada como principal referência para desenvolvimento deste estudo.

1.1.4 O que é a Analogia

Ainda que o direito e seu sistema normativo esteja em constante mudança para se adaptar à realidade, é impossível que o legislador ou as leis sejam capazes de abarcar ou prever todos os casos possíveis. Isso ocorre não só pela velocidade em que novas situações capazes de gerar fatos jurídicos ocorrem, mas também pela morosidade do próprio processo legislativo.

A existência de uma lacuna normativa não é sinônimo de total inexistência de normas jurídicas, mas sim de inexistência de uma determinada regra sobre um tema específico (KOCH, RUSSMAN, 1997, p. 254, apud LARENZ, 1997, p. 533). Sobre lacunas normativas, Larenz ensina que:

Da lacuna da lei distinguem alguns a lacuna do direito. Por tal pode entender-se o caso em que uma lei particular não está incompleta em si, quer dizer, comparada com seu plano regulador, mas sim na ordem jurídica em conjunto, enquanto deixa legislativamente por regular todo um sector que carece de uma regulação ou não contém um instituto jurídico que deva conter. (LARENZ, 1997, p. 533).

Frente à notória impossibilidade de se regulamentar todas as situações, surgiram os métodos de integração da norma. Esses métodos estão previstos no art. 4º da LINDB, que dispõe, *ipsis litteris* “Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito”.

A analogia, portanto, é um método de integração jurídica que consiste no emprego de uma lei em uma situação para a qual não foi originalmente concebida. A aplicação analógica pode se limitar a uma única norma ou pode compreender um conjunto delas. Entretanto, a Analogia não pode ser aplicada em fatos que o legislador deliberadamente decidiu não legislar, se omitiu de fazê-lo ou o fez de forma vaga, pois estas não constituem lacunas do direito, mas sim escolhas propositais do legislador (LARENZ, 1997).

Para evitar que a analogia seja aplicada de forma arbitrária, é necessário que a norma selecionada para aplicação tenha algum grau de nexos ou proximidade com o caso concreto não regulado.

Tartuce comenta que a analogia não pode ser confundida com a interpretação extensiva: enquanto, no primeiro caso, a competência de uma norma é rompida, permitindo a aplicação desta além do seu campo inicial de atuação, no segundo caso, “apenas amplia-se o sentido da norma, havendo subsunção” (TARTUCE, 2017).

Em síntese, a analogia é um método de integração jurídica que pressupõe o preenchimento de três requisitos para sua aplicação:

- 1) a existência de uma lacuna normativa, ou seja, um fato jurídico não regulamentado pelo legislador;
- 2) a existência de regulamentação para fato jurídico semelhante, coincidente ao fato não regulamentado/que se pretende regulamentar, mas não idêntica; e
- 3) a existência de ponto(s) em comum entre o fato não regulamentado e o fato regulamentado, e que esse aspecto comum seja o elemento central da proposta de aplicação analógica.

1.2 Justificativa da Pesquisa

Atualmente inexistente marco normativo para a utilização de Inteligência Artificial no Brasil, ainda que projetos de lei sobre estejam em tramitação. Independentemente da existência ou não de regulamentação, sistemas de IA já são uma realidade e já se encontram em utilização, tanto por entes públicos quanto por entes privados.

As IAs precisam tratar grandes quantidades de dados pessoais e/ou dados sensíveis para seu funcionamento, sendo possível identificar disfunções associadas a esse tratamento, tais como falsas correlações, discriminações estatísticas e a imputação de vieses cognitivos. Os problemas decorrentes do tratamento de dados são melhor analisados no tópico 2.1; pode-se adiantar, contudo, que possuem em comum — além do fato de

serem produtos de decisões automatizadas — um potencial atentatório aos direitos fundamentais.

Portanto, considerando-se que:

- 1) os problemas citados existem;
- 2) apesar de a maioria dos países já possuir normas próprias sobre a proteção de dados, inexistem tratados internacionais sobre os temas;
- 3) recomendações internacionais — como as da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para IA — e legislações como as da UE já observaram que o tratamento de dados pessoais é matéria de competência comum tanto às legislações que abordam a proteção de dados pessoais quanto às que versam sobre IA;
- 4) há a tendência mundial de uniformização normativa, de modo que as legislações dos mais variados temas venham a convergir;
- 5) a legislação brasileira de proteção de dados, a LGPD, possui forte semelhança com a legislação europeia sobre o tema — o RGPD — e que essa semelhança é um exemplo da supracitada tendência de uniformização normativa;
- 6) a UE já aprovou diretrizes éticas para o desenvolvimento de IAs, que estas diretrizes estão interligadas à temática da proteção de dados pessoais e pressupõem/exigem que tal proteção seja assegurada nos moldes previstos pelo RGPD

O presente estudo se propõe a analisar se é possível — perante a lacuna normativa existente — aplicar a LGPD, de forma analógica, aos sistemas de IA. Também é analisada a existência de diretrizes para regulamentar as IAs no Brasil e se essas diretrizes estão em conformidade com as normas estabelecidas na LGPD, assim como as Diretrizes Éticas para IA do Conselho Europeu estão em alinhamento com o RGPD.

Sabendo das proximidades/semelhanças entre a LGPD e o RGPD e que sistemas de IA ainda não se encontram efetivamente regulamentados² em ambos os ordenamentos (brasileiro e europeu), essas leis foram escolhidas como pontos centrais de referência para o desenvolvimento do estudo.

A sugestão de aplicação analógica que este estudo propõe visa aumentar a garantia de que esses sistemas não estão operando à margem da lei. Conforme exposto no tópico 2.1, proteger o tratamento de dados pessoais é uma forma de proteger o próprio indivíduo, o que garante uma maior segurança jurídica a operadores e usuários.

A opção pelo agrupamento contínuo dos termos “proteção” e “tratamento” pretende aludir à sua usual ocorrência subsequente ou simultânea, ainda que seus significados sejam diferentes.

No contexto do séc. XXI, uma era em que dados são enxergados como o novo petróleo³, dificilmente existem softwares automatizados que não realizam algum tipo de tratamento, seja este expresso através da coleta ou do armazenamento de dados. Ademais, ao meu entendimento, negar este tratamento é negar um fato e isso, além de errôneo, influenciaria no resultado final do estudo.

1.3 Problema de pesquisa e hipótese

O problema de pesquisa cinge em torno da ausência de uma regulamentação específica para sistemas de IA que realizam tratamento de dados pessoais. A partir da problemática apresentada, originou-se a questão a qual se pretende responder: ante a ausência de normas específicas sobre o tema (tratamento de dados por sistemas de IA), por que/é possível aplicar a LGPD a estes sistemas?

Para que o questionamento proposto seja respondido, as seguintes questões devem ser previamente sanadas:

² Por essa expressão, entenda-se “ainda não possuem normas próprias, nos moldes da LGPD ou do RGPD”.

³ <https://www.istoedinheiro.com.br/os-dados-sao-o-novo-petroleo/>
<https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html>

- 1) Por que é necessário regulamentar o tratamento de dados por sistemas de IAs?
- 2) Como essas questões (proteção e tratamento de dados pessoais e utilização de IAs) estão sendo regulamentadas internacionalmente? Existem normas internacionais sobre o tema?
- 3) Como a UE — na qual inspiramos nossa legislação de proteção de dados pessoais — regula a proteção de dados pessoais? E o tratamento desses dados por IAs? O que podemos aprender com a experiência europeia?
- 4) Como essas questões (proteção e tratamento de dados pessoais e utilização de IAs) estão sendo regulamentadas pelo Brasil?
- 5) Apesar de não ter sido desenvolvida com essa finalidade (de regulamentar IAs), a LGPD poderia ser aplicada analogicamente a esse sistemas?
- 6) Por que a LGPD foi escolhida como a norma de referência para ser utilizada nesse processo/nessa sugestão de integração analógica?
- 7) É possível a aplicação analógica da LGPD a sistemas de IA? Como essa aplicação deve ser feita?

As perguntas de número 1, 2 e 3 serão respondidas, respectivamente, nos tópicos 2.1, 2.2 e 2.3. As perguntas 4 e 5 são respondidas no tópico 2.4. Já as perguntas de número 6 e 7 são respondidas no tópico 2.5. Por fim, o capítulo 3 (Conclusão) é dedicado a apresentar os resultados obtidos.

1.4 Limitações do Estudo

Ainda que o presente estudo aborde como se deu o desenvolvimento de normas de proteção e tratamento de dados pessoais e de utilização de sistemas de IA em um contexto internacional, a tese não se debruça sobre o direito comparado.

As disposições presentes na Resolução Nº 332 de 21/08/2020 do Conselho Nacional de Justiça não são levadas em consideração por esse estudo, e isso ocorreu pois entendo que as recomendações referentes ao tratamento de dados pessoais por IAs lá presentes carecem de eficácia substancial. Conforme consta da resolução, os arts. 6 e 13 apenas determinam, respectivamente, que devem ser observadas as cautelas necessárias quanto ao tratamento de dados por IAs e que os dados devem ser provenientes de fontes seguras, mas sem definir quais seriam essas cautelas ou o que seriam fontes consideradas seguras.

2. DESENVOLVIMENTO

2.1 Por que é necessário regulamentar o tratamento de dados pessoais por IAs?

Em conformidade com o exposto no tópico 1.1.2, sabe-se que sistemas de IAs têm seu funcionamento embasado nos chamados algoritmos, que são uma “sequência de instruções que informa ao computador o que ele deve fazer” (CALABRICH, 2020). Para que essa sequência de instruções seja criada e executada, é necessário que os sistemas de IA sejam “alimentados” com quantidades massivas de dados pessoais, que posteriormente serão tratados, observando a finalidade específica do software em desenvolvimento.

Durante sua fase de criação e desenvolvimento, os dados com que a máquina tem contato apresentam-se das mais distintas formas possíveis — textos, imagens, estatísticas, gráficos etc. —, de modo que todos são levados em consideração, indistintamente, pelos sistemas de IA que realizam seu tratamento.

Em teoria, esse tratamento igualitário — que considera todas as fontes de alimentação como válidas, atribuindo a todas o mesmo valor — deveria

assegurar uma maior imparcialidade no funcionamento dos algoritmos; isso, contudo, não é o que ocorre.

Tem-se constatado que *biases* (vieses, tendências, preconceitos) dos desenvolvedores de IA, de alguma forma, são transmitidas e, conseqüentemente, reproduzidas por esses sistemas. Essa reprodução de preconceitos por parte das máquinas produz um fenômeno denominado Discriminação Estatística, e é apenas um dos possíveis problemas decorrentes do tratamento de dados pessoais.

A Discriminação Estatística é caracterizada pela “generalização de que pessoas com tais características têm maior probabilidade de agir de certa maneira ou de apresentar determinadas qualidades” (DONEDA, SCHERTEL, SOUZA e ANDRADE, 2018, p. 5). Esses autores explicam que, apesar de o método estatístico ser aplicado corretamente, ele desconsidera indivíduos “que destoam muito do padrão” — também chamados de “casos atípicos” — o que ocasiona resultados que não reproduzem fielmente a realidade ou que são totalmente alheios a ela.

Segundo CALABRICH:

Estatísticas e fórmulas podem embutir dados falsos ou imprecisos, falsas correlações — aparentes relações que não traduzem causa-efeito, com confusão entre correlação e causalidade, correlações que são frutos de pura e simples discriminação, perpetuando injustiças. [...] Dados, por si sós, não compreendem causas e efeitos; humanos sim. [...] Algoritmos podem também confirmar e naturalizar preconceitos, a depender de quais sejam seus inputs e de como os processarão (CALABRICH, 2020, p. 3).

Até o presente momento, não se sabe exatamente como impedir ou o que tem causado a transmissão — e, conseqüentemente, a reprodução — desses preconceitos dos desenvolvedores para o sistemas de IA. No entanto, observa-se maior ocorrência desse tipo de problema em casos de sistemas que se utilizam do que a nossa LGPD denomina dados pessoais sensíveis⁴.

Através de uma simples pesquisa na internet, facilmente identificam-se situações em que o tratamento de dados por sistemas de IA se tornou um

⁴ Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural

problema. Alguns dos casos mais famosos, inclusive, envolvem multinacionais da tecnologia como Google e Microsoft.

Na primeira situação, por exemplo, uma IA do aplicativo *Google Photos*, desenvolvida para realizar reconhecimento facial, sempre associava pessoas negras a gorilas ou a chimpanzés, mas nunca a pessoas. A solução ofertada pela empresa foi “apagar” o problema, retirando esses animais da base de dados da IA e, conseqüentemente, impedindo-a de continuar fazendo tal associação.⁵ Na segunda situação, um *chatbot* — desenvolvido para entreter pessoas por meio de “conversas informais e divertidas” na rede social *Twitter* — foi retirado do ar menos de 24h após sua ativação, pois começou a produzir e reproduzir ofensas e sentenças de cunho racista, misógino e até mesmo de apoio à ideologia nazista⁶.

Os exemplos citados são úteis para expor como o tratamento automatizado de grandes quantidades de dados pessoais — sensíveis ou não — pode conter erros e imprecisões, bem como refletir vieses cognitivos. Além disso, eles demonstram a necessidade do direito e da legislação em se modernizarem para resguardar os dados pessoais e prevenir tratamentos abusivos ou não autorizados.

De acordo com o entendimento de Doneda, Schertel, Souza e Andrade (2018, p. 3), exemplos como esses comprovam o potencial de violação aos direitos fundamentais das decisões automatizadas, principalmente daquelas desenvolvidas sem observar determinados parâmetros éticos e legais.

O principal objetivo da LGPD, conforme extraído de seu art. 1º, é “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, e uma das formas mais eficazes de se fazer isso é justamente coibindo que o tratamento automatizado de dados pessoais produza resultados discriminatórios.

Proteger o tratamento de dados é proteger dados pessoais, e proteger dados pessoais, por sua vez, é proteger o próprio indivíduo e sua

⁵ [Google conserta seu algoritmo “racista” apagando os gorilas](#)

⁶ [Exposto à internet, robô da Microsoft vira racista em 1 dia](#)

personalidade; isso, por si só, já são justificativas mais do que razoáveis para regulamentar essas situações.

Considerando:

- 1) os citados problemas decorrentes do tratamento de dados pessoais;
- 2) o tratamento de dados pessoais por IAs; e
- 3) a necessidade de regulamentação desses temas;

os próximos tópicos deste estudo (2.3 e 2.4) se dedicam a analisar, respectivamente, as legislações internacionais e europeias sobre os temas, de forma a examinar como essas questões são enfrentadas por outras nações e o que podemos aprender com essas experiências.

No tópico 2.3, foram selecionadas legislações com que o Estado brasileiro tenha se comprometido ou que possam ser utilizadas como referência para normativas brasileiras. Já a legislação europeia, tratada no tópico 2.4, foi selecionada não só por ser considerada por juristas como uma das mais avançadas sobre o assunto, mas principalmente pelo fato de o RGPD europeu ter servido como principal inspiração para a LGPD.

2.2 As legislações internacionais sobre proteção e tratamento de dados pessoais e utilização de IAs

Atualmente, poucos países possuem em seus ordenamentos leis que façam referência a proteção e tratamento de dados e à utilização destes por IAs, ou que tenham sido editadas para tratar especificamente sobre o tema. A maior parte das normas atualmente em vigor sobre o assunto se originaram nos chamados países desenvolvidos, o que é uma consequência direta do fato de esses países atuarem, também, como os principais produtores e receptores de fluxos de informações.

A União Europeia (UE) pode ser considerada o maior bloco de países que contêm normas em comum sobre ambas as temáticas (de proteção e tratamento de dados e de utilização de IAs). Ainda que cada país tenha autonomia para redigir suas próprias normas sobre essas matérias — respeitando suas soberanias, regionalidades, tradições etc. — e cada

ordenamento tenha suas particularidades, o que sucede na UE é a existência de um alinhamento normativo entre os países membros do bloco, o que possibilita o livre fluxo de dados entre as nações. Esse alinhamento se dá não só pela própria forma de organização e de processo legislativo da UE, mas também em razão do fenômeno de uniformização normativa que pode ser observado mundialmente.

Collin Bennett⁷ e Joel Reidenberg⁸ defendem que o movimento de uniformização normativa acentuar-se-á ainda mais após todos os países demonstrarem-se capazes de instituir condições mínimas de proteção aos dados pessoais. Os autores destacam também que a assinatura de um documento de tal espécie pressupõe e representa interesse dos governos subscritores em harmonizar suas legislações.

O sistema em vigência na UE está embasado em normas editadas pelo Parlamento Europeu e se apresenta, no cenário moderno, como o modelo que mais se assemelha a um possível tratado internacional sobre a proteção e o tratamento de dados, justamente por: 1) assegurar uma eficácia mínima à proteção de dados pessoais; 2) possuir caráter internacional/internacionalista; e 3) contemplar um número significativo de países signatários.

Ainda que o sistema europeu mostre-se o mais promissor, não pode ser considerado um tratado internacional, muito menos uma solução para os problemas atinentes à proteção e ao tratamento de dados a nível internacional

Por fim, segundo Doneda:

“No momento, não podemos identificar normas ou tratados de âmbito internacional ou global que se dirijam direta e eficazmente ao problema da proteção de dados pessoais. Temos, sim, uma série de normativas de âmbito nacional, além de instrumentos internacionais restritos a blocos de países”. (DONEDA, 2020)

⁷ BENNETT, Collin. *Regulating Data, Privacy Protection and Public Policy in Europe and the United States*. Ithaca, Cornell University Press, 1992

⁸ REIDENBERG, Joel. *E-commerce and transatlantic privacy*. *Houston Law Review* 717, 2001.

Em relação às regulamentações de sistemas de IA, tanto a UE quanto a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) emitiram diretrizes para a sua utilização, pois ambos já haviam constatado que editar uma legislação específica sobre o assunto era tarefa necessária⁹ para diminuir a incidência de erros capazes de gerar violações a direitos fundamentais.

Neste tópico, o objeto de análise será limitado às orientações expedidas pela OCDE, tendo em vista que a regulamentação de IA pela União Europeia é objeto de discussão do tópico 2.3 deste estudo.

O Conselho sobre Inteligência Artificial da OCDE estabeleceu, em maio de 2019, uma recomendação¹⁰ para o desenvolvimento de IAs, incluindo uma série de princípios a serem adotados ao se elaborar esses sistemas. O Brasil, junto a governos de 41 países, foi um dos signatários, ainda que não seja membro da referida Organização — tamanha sua relevância.

Visando uma IA mais confiável e transparente, os assinantes da cartilha em questão se comprometem a promover e implementar os seguintes princípios:

- I) o desenvolvimento de IAs deve se dar de forma sustentável e inclusiva, buscando o bem-estar social e um crescimento inclusivo;
- II) a IA deve respeitar os Direitos Humanos, o Estado de Direito e os valores democráticos, contribuindo para uma sociedade mais justa e imparcial;

9

<https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming/?sh=7b9e24f9a2b4>
<https://www.ft.com/content/025315e8-7e4d-11e9-81d2-f785092ab560>
<https://www.loc.gov/law/help/artificial-intelligence/international.php>

¹⁰ Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, 2020. Disponível em: <<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>>. Acesso em: 19 de set. de 2020.

III) o desenvolvimento e funcionamento de IAs deve ocorrer de forma transparente;

IV) sistemas de IA precisam operar de forma segura, e, para isso, riscos potenciais devem ser continuamente avaliados e suprimidos; e

V) a responsabilidade pelo desenvolvimento e implementação de uma IA deve ser dos indivíduos ou empresas que a criaram ou a operam.

Ainda que não possuam força normativa e sua inobservância não acarrete nenhum tipo de sanção, os princípios aqui apresentados buscam estabelecer referenciais éticos para o desenvolvimento de sistemas de IA, de maneira que os países comprometidos com as citadas recomendações disponham de algum tipo de orientação para quando forem tratar sobre o tema em seus respectivos territórios.

Até o presente momento, poucos Estados se dedicaram a legislar sobre a IA e nenhum país possui uma regulamentação forte ou efetiva sobre o tema. Notoriamente, países que já se dedicam a fomentar o desenvolvimento e estabelecer regulamentações para IAs estão um passo à frente dos que ainda nem discutiram o assunto.

De qualquer forma, a realidade é a de que não há qualquer tipo de tratado ou normas internacionais que regulem as temáticas de Sistemas de IA ou de Dados Pessoais e seu tratamento, apenas diretrizes e orientações. As fontes de inspiração para uma legislação nacional, portanto, são poucas, e a possibilidade de uniformização normativa sobre esses temas em um nível internacional é menor ainda.

2.3 As legislações europeias sobre proteção e tratamento de dados pessoais e utilização de IAs

Em consonância com as informações expostas no tópico anterior, atualmente, as normas de proteção de dados pessoais sancionadas pelo Parlamento Europeu são vistas por estudiosos como as mais avançadas em vigor, e se mostram efetivamente capazes de implementar um nível pequeno

— mas relevante o suficiente para ser considerado referência — de segurança aos dados pessoais.

A proteção e o tratamento de dados na União Europeia, hoje, encontram-se compilados e uniformizados pelo Regulamento 2016/679, também conhecido por *General Data Protection Regulation* (GDPR, ou RGD — Regulamento Geral para a Proteção de Dados).

Conforme seu art. 2º, “1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados”¹¹, de maneira que a competência dessa legislação engloba qualquer operação que envolva a utilização de dados pessoais, seja ela realizada de forma manual ou automatizada.

A competência territorial do RGD compreende todos os países membros da UE e regulamenta praticamente toda a temática de proteção e tratamento de dados nesses Estados. Resta às nações da UE competência para legislar apenas sobre questões declaradamente atribuídas pelo RGD, tais como, a notificação de violação de dados pessoais ou a transferência de dados a países terceiros (ambas previstas no art. 40º do Regulamento).

A proteção de dados é vista pela UE como um tema de direitos humanos, estando intrinsecamente conectada ao direito à privacidade que, por sua vez, é considerado um direito fundamental e um dos pressupostos de um Estado democrático (DONEDA, 2020).

A proteção às pessoas — e, portanto, aos seus dados pessoais — é uma obrigação de todas as nações europeias, sendo essencial para garantir a livre circulação das primeiras nas segundas. Uma vez que a referida livre circulação, no contexto europeu, é um dos objetivos finalísticos da própria UE, fica claro o porquê da preocupação com a existência de uma legislação sistematizada e uniformizada para os países membros do bloco.

¹¹ <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>, p. 32

Em relação à Inteligência Artificial, constata-se que a União Europeia ainda não sancionou um Regulamento geral sobre o tema, nos moldes do realizado com a temática de proteção e tratamento de dados. A inexistência de uma regulamentação geral não é sinônimo, contudo, de ausência de regulamentação: além de países como Alemanha, Holanda, Itália, Reino Unido já possuírem suas próprias estratégias nacionais¹², a Comissão Europeia¹³ publicou, em abril de 2019, um documento que estabeleceu diretrizes éticas para instruir o desenvolvimento desses sistemas.

Essas diretrizes objetivam a criação da intitulada “*trustworthy AI*” (“IA confiável e segura”¹⁴), estabelecendo, para isso, três critérios: 1) devem estar em conformidade/observância com a Lei; 2) deve cumprir princípios éticos; e 3) devem ser robustas.

Conforme determinado pela Comissão Europeia, para que os sistemas de IA possam atingir os parâmetros fixados e serem considerados como seguros e confiáveis (“*trustworthy*”), estes devem se submeter aos seguintes “requisitos-chave” (“*key requirements*”):

I) *Human agency and oversight* (“Supervisão Humana”): o desenvolvimento e a utilização de IAs devem ser sempre supervisionados, de forma que a autonomia humana e os direitos fundamentais não possam ser ignoradas ou subjugadas por ocasião do funcionamento desses sistemas.

II) *Technical robustness and safety* (“Robustez Técnica e Segurança”): sistemas de IAs devem ser “seguros e confiáveis” (“*trustworthiness on IA*”), de forma que sejam capazes de prever, evitar e, caso necessário, corrigir eventuais erros por eles cometidos.

III) *Privacy and Data Governance* (“Privacidade e Governança de Dados”): a proteção aos dados pessoais — e, conseqüentemente, a privacidade dos indivíduos — deve ser garantida em todos os seus estágios de tratamento/utilização. Ademais, o acesso a esses dados

¹² http://eur-ws.org/Vol-2771/AICS2020_paper_53.pdf

¹³ Órgão responsável por propor legislações e políticas públicas, além de ser responsável por aplicar as decisões do Parlamento Europeu (PE) e o Conselho da União Europeia (CUE).
Fonte: https://ec.europa.eu/info/about-european-commission/organisational-structure_pt

¹⁴ Tradução minha;

personais deve ser controlado e limitado somente a seus titulares ou aqueles com direito de utilizá-los.

IV) *Transparency* (“Transparência”): sistemas de IA devem ser transparentes, ou seja, devem ser capazes de explicar os fundamentos utilizados para a tomada de uma decisão. Ademais, nessa obrigatoriedade das IAs em fornecer a explicação para suas decisões, está incluído também o ônus de fornecer os argumentos e documentos por elas utilizados na elaboração.

V) *Diversity, non-discrimination and fairness* (“Diversidade, não discriminação e justiça”): tanto dados pessoais utilizados por sistemas de IA quanto o processo de tratamento dos dados por esses sistemas podem ser influenciados por vieses, o que acarretaria situações de discriminação, ainda que não intencional. É necessário, portanto, que IAs possuam equipes de desenvolvimento etnicamente diversas, além de assegurar a participação da maior quantidade possível de cidadãos no processo.

VI) *Societal and environmental well-being* (“Responsabilidade Social e Ambiental”): o desenvolvimento e utilização de IAs deve ser realizado de forma ecologicamente sustentável. Além disso, possíveis impactos do emprego de IAs devem sempre ser levados em consideração, principalmente quando essa utilização se der em contextos relacionados a processos eleitorais e democráticos, formação de opiniões e/ou decisões políticas.

Alguns requisitos chave (como os de número III, IV e V) claramente são similares a previsões contidas no RGPD e devem ser observados por sistemas de IA que operam em território europeu.

Essa semelhança de previsões ocorre porque, no ordenamento europeu, as temáticas da proteção de dados e do tratamento desses por IAs estão intrinsecamente conectadas. O legislativo europeu — ao contrário do brasileiro, conforme exposto no tópico 2.4 — já identificou esses fatos, fazendo questão de garantir que as legislações de ambas as temáticas estejam em harmonia e tenham a mesma finalidade.

Conforme exposto no tópico 2.2, o alinhamento normativo entre legislações não é coincidência, e já foi observado por autores como Bennett, Doneda e Reidenberg no estudo da proteção de dados pessoais. Ainda que os referidos estudiosos tenham constatado a tendência de “uniformização normativa internacional”, principalmente nas legislações de proteção e tratamento de dados, o fenômeno não é algo novo nem restrito somente a essa temática¹⁵. O que se observa agora é apenas uma extensão desse fenômeno, de forma a abarcar também a regulação dos sistemas de IA.

Além disso, apesar de tanto o Brasil quanto a UE não possuírem normas específicas sobre a utilização de IAs, pode-se verificar que os níveis de regulamentação da UE sobre a temática se encontram mais avançados, e as citadas diretrizes éticas são um exemplo disso.

Embora uma regulamentação “mais forte” não impeça os países membros da UE de sofrerem com problemas inerentes à proteção de dados ou sistemas de IAs — como os megavazamentos¹⁶ de dados ou IAs influenciadas por um *bias/viés* cognitivo¹⁷ — suas ocorrências são muito menos frequentes e/ou causam danos menores em nações europeias que contam com esse tipo de regulamentação do que nas que possuem uma regulamentação mais permissiva ou nenhuma regulamentação.

2.4 As leis brasileiras sobre proteção e tratamento de dados pessoais e utilização de IAs

Em consonância com o exposto em tópicos anteriores, sabe-se que a existência de legislações que versam de forma específica e sistemática sobre proteção e tratamento de dados pessoais é um fenômeno relativamente recente. O caso brasileiro não é diferente: a atual legislação sobre proteção

¹⁵ É fato notório a existência de documentos (tais como Acordos, Cartilhas, Tratados etc.) internacionais regulando os mais diferentes assuntos — da circulação de mercadorias à extradição de pessoas, de normas sobre viagens internacionais à imposição de embargos econômicos etc. Esses tipos de acordos entre nações ocorrem desde que estas surgiram, sendo possível observar que a uniformização de suas legislações sobre um determinado assunto — quando não constitui o próprio objeto do acordo — é a consequência mais comum da celebração deste.

¹⁶ sobre vazamentos de dados na UE:

¹⁷ Sobre sistemas IA e *bias*es:

de dados pessoais — unificada em torno de uma norma específica, a LGPD — só passou a vigorar em setembro de 2020.

A temática da proteção de dados pessoais no Brasil pode ser dividida em dois momentos: um anterior e um posterior à denominada “compreensão jurídica da internet”. Segundo Fortes (2016, p. 109, apud DIAS e BOLESINA, 2017, p. 6), esse fenômeno é uma consequência da democratização e popularização do acesso à internet — que começaram no início dos anos 2000 — e foi responsável por mudar o debate jurídico em torno dela, a qual passou a ser enxergada “como fator hermenêutico, isso é, como um elemento que deve ser avaliado na interpretação do Direito”.

No primeiro momento, anterior ao fenômeno da compreensão jurídica da internet, o ordenamento jurídico brasileiro até contava com a existência de normas que versavam sobre a proteção dos dados pessoais, como algumas disposições constitucionais principiológicas (tais como direitos à privacidade, acesso à informação, inviolabilidade de comunicações etc.), o *Habeas Data*¹⁸ e o art. 43 do Código de Defesa do Consumidor (CDC)¹⁹. Ainda que as referenciadas normas ofereçam um ponto de partida para a temática da proteção de dados pessoais em nosso ordenamento, não consideraram — seja durante a elaboração/tramitação de seus projetos, seja depois de sancionadas — os possíveis impactos do tratamento e/ou da utilização abusiva de dados pessoais²⁰.

¹⁸ Sobre o tema, Doneda (2020) comenta que: “[...] a Constituição brasileira contemplava o problema da informação, de início, por meio das garantias à liberdade de expressão e do direito à informação. Além disso, a Constituição considera invioláveis a vida privada e a intimidade (art. 5º, X), estabelece a garantia da inviolabilidade especificamente para a interceptação de comunicações telefônicas, telegráficas ou de dados (art. 5º, XII), bem como institui o *Habeas Data* (art. 5º LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. A Constituição ainda protege uma série de aspectos relacionados à privacidade, proibindo a invasão de domicílio (art. 5º, XI) e a violação de correspondência (art. 5º, XII).”

¹⁹ Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

²⁰ Se pararmos para refletir, essa preocupação é incabível/inexistia à época. O fenômeno de se reconhecer uma pessoa “pela representação de sua personalidade que é fornecida pelos seus dados pessoais” (DONEDA, 2020) é recente, característico do momento pós compreensão jurídica da internet. Impossível ao legislador de um período totalmente distinto do nosso — que seria o da era pré-popularização da internet — prever todos os possíveis problemas dela decorrentes, e muito menos a forma como se desenvolveriam.

Já no segundo e atual momento — do qual podemos citar, a título exemplificativo, a Lei de Acesso à Informação Pública (Lei 12.527/2011) e o Marco Civil da Internet (Lei n. 12.965/2014) —, constata-se que normas que dispõem sobre a proteção (e, conseqüentemente, tratamento) de dados pessoais já são editadas levando em consideração possíveis utilizações abusivas de dados pessoais.

Schertel (2019, p. 45) fundamenta que essa mudança legislativa baseia-se “na ideia de que não existem mais dados irrelevantes em face do processamento automatizado e ubíquo de dados na sociedade da informação”. Dias e Bolesina (2017, p. 4) adotam entendimento semelhante, alegando que tal alteração do entendimento legislativo ocorreu pois a internet passou a ser vista como um “fator hermenêutico”, digna de uma legislação própria.

Verifica-se que, até a concepção da LGPD, em 2018, inexistia no Brasil uma norma editada para discorrer especificamente sobre os temas da proteção e tratamento de dados. Ainda que houvesse leis que tratassem de tópicos pertinentes ao assunto, essas o faziam de forma parcial, fragmentada, o que não fornecia um nível adequado de proteção e aumentava a insegurança jurídica. A LGPD, portanto, é o produto da primeira experiência de “sistematização legislativa” das normas referentes à proteção de dados pessoais no Brasil.

A maior inovação produzida por esta Lei foi a criação e o estabelecimento do denominado “modelo *ex ante* de proteção de dados”. Idealizado e concebido no contexto atual da sociedade da informação, esse modelo fundamenta-se nas premissas-base de que: 1) inexistem dados pessoais insignificantes; e 2) dados pessoais constituem uma forma de representação do indivíduo perante a sociedade (conforme explicado no tópico 1.1.1); e defende que o tratamento de dados pessoais, “por influenciar na representação da pessoa na sociedade, pode afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais” (SCHERTEL, 2019, p. 45).

Conforme já mencionado nos tópicos 1.1.3 e 1.2, a LGPD inspira-se fortemente” no RGPD europeu, compartilhando disposições semelhantes com este (como as que abordam o processamento de dados ou as decisões automatizadas).

A LGPD foi a primeira lei que assegurou uma eficácia horizontal na temática do tratamento de dados, ou seja: foi a primeira norma a instituir que o respeito aos direitos fundamentais durante o tratamento deve ser observado tanto no contexto das relações particular-Estado quanto na das relações particular-particular. Essa lei também introduziu ao ordenamento brasileiros conceitos importantes, tais como os relativos aos Dados Pessoais Sensíveis e Anônimos, Bancos de Dados, Tratamento de dados, Transferência internacional de dados, entre outros.

A proteção e o tratamento de dados pessoais são temas recentes, que desafiam legisladores do mundo todo. Apesar disso, observa-se que a legislação brasileira sobre o assunto está atualizada e em consonância com as legislações consideradas mais desenvolvidas, até mesmo utilizando-as como referência, como a legislação da própria UE. O mesmo, contudo, não pode ser dito das normas que falam sobre IA.

Atualmente, sistemas de IA em utilização no Brasil não possuem nenhuma regulamentação específica; essa lacuna legislativa ocorre em razão da própria morosidade do processo legislativo e da ausência de interesse/prioridade do legislador. Por outro lado, já existem Projetos de Lei que dispõem sobre o tema, tais como os PLs 5051/2019²¹ e 21/2020²², os quais ainda devem demorar um tempo considerável até serem aprovados e entrarem em vigor.

Apesar da existência desses PLs, a lacuna normativa sobre IA persiste em nosso ordenamento e, até que normas específicas sobre IAs sejam aprovadas, poder público e iniciativa privada continuarão tratando dados pessoais para projetar, desenvolver e utilizar sistemas de IA.

²¹ [PL 5051/2019;](https://bernardodeazevedo.com/conteudos/projeto-de-lei-institui-a-politica-nacional-de-inteligencia-artificial/)
[https://bernardodeazevedo.com/conteudos/projeto-de-lei-institui-a-politica-nacional-de-inteligencia-artificial/;](https://bernardodeazevedo.com/conteudos/projeto-de-lei-institui-a-politica-nacional-de-inteligencia-artificial/)

²² [PL 21/2020 — Portal da Câmara dos Deputados - Portal da Câmara dos Deputados;](#)
[Projeto cria marco legal para uso de inteligência artificial no Brasil - Notícias;](#)

Ciente da necessidade de regulamentação²³ e em consonância com o compromisso internacional assumido²⁴, o Ministério da Ciência, Tecnologia e Inovações brasileiro publicou, em 6 de abril de 2021, a Estratégia Brasileira de Inteligência Artificial (EBDIA). Instituída em consonância com as Recomendações da OCDE e das Diretrizes da UE para IA, a EBDIA tem como finalidade “nortear as ações do Estado brasileiro em prol do fortalecimento da pesquisa, desenvolvimento e inovações de soluções em Inteligência Artificial”²⁵ e “garantir a inovação no ambiente produtivo e social na área de Inteligência Artificial”²⁶.

Ainda que a EBDIA estabeleça um mínimo de orientação para o Estado e para operadores, não possui qualquer força vinculante e/ou previsão de penalidade para casos de sua não observância, constituindo, portanto, meras diretrizes.

2.5 É possível uma aplicação analógica da LGPD a sistemas de IA? Como deve ser realizada?

Reconhecendo:

- 1) a lacuna normativa exposta/existente;
- 2) o potencial de violação a direitos fundamentais existente, derivado da citada lacuna;
- 3) que o desenvolvimento de sistemas de IA deve estar em consonância e alinhamento com as normas de proteção de dados pessoais já em vigência; e
- 4) que o principal objetivo da LGPD é “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”²⁷;

²³ Vide tópico 2.1;

²⁴ Vide tópico 2.2;

²⁵ Inciso I, art. 1º da EBDIA;

²⁶ Inciso II, art. 1º, EBDIA;

²⁷ LGPD, art. 1º;

o presente estudo propõe que a LGPD seja aplicada de forma analógica aos sistemas de IA. Essa aplicação analógica pretende assegurar que IAs observarão as normas de proteção de dados pessoais, atenuando ou até mesmo prevenindo que o tratamento automatizado de dados pessoais por esses sistemas produza resultados discriminatórios e/ou atentatórios a direitos fundamentais.

A escolha da LGPD como a norma de referência a ser utilizada no processo de integração analógica não se deu aleatoriamente, mas sim fundamentada em sua proximidade com o ordenamento europeu, suas disposições sobre o tratamento de dados e no fato deste já estar em vigência.

Conforme exposto no tópico 1.1.4, a aplicação analógica exige o preenchimento de três requisitos, quais sejam:

- 1) existência de lacuna normativa, de um fato jurídico não regulamentado pelo legislador;
- 2) existência de regulamentação para fato jurídico semelhante ao fato não regulamentado/que se pretende regulamentar, mas não idêntica a ele; e
- 3) existência de ponto(s) em comum(ns) entre o fato não regulamentado e o fato regulamentado.

Como exposto ao longo deste trabalho, esses requisitos encontram-se preenchidos.

A intenção do presente trabalho, contudo, não é comentar artigo por artigo da LGPD, mas sim analisar se algum desses — e quais — são aplicáveis a sistemas de IA, quando da realização do tratamento de dados por estes.

Considerando a lacuna existente quanto à regulamentação do tratamento de dados pessoais por IAs (vide tópico 2.1), ao preenchimento dos requisitos para aplicação analógica e à finalidade da LGPD (exposto em seu art. 1º) — e até mesmo as diretrizes fixadas na EBDIA — sugere-se que

os seguintes artigos da LGPD sejam aplicados aos sistemas de IA que realizam o tratamento de dados:

- art. 1º, que dispõe sobre os objetivos e motivos para a existência de uma lei que trate sobre proteção e tratamento de dados pessoais;
- art. 2º, que dispõe quais são os fundamentos para a disciplina da proteção dos dados pessoais;
- arts. 3º e 4º, que dispõem, respectivamente, sobre os casos em que as normas de proteção de dados pessoais devem e não devem ser aplicadas;
- art. 5º, que expõe os principais conceitos utilizados/referenciados na disciplina de proteção e tratamento de dados pessoais;
- art. 6º, que dispõe os princípios que devem ser observados durante o tratamento de dados;
- art. 7º, que delimita as possibilidades em que o tratamento de dados pessoais podem ocorrer;
- art. 9º, que dispõe que as informações relativas ao tratamento de dados pessoais devem estar facilmente acessíveis a seus titulares, além de serem disponibilizadas de forma clara, adequada e ostensiva;
- art. 11, que delimita as possibilidades em que o tratamento de dados pessoais sensíveis pode ocorrer;
- art. 12, que dispõe que dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido;
- art. 15, que explicita as hipóteses que acarretam o término do tratamento de dados pessoais;
- art. 16, que dispõe que os dados pessoais devem ser eliminados após o término de seu tratamento e também elenca as exceções a essa obrigatoriedade;

- art. 20, que dispõe que o titular dos dados tem direito de solicitar a revisão de decisões resultantes do tratamento automatizado de dados pessoais capazes de afetar seus interesses; e
- arts. 23 e 24, que dispõem sobre o tratamento de dados pessoais pelos integrantes da administração pública direta e indireta.

3. CONCLUSÃO

Conforme exposto ao longo do texto, as temáticas de proteção e tratamento de dados pessoais e de utilização de sistemas de IA estão intimamente conectadas. Inexistem IAs que funcionem sem quantidades massivas de dados, assim como, no contexto do século XXI, inexistente tratamento de dados que não seja realizado por um sistema automatizado.

O legislador brasileiro precisa entender que a elaboração de normas sobre sistemas de IA pressupõe e necessita da existência prévia de normas eficazes sobre proteção e tratamento de dados, visto que um não pode ocorrer sem o outro. Nesse sentido, considerando 1) a já vigência de uma norma sobre proteção de dados pessoais; e 2) a inexistência de normas sobre IAs, este estudo se dedicou a verificar a possibilidade de uma aplicação analógica da LGPD a esses sistemas, de modo que sua viabilidade se mostra confirmada.

Esta pesquisa, obviamente, foi desenvolvida sem a pretensão de se esgotar o debate sobre o tema, porém consciente de que proteger o tratamento de dados é proteger dados pessoais, e proteger dados pessoais, por sua vez, é proteger o próprio indivíduo e sua personalidade.

Deve-se destacar que a aplicação analógica sugerida não é a solução ideal para a lacuna atualmente existente no ordenamento jurídico pátrio. A presente proposta visa evitar ou pelo menos diminuir os danos ou resultados discriminatórios que podem ocorrer no processo de tratamento automatizado de dados pessoais por IAs. Nesse sentido, Danilo Doneda escreveu:

A classificação dos dados pessoais e uma consequente determinação das categorias de dados que se prestariam ou não a

um determinado tratamento é útil para dinamizar a disciplina e facilitar a delimitação dos tratamentos de dados que devam estar sujeitos a um maior controle ou até mesmo vetados. Essa classificação, porém, não deve ser absoluta nem funcionar como última instância de legitimação do tratamento de dados, haja vista que a imensa variedade de ambientes, finalidades e técnicas utilizadas podem determinar uma natureza ofensiva mesmo no tratamento de dados que, originariamente, não eram qualificados como “dados sensíveis” (DONEDA, 2020)

Ademais, conforme destacado ao longo do texto, observa-se um fenômeno de convergência internacional dos ordenamentos em relação a diversos assuntos, e não tem sido diferente para os temas de proteção e tratamento de dados e utilização de IAs.

REFERÊNCIAS BIBLIOGRÁFICAS

ARTICLE 19; PRIVACY INTERNATIONAL. Privacy and the Freedom of Expression in the Age of Artificial Intelligence. 2018.

ATHENIENSE, Alexandre Rodrigues; RESENDE, Tatiana Carneiro. A inteligência artificial e outras inovações tecnológicas aplicadas ao direito. In: FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gamba Prata de (Coord.). Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia - 2017. Belo Horizonte: Fórum, 2018. p. 69-96. ISBN 978-85-450-0453-0.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 02 de set. de 2020.

Brasil. Escola Nacional de Defesa do Consumidor. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010.

BENNETT, Collin. Regulating Data, Privacy Protection and Public Policy in Europe and the United States. Ithaca, Cornell University Press, 1992.

CARVALHO, Angelo Gamba Prata de. Juristas e ludistas no século XXI: a realidade e a ficção científica do discurso sobre o futuro da advocacia na era da informação. In: FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gamba Prata de (Coord.). Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia - 2017. Belo Horizonte: Fórum, 2018. p. 185-199.

CALABRICH, Bruno Freire de Carvalho. Discriminação algorítmica e transparência na Lei Geral de Proteção de Dados pessoais. Revista de Direito e as Novas Tecnologias | vol. 8/2020 | Jul - Set / 2020

DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados. 2 ed, São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo C. M.; SCHERTEL, Laura M.; SOUZA, Carlos A. P.; ANDRADE, Norberto N. G. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. Pensar - Revista de Ciências Jurídicas 23(04):1-17, 2018.

GARCIA, Eugênio V. Inteligência Artificial, Paz e Segurança: Desafios para o Direito Internacional Humanitário. Cadernos de Política Exterior nº 8 Instituto de Pesquisa de Relações Internacionais (IPRI), 2019.

GUARIENTO, Daniel Bittencourt; MARTINS, Ricardo Maffeis. PL 21/2020: a criação de um marco legal é apenas o primeiro passo para a sustentabilidade da inteligência artificial no Brasil. Migalhas, 08 de mai. de 2020. Disponível em:

<https://migalhas.uol.com.br/coluna/impressoes-digitais/326369/pl-21-2020--a-criacao-de-um-marco-legal-e-apenas-o-primeiro-passo-para-a-sustentabilidade-da-inteligencia-artificial-no-brasil>>. Acesso em: 05 de mar. de 2021.

JOBIN, Anna; IENCA, Marcello; VAYENA, Effy. Artificial Intelligence: the global landscape of ethics guidelines. Health Ethics & Policy Lab, ETH Zurich, 2019.

LOC. Library of Congress, 2019. Regulation of Artificial Intelligence: International and Regional Approaches. Disponível em: <https://www.loc.gov/law/help/artificial-intelligence/international.php>>. Acesso em: 11 de fev. de 2021.

LOC. Library of Congress, 2019. Regulation of Artificial Intelligence: The Americas and The Caribbean. Disponível em: <https://www.loc.gov/law/help/artificial-intelligence/americas.php#_ftnref67>. Acesso em: 11 de fev. de 2021.

MARCONDES, PYR. Qual a diferença entre inteligência Artificial, *Machine Learning* e *Deep Learning*? Proxima, 08 de mar. de 2017. Blog do Pyr. Disponível em: <<https://www.proxima.com.br/home/proxima/blog-do-pyr/2017/03/08/qual-a-diferenca-entre-inteligencia-artificial-machine-learning-e-deep-learning.html>>. Acesso em: 02 de mai. de 2020.

MEDVEDEVA, Masha; VOIS, Michael; WIELING, Martijn. Using machine learning to predict decisions of the European Court of Human Rights, 2020.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. Caderno Especial LGPD. p. 35-56. São Paulo: Ed. RT, novembro 2019.

MURGIA, Madhumita; SHRIKANTH, Siddarth. How governments are beginning to regulate AI. Financial Times, Londres/Hong Kong, 30 de mai. de 2019. Disponível em: <<https://www.ft.com/content/025315e8-7e4d-11e9-81d2-f785092ab560>>. Acesso em: 16 de abr. de 2021.

OECD Principles on IA. OECD.org, 2020. Disponível em: <<https://www.oecd.org/going-digital/ai/principles/#:~:text=The%20OECD%20Principles%20on%20Artificial,Council%20Recommendation%20on%20Artificial%20Intelligence.>>. Acesso em: 05 de out. de 2020.

PIERCE, Jadzia. *President Trump signs Executive Order on Artificial Intelligence*. *Inside Privacy*, 11 de fev. de 2019. *Artificial Intelligence (AI); Data Privacy*. Disponível em: <https://www.insideprivacy.com/data-privacy/president-trump-signs-executive-order-on-artificial-intelligence/?_ga=2.164284666.496501142.1619457246-1259581809.1618090108>. Acesso em: 25 de mai. de 2021.

Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, 2020. Disponível em: <<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>>. Acesso em: 19 de set. de 2020.

REIDENBERG, Joel. E-commerce and transatlantic privacy. *Houston Law Review* 717, 2001.

RIGHT, Jasmine; VERITY, Andrej. *Artificial Intelligence Principles for Vulnerable Populations in Humanitarian Contexts*, 2020.

RIGUEIRA, Marina. Qual é a diferença entre AI, *machine learning* e *deep learning*. *IMasters*, 13 de mar. de 2017. Disponível em: <<https://imasters.com.br/desenvolvimento/qual-e-diferenca-entre-ai-machine-learning-e-deep-learning/?trace=1519021197&source=single>>. Acesso em: 02 de mar. de 2021.

SILVA, Nilton Correia da. Notas iniciais sobre a evolução dos algoritmos do VICTOR: o primeiro projeto de inteligência artificial em supremas cortes do mundo. In: FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (Coord.). *Tecnologia jurídica & direito digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018*. Belo Horizonte: Fórum, 2018. p. 89-94. ISBN 978-85-450-0584-1.

SOUSA, Maria Eliane Alves de. Direitos humanos e princípios comuns entre inteligência artificial e direito à saúde. Cadernos Ibero- Americanos de Direito Sanitário. 2020 jul./set.; 9(3): 26 - 48.

TARTUCE, Flávio. Manual de direito civil: volume único. 7. ed. rev., atual. e ampl. - Rio de Janeiro; Forense; São Paulo: MÉTODO, 2017.

THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN. The Networking and Information Technology Research and Development - NITRD Program, out. de 2016. Disponível em: <https://www.nitrd.gov/news/national_ai_rd_strategic_plan.aspx>. Acesso em: 02 de fev. de 2021.

VALENTE, Jonas. Europa lança diretrizes éticas para uso de Inteligência Artificial. Agência Brasil, 13 de abr. de 2019. INTERNACIONAL. Disponível em: <<https://agenciabrasil.ebc.com.br/internacional/noticia/2019-04/europa-lanca-diretrizes-eticas-para-o-uso-da-inteligencia-artificial>>. Acesso em: 19 de jan. de 2021.

WALCH, Kathleen. AI laws are coming. Forbes, 20 de fev. de 2020. COGNITIVE WORLD. Disponível em: <<https://www.forbes.com/sites/cognitiveworld/2020/02/20/ai-laws-are-coming/?sh=7b9e24f9a2b4>>. Acesso em: 09 de mar. de 2021.

ZADONAI, Amanda Closs; ARGILES, André Vátimo. Incidente de segurança: o vazamento de dados de clientes do Banco Inter sob a perspectiva da Lei 13.709/2018