INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 04 · n. 01 · janeiro/abril 2023 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.4.n.1

04

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

IJDL – INTERNATIONAL JOURNAL OF DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM
Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Rua Paulo Ribeiro Bastos, 211 – Jardim Atlântico – CEP 31710-430
Belo Horizonte/MG – Brasil – Tel.: (31) 99412.0131
www.editoraforum.com.br / E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil / Distribuída em todo o Território Nacional

IN61 International Journal of Digital Law – IJDL. – ano 1, n. 1 (abr. 2020) –.– Belo Horizonte: Fórum, 2020-.

Quadrimestral; Publicação eletrônica
ISSN: 2675-7087

1. Direito. 2. Direito Digital. 3. Teoria do Direito. I. Fórum.

CDD: 340.0285
CDU: 34.004

Coordenação editorial: Leonardo Eustáquio Siqueira Araújo
Aline Sobreira
Capa: Igor Jamur
Projeto gráfico: Walter Santos

Sumário
Contents

EDITORIAL 5

EDITORIAL 7

O devido processo tecnológico na prestação de serviços digitais (tratamento de conteúdo digital) sob responsabilidade das *big techs*

The technological due process in the provision of digital services (digital content treatment) under the responsibility of big techs

Ricardo de Holanda Melo Montenegro 9

1 Introdução 10
2 Lacunas regulatória e legislativa para serviços digitais 13
3 Devido processo tecnológico 17
3.1 Panorama internacional sobre regulação de serviços digitais 24
3.2 Exemplo de ausência de transparência no tratamento de conteúdo digital 26
3.3 Proposta de eixos estruturantes para tratamento de conteúdo digital 26
4 Considerações finais 30
Referências 33

Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT

The challenges regarding the preservation of privacy and data protection in the face of the IoT equipment

Vivian Lima López Valle, Bruna Gavron Barbosa 35

1 Introdução 36
2 A relevância da *internet* na sociedade de informação 37
3 Os direitos fundamentais à privacidade e à intimidade na Constituição de 1988 39
4 O tratamento de dados por meio da Lei Geral de Proteção de Dados como forma de preservar o direito à privacidade 42
5 A proteção da privacidade nos dispositivos IoT com base na Lei Geral de Proteção de Dados 48
6 Caso iRobot – aquisição da iRobot pela Amazon 53
7 Conclusões 56
Referências 58

Hipótese de tratamento de dados sensíveis: dado biométrico e relação de trabalho

Sensitive data processing hypothesis: biometric data and work relationship

Rafael Tedrus Bento 63

1 Introdução 64

2 Por existirem dois outros meios de controle de ponto, seria o tratamento de dado biométrico cumpridor do princípio da necessidade? 68

3 O General Data Protection Regulation e o dado biométrico 69

4 Conclusão 73

Referências 74

La Inteligencia Artificial: Una herramienta que revoluciona la compra pública

Artificial Intelligence: A tool that revolutionizes public procurement

Juan Francisco Diaz Colmachi 77

1 Introducción 78

2 La Inteligencia Artificial 79

3 Aplicación de la Inteligencia Artificial 80

4 La Inteligencia Artificial en la contratación pública 81

5 Conclusiones 83

Referencias 84

Avances de la administración colombiana en la era digital

Advances of the Colombian administration in the digital age

Augusto Hernández Becerra 87

1 Introducción 88

2 Hacia la digitalización de la Administración de Colombia 89

2.1 Las primeras leyes 90

2.2 Creación del Ministerio de Tecnologías de la Información y las Comunicaciones 90

2.3 La reforma de los procedimientos administrativos en 2011 91

2.4 Leyes contra la corrupción 92

2.5 Legislación sobre publicidad de los actos oficiales 94

6 Legislación sobre transparencia 95

4.7 La política de Gobierno abierto o Estado abierto 98

2 En las fronteras de la Inteligencia Artificial 100

3 Conclusiones 103

Referencias 105

SOBRE A REVISTA 107

DIRETRIZES PARA AUTORES 109

Condições para Submissões 115

Política de Privacidade 116

Author Guidelines 119

Conditions for submissions 125

Privacy statement 126

EDITORIAL

Chegamos ao décimo número da *International Journal of Digital Law*. Conforme anunciado no editorial anterior, a *IJDL*, mesmo sendo um periódico iniciante, já é uma das revistas mais citadas na área, conforme as métricas do Google.

Procuramos, nesta edição, manter o critério inovador e dar ênfase a artigos que tratem da tecnologia e do direito a partir de pressupostos éticos e conscientes. A tarefa de consolidação dos pressupostos da Constituição de 1988 se mantém como mote das pesquisas que interessam à revista.

Os artigos versam, de forma aprofundada e cuidadosa, sobre temas sensíveis, como devido processo legal digital, responsabilidade das *big techs*, direito à privacidade, proteção de dados, inteligência artificial, dados biométricos e modernização da administração pública.

Como sempre, reitero meus agradecimentos à Editora Fórum pelo apoio incondicional ao projeto e pela primorosa editoração da revista.

Emerson Gabardo
Editor-chefe da IJDL

EDITORIAL

We have reached the tenth issue of the *International Journal of Digital Law*. As announced in the previous editorial, the *IJDL*, despite being a beginner journal, is already one of the most cited journals in the area, according to Google metrics.

In this issue, we have sought to maintain an innovative approach and emphasize articles that deal with technology and law based on ethical and conscious assumptions. The task of consolidating the assumptions of the Brazilian Constitution of 1988 remains the motto of research that interests the journal.

The articles deal in-depth and carefully with sensitive topics, such as digital due process, the big techs liability, the right to privacy, data protection, artificial intelligence, biometric data, and the modernization of public administration.

As always, I reiterate my thanks to *Editora Fórum* for the unconditional support of the project and the exquisite editing of the journal.

Emerson Gabardo
IJDL Editor in Chief

DOI: 10.47975/digital.law.vol.4.n.1.montenegro

O devido processo tecnológico na prestação de serviços digitais (tratamento de conteúdo digital) sob responsabilidade das *big techs*[I]

The technological due process in the provision of digital services (digital content treatment) under the responsibility of big techs

Ricardo de Holanda Melo Montenegro[*]
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa
(Brasília, Distrito Federal, Brasil)
ricardoholanda@gmail.com
https://orcid.org/0000-0001-9152-1749

Recebido/Received: 26.04.2023/ April 26th 2023
Aprovado/Approved: 31.06.2023/ June 31st 2023

Resumo: O objetivo principal da pesquisa é apontar problemas enfrentados pelos consumidores na prestação de serviços digitais das *big techs*, relacionada ao tratamento (moderação) de conteúdo digital (TCD) e ao devido processo tecnológico. Alguns desses problemas são a falta de transparência; o abuso da figura jurídica do consentimento; a violação à privacidade (digital) e a falta de controles de acesso ao conteúdo digital (rastreabilidade) pelo consumidor; a ausência de canais de atendimento multimeios adequados; protocolos de atendimento rastreáveis e prazos para respostas; a inexistência de meios equilibrados para defesa e atendimento ao consumidor. Para tanto, é utilizado o método exploratório descritivo, mapeadas algumas lacunas regulatórias, para entender como a regulação de plataformas e serviços digitais é feita internacional e nacionalmente, e comparados os serviços

[I] Como citar esse artigo/How to cite this article: MONTENEGRO, Ricardo de Holanda Melo. O devido processo tecnológico na prestação de serviços digitais (tratamento de conteúdo digital) sob responsabilidade das big techs. *International Journal of Digital Law*, Belo Horizonte, v. 4, n. 1, p. 9-34, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.montenegro.

[*] Pós-graduando em Direito Digital e Proteção de Dados pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) (Brasília, Distrito Federal, Brasil). Graduado em Direito pelo Centro Universitário e em Engenharia de Computação (Uniesp) pela Universidade Potiguar. Especialista em Direito Público pela Universidade de Caxias do Sul (UCS) e Escola Superior da Magistratura Federal do Rio Grande do Sul (Esmafe/RS). Advogado. Conciliador na Justiça Federal (Paraíba). Técnico em Regulação na Agência Nacional de Telecomunicações (Anatel). *E-mail*: ricardoholanda@gmail.com.

tradicionais de (tele)comunicação e radiodifusão (telefonia, rádio, televisão) com a forma de difusão de conteúdo digital e (tele)comunicação dos serviços digitais prestados pelas *big techs*. O artigo apresenta estudo de caso com impacto coletivo que retrata a falta de transparência e elenca os requisitos que descumprem o devido processo tecnológico e violam o princípio da paridade de armas. Discute, ainda, algoritmos, tomadas de decisões automatizadas e Inteligência Artificial. Ao final, direciona a discussão técnica e as considerações finais para o aprimoramento de requisitos ao devido processo tecnológico e apresenta, por meio de eixos estruturantes (ex.: trilhas de auditoria, autonomia do consumidor para controlar o acesso a seu conteúdo digital personalíssimo, fiscalização conciliatória *online*), sugestões para melhorar a experiência dos consumidores e tornar o ambiente digital mais justo.

Palavras-chave: Devido processo tecnológico. Tecnologia jurídica. Direito digital. Direito do consumidor. Moderação de conteúdo digital. Regulação de plataformas.

Abstract: The main objective of the research is to point out problems faced by consumers in the provision of digital services by big techs, related to the treatment (moderation) of digital content (TCD) and due technological process. Some of these problems are the lack of transparency; the abuse of the legal figure of consent; the violation of (digital) privacy and the lack of controls on access to digital content (traceability) by the consumer; the absence of adequate multimedia service channels, traceable service protocols, and deadlines for responses; the lack of balanced means for consumer defense and service. To this end, the descriptive exploratory method is used, mapping some regulatory gaps to understand how the regulation of digital platforms and services is done internationally, nationally, and comparing traditional (tele)communication and broadcasting services (telephony; radio, television) with the form of digital content dissemination and (tele)communication of digital services provided by big techs. The article presents a case study with collective impact that portrays the lack of transparency, and lists the requirements that fail to comply with the technological due process and violate the principle of parity of arms. It also discusses algorithms, automated decision-making and artificial intelligence. In the end, it directs the technical discussion and final considerations to the improvement of technological due process requirements, and presents, through structuring axes (*e.g.* audit trails, consumer autonomy to control access to their very personal digital content, online conciliatory inspection), suggestions to improve the consumer experience and make the digital environment fairer.

Keywords: Due to the technological process. Legal tech. Digital law. Consumer law. Digital content moderation. Platform regulation.

Sumário: 1 Introdução – **2** Lacunas regulatória e legislativa para serviços digitais – **3** Devido processo tecnológico – **3.1** Panorama internacional sobre regulação de serviços digitais – **3.2** Exemplo de ausência de transparência no tratamento de conteúdo digital – **3.3** Proposta de eixos estruturantes para tratamento de conteúdo digital – **4** Considerações finais – Referências

1 Introdução

Antes de iniciar o estudo sobre o devido processo tecnológico é importante entender o cenário tecnológico e jurídico experimentado pelas sociedades digitais. Dessa forma, cabe destacar que o quantitativo de demandas e conflitos relacionado à moderação de conteúdo digital e a violação de liberdade de expressão aumentam exponencialmente e caminham para um volume de infrações nos direitos de consumidores, violações de direitos fundamentais e a liberdade econômica, sem precedentes, fruto dessa nova revolução, que é tecnológica, e em razão de os cidadãos e a economia (digital) estarem hiperconectados.

O exercício da cidadania e da liberdade de expressão, os meios de trabalho e a produção, a partir da massificação ou universalização da *internet*, mudaram. A democratização de meios de comunicação sociais (digitais), a tecnologia móvel amplificam o debate público e a cibercultura,[1] que, durante décadas, permaneceu restrita à comunicação presencial (diálogos), telefonia fixa (voz) e a meios de comunicação em massa unidirecionais, como o rádio (AM, FM) e a televisão.

É nesse contexto que o devido processo tecnológico e a moderação de conteúdo digital ganham força no cenário atual, ponto central deste artigo, que tem como objetivo geral abordar o conceito, carente de referências em português, e a prestação de serviços digitais pelas *big techs*[2] aos consumidores, quando se deparam com o Tratamento de Conteúdo Digital (TCD) e a ausência de requisitos e transparência desse "poder moderador".

De acordo com Gomes, conteúdo digital é qualquer dado fornecido digitalmente.[3] Portanto, tratamento (moderação) de conteúdo digital pode ser entendido, de modo simples, como filtrar ou controlar dados ou informações geradas por terceiros (humanos), ou criadas e difundidas por dispositivos digitais e programas de computador (algoritmos, Inteligência Artificial) – robôs –, o que deve ser realizado com transparência, paridade de armas, contraditório e ampla defesa, a partir de regras pré-estabelecidas, diante de conteúdos ilícitos, por violação a direitos humanos e fundamentais, do descumprimento de termos e políticas de uso de serviços digitais, que podem justificar o bloqueio ou exclusão de conteúdo digital, o banimento ou a suspensão de acesso ao serviço digital.

Dessa forma, a maneira como esses agentes de mercado controlam a economia de um país e a comunicação social, combinado com a hiperessencialidade da economia digital e o uso de dispositivos móveis para a manutenção da vida humana e de empresas, é o novo panorama econômico-jurídico-tecnológico que exige das ciências jurídicas uma atualização no modo como o Estado exerce seus poderes, pois a moderação de conteúdo digital tem colocado em xeque direitos fundamentais.

A moderação por meio de bloqueio de conteúdo digital, banimento ou suspensão de uma rede social digital ou acesso a aplicativo, sem a observância do devido processo tecnológico, pode inviabilizar a renda de uma família, de um autônomo prestador de serviços, o faturamento de uma empresa, a manutenção da vida de

---

1 "Cibercidadania", ou cibercultura, é definida como o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço. (LÉVY, 1995).

2 *Big techs* podem ser definidas como empresas de tecnologia da informação e comunicação (TIC), configuradas como grandes conglomerados econômicos que executam e prestam serviços digitais a diversos segmentos da economia de um país, incluindo comunicação social, além de conectar produção a consumidores. Na Europa, as *big techs* recebem nomes como Very Large Online Platforms (VLOPs) or Search Engines (VLOSEs), respectivamente, Plataformas Online Muito Grandes e Motores de Busca Online Muito Grandes.

3 GOMES, 2021.

um artista, o pequeno comércio de um vendedor de cachorro-quente, a falência de pequenas empresas localizadas em comunidade ou bairro, a destruição da imagem de grandes conglomerados econômicos.

O termo "plataformas digitais", na definição de Valente, são sistemas tecnológicos que funcionam como mediadores ativos de interações, comunicações e transações entre indivíduos e organizações, operando sobre uma base tecnológica digital conectada, especialmente no âmbito da *internet*, provendo serviços calcados nessas conexões, fortemente lastreados na coleta e processamento de dados e marcados por efeitos da rede.[4]

As plataformas digitais ou *big techs*, atualmente, violam a soberania, pois possuem mais informações sobre seus cidadãos e economia do que o próprio Estado Constitucional, seus órgãos públicos, de inteligência e de defesa nacional.

A falta de políticas regulatórias para prestação de serviços digitais sob responsabilidade das plataformas digitais, em especial a moderação de conteúdo digital, coloca esse segmento econômico em autorregulação, ao mesmo tempo que não empodera o consumidor e não insere a participação social no centro das soluções.

De forma análoga, a moderação de conteúdo digital se assemelha ao poder de polícia administrativa, no entanto, mais eficiente que o próprio Estado Democrático de Direito e suas instituições públicas, pois as ações e decisões são automatizadas por programas de computadores calibrados por humanos (desenvolvedores e executivos de negócios).

Poder-se-iam equiparar essas questões de moderação de conteúdo digital mencionadas com os institutos jurídicos de "interdição de estabelecimentos, instalações ou equipamentos, assim como a apreensão de bens ou produtos", previstos na Lei Geral de Telecomunicações – LGT (Lei nº 9.472, de 16 de julho de 1997) –, que são mascaradas por não cumprimento de regras privadas estabelecidas pela própria plataforma digital, sem qualquer participação popular, consulta pública e legitimidade jurisdicional e política, sequer transparência.

Por isso, defende-se regulamentar e regular o tratamento de conteúdo digital, por meio de requisitos mínimos que assegurem o devido processo (legal) tecnológico, tendo em vista que esse tratamento, muitas vezes, infringe e restringe direitos.

Portanto, o estudo questiona em que medida existem ausências de transparência e de requisitos técnicos-jurídicos mínimos para assegurar o devido processo tecnológico deste segmento econômico (plataformas digitais e *big techs*), bem como investiga e elenca achados de assimetrias de informações no TCD, sob responsabilidade dessas.

[4] VALENTE, 2019, p. 170.

A natureza da pesquisa faz uso do método exploratório descritivo e, ao longo dos resultados do estudo, correlaciona as assimetrias a princípios espraiados no ordenamento jurídico brasileiro: transparência, ampla defesa, contraditório, paridade de armas. A pesquisa também explora caso concreto de plataforma digital que configura falha em massa na prestação de serviço ao consumidor, possíveis violações ao devido processo tecnológico em razão da falta de transparência e desrespeito ao princípio da paridade de armas.

Este artigo aborda uma perspectiva introdutória sobre o devido processo tecnológico e a prestação de serviços de tratamento (moderação) de conteúdo digital, sem pretender esgotar o tema, mas ampliar as discussões sobre o conceito e a importância de requisitos. Para isso, correlaciona lacunas regulatórias à prestação de serviços digitais pelas *big techs*.

O estudo apresenta uma combinação de ordens de discussões para o devido processo tecnológico, uma mais ampla, que se relaciona a algoritmo, a tomada de decisões automatizadas, e outra relacionada as atividades de moderação de conteúdo, transparência e informação adequada, privacidade, controle de acesso a conteúdo digital pelos consumidores.

Ao final, o estudo almeja maximizar o debate acadêmico, regulatório e de políticas públicas acerca do devido processo tecnológico e suas implicações para a moderação de conteúdo digital, sugerindo aprimoramentos de requisitos.

2 Lacunas regulatória e legislativa para serviços digitais

O atual cenário de moderação de conteúdo digital apresenta assimetria de informações por falta de transparência entre os demandantes, consumidores, que inclui empresas e autônomos e ofertantes (*big techs*), assim como em razão do poder de mercado em face de falta de concorrência e de eventuais condutas anticompetitivas associadas à moderação de conteúdo digital, pois, em sua maioria, não há tantos aplicativos, redes sociais e plataformas digitais substitutas com capilaridade *online* como as atuais (WhatsApp, Instagram, Facebook, Youtube, Twitter etc.).

Nesse sentido, é importante refletir como organizar e fiscalizar o funcionamento desses agentes de mercado (plataformas digitais e *big techs*) que realizam moderação de conteúdo digital, entender melhor os impactos por meio de uma análise de impacto regulatório e saber como o Estado deve agir, se portar diante de infrações a direitos de consumidores e violações a direitos fundamentais, como a liberdade de expressão e a livre manifestação do pensamento.

No Brasil, não há um órgão com competência para moderar conteúdo digital ou, pelo menos, acompanhar e fiscalizar os conflitos existentes entre as plataformas

digitais, *big techs* e os consumidores, tornando-os escravos digitais de seus termos de uso, políticas de dados e políticas de *cookies*.[5]

A competência mais próxima para tratamento (moderação) de conteúdo digital é a estabelecida para o Ministério das Comunicações, a quem cabe o papel de fiscalizar o conteúdo veiculado por emissoras de televisão, para cumprimento de regras definidas no Regulamento dos Serviços de Radiodifusão, aprovado pelo Decreto Presidencial nº 52.795/1963.

O maior desafio da atividade de moderar conteúdo digital é que, em analogia, nas rádios e televisões o conteúdo não era produzido diretamente por terceiros (consumidores), era uma escolha das emissoras. No entanto, nas redes sociais os consumidores são livres para apresentarem suas ideias, gerar e divulgar seu conteúdo. Por isso, é mais difícil moderar esse tipo de conteúdo (gerado por terceiros), o que exige a tutela com o devido processo tecnológico.

Nesse contexto de geração de conteúdo digital por terceiros (consumidores) e de sua moderação, o complexo é saber como as decisões estão sendo automatizadas, qual a motivação, em que medida há transparência dessas decisões tomadas por algoritmos e por inteligências artificiais.

Talvez seja possível extrair uma discussão de filosofia jurídica desse cenário, qual seja: o serviço digital prestado pelas plataformas na difusão de conteúdo digital pode ser equiparado à prestação de serviços de radiodifusão (rádio e televisão)? Parece ser uma via reflexiva, vez que possuem difusão de informações e de comunicação com mesmo ou maior potencial, e, considerando a finalidade de ambos os serviços, há certa similitude de características da atividade econômica, que só os diferenciam em razão do conteúdo (digital) ser gerado por terceiros. Todavia, também são retransmitidos e impulsionados em grandes blocos de difusão, comparável à uma rede retransmissora de televisão ou rádios.

Além do que, no contexto atual, as plataformas conseguem controlar melhor sua forma de atuação na comunicação (digital), por ser um serviço que utiliza como base a ciência de dados, a mineração dos dados por meio de mapeamentos de perfis comportamentais e geográficos de cada cidadão e empresa.

A Constituição Federal, em seu Capítulo V, "Da Comunicação Social", mesmo que possua toda a preocupação e tutele os bens jurídicos de liberdades de opinião

[5] *Cookies*: são uma forma de coletar informações sobre a navegação de usuários. Eles são capazes de registrar, por exemplo, os hábitos e as preferências dos usuários em páginas da *web*. De posse dessas informações, os servidores são capazes de distinguir usuários e assim fornecer páginas personalizadas, de acordo com os gostos do usuário específico. Além disso, também são capazes de rastrear as páginas navegadas, e em alguns casos de registrar o histórico de navegação (CALDERON, 2017, p. 185).

e expressão, de imprensa, de informação, de manifestação de pensamento, elenca, em seu art. 221, requisitos de moderação para veiculação de conteúdo.[6]

Destarte, a própria Constituição Federal (CF), como se observa no art. 221, apresenta descompasso com o cenário da revolução tecnológica vivida atualmente por causa dos serviços digitais e das demandas sociais que clamam por um ambiente digital mais sadio e pacífico.

Observando o aludido art. 221, parece possível pensar em uma proposta de emenda à Constituição (PEC) que viabilize proteção em nível constitucional, para que a prestação de serviços digitais, como a comunicação digital e a moderação de conteúdo realizada pelas plataformas digitais, se enquadrem também em princípios fundamentais e básicos para prestação de seus serviços.

Ao tempo que as plataformas não possuem obrigações mínimas relacionadas à prestação de serviços digitais no Brasil, os serviços de radiodifusão sofrem regulação, e isso confirma o abismo regulatório.

Já o Decreto Presidencial nº 52.795/1963 prevê, em seu art. 28, item 12, que os serviços de radiodifusão devem se sujeitar a preceitos e obrigações na organização da programação (conteúdo a veicular). Portanto, o Estado já define a programação de uma televisão moderando o conteúdo a veicular, por meio de diretrizes como: percentual mínimo para transmissão de programas educacionais, transmissão de serviço noticioso, limite máximo de tempo de publicidade comercial, além de estabelecer que as empresas de radiodifusão não devem transmitir programas que exponham pessoas a situações que, de alguma forma, redundem em constrangimento.

Igualmente, a moderação de conteúdo prevista no Decreto nº 5.296, de 2 de dezembro de 2004, estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência (p. ex.: auditiva ou visual), visa garantir o direito de acesso à informação por meio de percentual mínimo para veiculação de conteúdo com legenda oculta, que auxilia pessoas com deficiência auditiva, e audiodescrição, que auxilia pessoas com deficiência visual.

O que se observa nessas políticas é que nada mais são que marcos regulatórios para o segmento de comunicação social. Então, se há intervenção regulatória para um segmento que possui proteção em nível constitucional; portanto, não há justificativa plausível para não ocorrer com os serviços digitais prestados pelas *big techs* e plataformas digitais.

---

[6] "Art. 221. A produção e a programação das emissoras de rádio e televisão atenderão aos seguintes princípios:
I - preferência a finalidades educativas, artísticas, culturais e informativas;
II - promoção da cultura nacional e regional e estímulo à produção independente que objetive sua divulgação;
III - regionalização da produção cultural, artística e jornalística, conforme percentuais estabelecidos em lei;
IV - respeito aos valores éticos e sociais da pessoa e da família."

De modo semelhante, a Lei nº 13.709, de 14 de agosto de 2018, comumente chamada de LGPD (Lei Geral de Proteção de Dados), indica preocupação com a segurança de dados e define medidas técnicas e administrativas, para garantir rastreabilidade na violação (acidentais ou ilícitas) de proteção de dados pessoais, como prevê o art. 6º da LGPD.[7]

Outro exemplo de regulação tecnológica análoga para o setor privado é que as prestadoras de serviços de telecomunicação são submetidas a regras normativas e padrões de segurança cibernética como os previstos na Resolução nº 740, de 21 de dezembro de 2020, que aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, da Agência Nacional de Telecomunicações (Anatel).[8]

Logo, os setores econômicos (privados) farmacêutico, de saúde suplementar, telecomunicações, sistema financeiro, água, transportes, energia elétrica, aviação civil, dentre outros, são regulados e obrigados a seguir regras normativas mínimas, impostas pelo Estado Regulador. Porém, as plataformas digitais e *big techs* vivem em uma estrutura de mercado próxima ao monopólio (digital), autorregulado, e não respeitam regras básicas, mesmo sendo um dos setores econômicos com mais consumidores e de maior faturamento.

A regulação de conteúdo digital, por meio do devido processo tecnológico, pode proteger as minorias, jovens e idosos de um ambiente digital hostil, que difunde violência, notícias falsas, ódio, terrorismo, crimes sexuais, pornografia infantil, dentre outros temas críticos que a sociedade deve rechaçar para priorizar uma convivência pacífica, ao mesmo tempo que essa regulação deve fomentar o pluralismo de ideias e a liberdade econômica, a liberdade de aprender, pesquisar, divulgar o pensamento, a arte e o saber.

No entanto, a legislação brasileira ainda carece de um ato regulatório para prestação de serviços digitais e tratamento (moderação) de conteúdo digital, vez que a Lei Geral de Telecomunicações, a citada LGPD, o Marco Civil da Internet (MCI), o Código Brasileiro de Telecomunicações (CBT) e a Medida Provisória nº 2.228-1,

---

7 "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
(...)
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

8 "Art. 5º As pessoas naturais ou jurídicas envolvidas direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços de telecomunicações devem atuar em Segurança Cibernética observando as seguintes diretrizes:
(...)
VII - respeitar e promover os direitos humanos e as garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação do usuário dos serviços de telecomunicações; e,
VIII - incentivar a adoção de conceitos de *security by design* e *privacy by design* no desenvolvimento e aquisição de produtos e serviços no setor de telecomunicações."

de 6 de setembro de 2001, que cria a Agência Nacional de Cinema e regula obras audiovisuais, cinematográficas e videofonográficas e o Regulamento dos Serviços de Radiodifusão não abordam o tema conteúdo digital, nem a moderação.

De outra forma, em vários países já existem legislações e regulação para prestação de serviços digitais, como é o caso dos europeus, que aprovaram, recentemente, a Lei de Serviços Digitais e a Lei de Mercados Digitais, respectivamente chamado, em inglês, de Digital Services Act (DSA) e o Digital Markets Act (DMA). Estes visam criar um espaço digital que respeite os direitos fundamentais dos cidadãos e que garantam equidade de tratamento para empresas.

A Alemanha já possui seu marco regulatório: é o Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), de 2017.

Portugal aprovou a Carta de Direitos na Era Digital; os Estados Unidos estão debatendo a lei que proíbe a publicidade de vigilância (Banning Surveillance Advertising Act) e a Lei Americana de Inovação e Escolha OnLine (American Innovation and Choice Online Act).

Na Inglaterra, está em discussão a Lei de Segurança Online (Online Safety Bill).

Esses projetos e marcos regulatórios demonstram a importância de o Brasil ampliar as discussões e enfatizar o debate sobre a ausência de transparência e de requisitos técnicos-jurídicos para tratamento de conteúdo digital.

3 Devido processo tecnológico

São várias as nuances que envolvem o devido processo tecnológico. Logo, a abordagem conceitual desse instituto não se limita a decisões automatizadas e transparência, embora, atualmente, seja a mais discutida, esse artigo pretende jogar luz em outras preocupações esquecidas, como a privacidade, o controle e a rastreabilidade de acesso ao tratamento de conteúdo digital, sem levar em consideração, apenas, conteúdos gerados por terceiros em redes sociais, mas também simples dados (conteúdo) armazenados em nuvem.

A Academia tem associado o devido processo digital, eletrônico ou tecnológico, ao trâmite processual, a jurisdição, decisões automatizadas e requisitos técnicos-jurídicos mínimos relacionados a transparência e a direitos dos consumidores que utilizam serviços digitais, públicos ou privados. Também se encontram na literatura os termos regulação de plataformas e regulação de algoritmos que buscam tratar esses assuntos mencionados.

Entende-se que esses termos significam que o desenvolvimento de tecnologias digitais e de programas de computador (algoritmos, aplicações) deve respeitar o devido processo legal.

Antes de tecer comentários sobre o devido processo tecnológico, é importante entendermos um pouco sobre *legal technology* e a moderação de conteúdo digital.

O termo *legal technology*, definido por Hoffmann-Riem, "refere-se ao uso da tecnologia da informação nos campos jurídicos de atividades como assessoria jurídica, jurisprudência, na aplicação do Direito, mas também no processo legislativo".[9]

Uma das áreas que a *legal tech* aborda é a decisão automatizada por meio de programa de computador (*software*), e é o que ocorre com a moderação de conteúdo digital automatizada.

Para Citron, a automação de decisões elimina a criação de regras participativas. O código, não as regras, determina os resultados dos julgamentos. Os programadores inevitavelmente definem as regras estabelecidas e as incorporam de maneira que o público, os funcionários da plataforma e os tribunais não podem revisar.[10]

A professora e pesquisadora explica que o devido processo tecnológico fornece novos mecanismos para substituir as questões processuais que a automação de decisões coloca em risco e enfatiza que a regularidade processual é essencial para evitar a "arbitrariedade por algoritmo".

Não é desproporcional comentar que os sistemas de decisões automatizadas, utilizados pelas plataformas digitais para tratamento de conteúdo digital, funcionam por meio de algoritmos e inteligência artificial que burlam o direito administrativo, usurpam as funções jurisdicionais e do Estado Regulador, mitigam a soberania do país, a liberdade expressão e a livre manifestação do pensamento.

As questões de devido processo tecnológico relacionadas a tratamento de conteúdo digital não se resumem às redes sociais. O tema é tão relevante que, por exemplo, a elaboração de uma patente nacional por pesquisador brasileiro de universidade pública, a criação de estratégias militares, a guarda de informações de inteligência, segurança nacional, de segredos industriais e de negócios de empresas brasileiras, por meio de um simples aplicativo editor de texto, em que este armazena essas informações na nuvem (*cloud*) em outro país, já apontam para segurança cibernética deficitária e para um tratamento de conteúdo digital em que não há transparência, ou seja, que não se sabe como é controlado, quem e para que se acessam essas informações.

Enfatiza-se que não é possível ter acesso, com transparência, aos tratamentos de conteúdo digital realizados por esses agentes de mercado (*big techs*), principalmente porque as plataformas digitais e aplicativos justificam segredo industrial e de negócios.

Entende-se que conteúdo digital pode ser classificado em dados e informações produzidos ou coletados, acessíveis a titulares e controladores, segmentados ou

[9] HOFFMANN-RIEM, 2020, p. 183.
[10] CITRON, 2008.

organizados por meio de mineração de dados (*data mining*),[11] em razão de interesses de negócios privados ou de Estado, sendo o tratamento de conteúdo digital tão crítico quanto o tratamento de dados pessoais (sensíveis principalmente).[12]

A realidade é que as plataformas digitais controlam vários parâmetros para calibração de seus algoritmos e construção de seus conjuntos de dados (estruturados), *e.g.*: dados, informações, interconexões pessoais e empresariais, perfis de acesso e comportamentais. Por conseguinte, correlacionam esses parâmetros com o conteúdo digital e automatiza decisões, o que torna o tema extremamente crítico e útil para analisar e julgar pessoas e grupos, atividades que podem violar direitos humanos e o Estado Democrático de Direito.

Nessa linha, Citron e Pasquale alertam que grandes volumes de dados (*big data*) são cada vez mais explorados para classificar e avaliar indivíduos. Para eles, alguns especialistas aplaudem a remoção de seres humanos e suas falhas do processo de avaliação e justificam que os sistemas automatizados classificam todos os indivíduos da mesma forma, evitando, assim, a discriminação. Mas essa conta é enganosa, segundo esses pesquisadores, como os seres humanos programam algoritmos preditivos, seus preconceitos e valores são incorporados nas instruções do *software*, conhecidas como código-fonte e algoritmos preditivos.[13]

Zaki destaca que os fundamentos dos algoritmos de mineração de dados e a aprendizagem de máquina são a base da ciência de dados, utilizam métodos automatizados para analisar padrões e modelos para todos os tipos de dados, em aplicações que vão desde descobertas científicas à análise de negócios.[14]

É importante ressaltar que, quando os consumidores (pessoa física, empresas e autônomos) usam serviços digitais das *big techs*, entregam seus dados pessoais e de negócios, seus perfis de acesso, comportamentais e socioeconômicos, bem como seus segredos industriais e de negócios.

É quando pessoa física, sua vida privada e intimidade, é exposta por meio de aplicativos de mensagens instantâneas e das plataformas digitais (redes sociais), sem vigilância de seus titulares de conteúdo digital, sem qualquer controle de acesso, rastreabilidade e prestação de contas ao consumidor, tudo ao alcance dos novos donos do poder e dos operadores de plataformas.

---

[11] A mineração de dados é o processo de descoberta automática de informações úteis em grandes repositórios de dados. Técnicas de mineração de dados são implantadas para vasculhar grandes conjuntos de dados para encontrar padrões novos e úteis, que, de outra forma, poderiam permanecem desconhecidos. Eles também fornecem a capacidade de prever o resultado de uma observação futura, como o valor que um cliente gastará em uma loja *online* ou loja de tijolo e argamassa (TAN, 2019, p. 4).

[12] Dados pessoais sensíveis são definidos pela LGPD como dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

[13] CITRON; PASQUALE, 2014.

[14] ZAKI; MEIRA JR., 2020.

Hupffer e Petry destacam que, por meio da coleta e análise de dados pessoais do usuário, é possível não somente direcionar seus passos com base em seu comportamento, mas também prevê-lo e influenciá-lo por meio de algoritmos, de forma que o detentor da informação exerce controle sobre o titular dos dados. Além disso, os autores mencionam que, pelo controle comportamental digital, o titular dos dados perde a noção de liberdade e do exercício do controle sobre as próprias decisões, levando a um descontrole na formação de suas vontades ou, de outra forma, um "controle guiado" pelo algoritmo.[15]

Reforça-se que a vida privada é a violação clara do tratamento de conteúdo digital; portanto, esses temas anteriormente citados são direitos fundamentais caros à liberdade e à privacidade, que também devem ser defendidas da vigilância sem limites, dos excessos de controladores de conteúdo digital, das ações sem legitimidades política e jurídica, do uso não consentido, do uso para fins diversos que se distanciem dos direitos humanos ou violem o Estado Democrático de Direito.

De modo inclusivo, o Estado deve levar em consideração a vulnerabilidade informacional, fática e socioeconômica, a hipossuficiência (técnica, jurídica e científica), de seus cidadãos consumidores de tecnologias digitais, e que sofrem tratamento de conteúdo digital, pois, em sua maioria, não têm ideia como acontecem os tratamentos de dados pessoais e de conteúdo digital, verdadeiros mapeamentos da vida privada que estão nas mãos de controladores, sem controles. Portanto, o tema carece de maior atenção do Estado para mensurar e assegurar a não violação da dignidade humana e tutelar os direitos humanos no ambiente digital, contra o capitalismo de vigilância e a nova forma de colonialismo, o digital.

Por isso, há relevância em assegurar e criar políticas públicas que contemplem a prestação de serviços digitais sem defeitos e com transparência, sob responsabilidade das plataformas digitais.

Ademais, o tratamento de conteúdo digital indiscriminado, sem transparência, infringe o art. 14 do Código de Defesa do Consumidor (CDC), transcrito a seguir, que declaradamente fundamenta a responsabilidade do fornecedor de serviços por defeitos relativos à prestação deles, por informações insuficientes à sua fruição, que podem ser entendidas como violações ao devido processo tecnológico.[16]

---

[15] HUPFFER; PETRY, 2021, p. 128.

[16] "Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

§1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:

I - o modo de seu fornecimento;

II - o resultado e os riscos que razoavelmente dele se esperam (...)."

Em razão de as plataformas digitais coletarem todos esses dados e informações, consequentemente, elas têm o dever de prestar serviço com qualidade, transparência e informação adequada; portanto, devem refletir um tratamento de conteúdo digital mais participativo, rastreável e controlável por seus titulares. Se o conteúdo digital possui titular, mesmo consentido, devem existir mecanismos de segurança da informação e tecnológica que garantam como, quando e para que (finalidade) são usados seus conteúdos digitais personalíssimos (*e.g.*: perfis de acesso, comportamentais).

Poder-se-á dizer que a moderação de conteúdo digital é uma espécie de tratamento de conteúdo digital, semelhante ao que é realizado com tratamento de dados pessoais; portanto, requer atenção do Estado para produção de políticas públicas e regulatórias que contemplem as atividades econômicas das plataformas digitais, especialmente por ser fundamentada na combinação ciência de dados e conteúdo.

As *big techs* são prestadoras de serviços de Tecnologia da Informação e Comunicação (TICs) aos consumidores e não podem justificar sua inércia ou sua arbitrariedade, simplesmente indicando que suas decisões de tratamento de conteúdo digital foram tomadas por algoritmos automatizados, sem transparência, ampla defesa e contraditório, pois, se assim o fazem, se colocam em estado de cegueira deliberada, por vezes monetizada, uma forma de corrupção privada por priorizar conteúdos ilegais que ferem os direitos humanos.

Os algoritmos são mecanismos tecnológicos criados pelas *big techs,* alinhados às políticas de seus negócios e concorrência, sem a validação e supervisão das partes (consumidores, poderes e instituições do Estado Democrático de Direito), que se comportam como autoridades de Estado, tomam decisões típicas de Estado para moderar (tratar) conteúdo digital, a partir de regras por aquelas estabelecidas, sem qualquer participação e controle social ou estatal, com pouco ou quase nenhuma transparência, sem prestação de contas (*accountability*), por meio de políticas privadas constantes de seus termos de uso e contratos de adesão.

O que está em jogo são decisões automatizadas por algoritmos para tratamento de conteúdo digital, calibradas por decisões estratégicas de negócios de tecnologia e inteligência artificial complexos, que são tomadas sem levar em consideração requisitos de liberdade de expressão, de liberdade econômica, que amparam arbitrariedades e censura, que podem implicar abuso de posição dominante, em concorrência desleal, e também suscitar condutas de infração à ordem econômica, prejudiciais à livre concorrência.

Posto isso, o devido processo tecnológico pode ser definido como procedimentos tecnológicos-jurídicos que visam assegurar igualdade material tecnológica, transparência, ampla defesa, contraditório, paridade de armas e requisitos mínimos

para que o titular possa realizar controle de conteúdo digital e receber informação adequada, quando suas informações (dados e conteúdo) pessoais estiverem em poder de terceiros ou em litigância com esses.

Portanto, as plataformas digitais e aplicativos digitais de *big techs* devem obedecer a um regramento mínimo quando realizar tratamento de conteúdo digital e prestar serviços digitais, ao tomar decisões automatizadas com o uso de algoritmos computacionais e Inteligência Artificial, ou por meio de decisões não automatizadas executadas por meio de conselhos de supervisão e recursos humanos, como no caso do Oversight Board, do Facebook.

A inadequação da moderação de conteúdo digital realizada pelas *big techs* no Brasil, por meio de automação de decisões, viola o devido processo tecnológico e não pode ser tolerado, ignorado pelos consumidores e Estado.

Portanto, se faz necessário uma atualização do arcabouço jurídico no âmbito dos direitos regulatório, administrativo, consumerista, em defesa das funções jurisdicionais, do poder investigatório, de fiscalização da lei e da Constituição Federal.

Kaye recomenda em seu relatório sobre promoção e proteção dos direitos de liberdade de opinião e expressão, que as políticas de acesso à informação devem ter regras claras para informações que podem ser retidas (moderadas), assim como mecanismos eficazes de reclamação e apelação, com forte implementação de sistemas de revisão e monitoramento.[17]

Esse conselho de Kaye reforça as discussões contidas neste estudo e deve ser aproveitado no tratamento de conteúdo digital brasileiro, além de refletir a necessidade de uma nova estrutura normativa e organizacional para inovar o Estado Regulador.

No Brasil, o art. 19, da Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet –, estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil e responsabilidades sobre conteúdo digital.[18]

Todavia, segundo a referida legislação, os conteúdos digitais gerados por terceiros não seriam elementos jurídicos para responsabilizar civilmente as plataformas digitais, nem os provedores de conexão, em respeito ao devido processo tecnológico, à exceção de quando esses são notificados e permanecem em estado de cegueira deliberada.

---

[17] KAYE, 2018.

[18] "Seção III – Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros (...):

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário."

Entende-se que a mera notificação do consumidor indicando à plataforma digital dano decorrente de conteúdo gerado por terceiros ou conteúdo ilegal, quando acompanhada da inércia de ação das plataformas digitais, também as responsabiliza, e não apenas a ordem judicial, como previsto no art. 19.

Dessarte, as decisões por uso de certos parâmetros e configuração de rede neural artificial, a aplicação de técnicas de aprendizagem de máquina (*machine learning*) e de Inteligência Artificial, a análise preditiva (processo de usar dados para prever resultados futuros), a identificação de padrões em dados massivos, empregadas no desenvolvimento de *software* (algoritmos), são recursos tecnológicos que facilitam a multiplicação de conteúdo digital em massa, automatizados (robotizados), ao mesmo tempo que proporcionam realizar *broadcasting* (replicação) de conteúdo digital tratado.

Ou seja, a segmentação das informações (*data mining*) e de conteúdo digital correlacionada aos perfis comportamentais de acesso e interesses comerciais, de usuários, grupos, Estados e geopolítica, possíveis a partir de coleta, armazenagem e organização, estão sob controle das plataformas digitais, e, por esse motivo técnico, as *bigs techs* devem ser responsabilizadas pelas formas que usam.

Ao cogitar forma análoga à operação das plataformas digitais, caso empresas do setor de comunicação social, em cadeia nacional, veiculassem conteúdos por meio de seus serviços de radiodifusão (televisão e rádio), para fins de violações ao Estado Democrático de Direito, aos direitos humanos, apologia ao crime, violência e terrorismo, igualmente seriam responsabilizadas.

Nunes e Paolinelli explicam que o *design* de plataformas públicas deve ser pensado para preservar o devido processo tecnológico e para promover participação paritária e equilibrada entre os litigantes, a fim se evitarem distopias de litigâncias que tendem a aprofundar o fosso de desigualdades, e destacam que as transformações que a tecnologia pode trazer ao processo brasileiro exige ressignificação urgente das garantias processuais-fundamentais. Contraditório na dinâmica de comparticipação, dever de fundamentação, ampla defesa (sobretudo, na dimensão técnica de fortalecimento do papel do advogado) e isonomia devem resgatar a função corretiva do devido processo, compreendido, agora, como devido processo tecnológico.[19]

Outro ponto de discussão atual é a falta de *transparência e a violação ao devido processo tecnológico, observadas no funcionamento do aplicativo ChatGPT, vez que esse não cita fonte. Eis que surgem dúvidas básicas e técnicas: todo esse conteúdo digital armazenado, distribuído e tratado pelo ChatGPT foi produzido com Inteligência Artificial* do aplicativo ou recursos humanos da empresa? Ou foi realizada

[19] NUNES; PAOLINELLI, 2021, p. 395-425.

uma coleta em massa na *internet* sem preocupação de indicar a fonte (origem) e com inobservância aos direitos autorais?

As informações fornecidas pelo ChatGPT também são procedentes de tratamento de conteúdo digital. Importante lembrar que o tratamento de conteúdo digital pode envolver não apenas texto, mas análises de imagens (fotos), voz, vídeos, informações personalíssimas como biometria, face, íris etc.

Portanto, em face do exposto, esses são motivos técnicos e elementos jurídicos que demonstram a necessidade de as plataformas digitais respeitarem o devido processo tecnológico, investirem em estruturas de defesa do consumidor e de direitos humanos.

3.1 Panorama internacional sobre regulação de serviços digitais

Vários países já aprovaram leis que buscam regular os serviços digitais prestados pelas *big techs*, entre eles o tratamento de conteúdo digital. Algumas leis estabelecem regras de transparência para prestação desses serviços, prazos de atendimento, formas de notificação, reforçam a tutela de bens jurídicos, como a privacidade, liberdade de expressão e opinião, criam novos direitos consumeristas.

A Alemanha, por exemplo, já possui seu marco regulatório, é o Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), de 2017, traduzido como ato para melhorar a aplicação da lei nas redes sociais, que define, na Seção 3, que as plataformas digitais de rede social devem manter um relacionamento eficaz e transparente, com procedimentos para lidar com reclamações sobre conteúdo ilegal de acordo, fornecendo aos consumidores um sistema facilmente reconhecível e de acesso direto, viável e permanentemente disponível para a apresentação de reclamações sobre práticas ilícitas.[20]

O ato estabelece o prazo de 24 horas para que as plataformas digitais removam conteúdo manifestamente ilegal, ou em até 7 dias, caso esteja envolvida instituição autorregulada. Todavia, deve reter o conteúdo, como prova, por 10 semanas e notificar imediatamente as partes e os motivos de sua decisão.

Em Portugal, foi elaborada a Carta de Direitos na Era Digital, que tutela a sociedade contra a geolocalização abusiva, contra a desinformação, que a define como toda narrativa comprovadamente falsa ou enganadora, criada e divulgada para obter vantagens econômicas ou para enganar deliberadamente o público.[21] Além disso, afirma a importância de a Inteligência Artificial respeitar os direitos humanos, consagra a neutralidade de conteúdo (art. 10º) como “direito à neutralidade

[20] ALEMANHA, [2017].
[21] REPÚBLICA PORTUGUESA, [2021].

da *internet*" e define direitos para os consumidores de serviços das plataformas digitais, como os previstos no art. 14.

A União Europeia aprovou duas leis, a Lei de Serviços Digitais e a Lei de Mercados Digitais, respectivamente Digital Services Act (DSA) e Digital Markets Act (DMA). Ambas visam criar um espaço digital seguro, que prioriza a proteção a direitos fundamentais de usuários e estabelece condições equitativas para empresas.

O Digital Services Act define que as plataformas com mais de 45 milhões de usuários terão obrigação de cumprir a lei até 17 de junho de 2023, e plataformas com menos de 45 milhões terão de obedecer ao DSA até 17 de fevereiro de 2024.

O DSA define o que é conteúdo ilegal, em resumo, quaisquer informações que estejam em desconformidade com direito da União Europeia ou de seus Estados-membros.[22] Em relação à moderação de conteúdo, define como atividades, automatizadas ou não, empreendidas por prestadores de serviços intermediários, destinadas em especial a deletar, identificar e combater os conteúdos ilegais ou informações incompatíveis com os seus termos e condições fornecidos pelos destinatários do serviço, incluindo as medidas tomadas que afetam a disponibilidade, visibilidade e acessibilidade desses conteúdos ilegais ou dessas informações, como a despromoção, a desmonetização, a desativação do acesso ou a supressão deles, ou que afetem a capacidade de os destinatários do serviço fornecerem essas informações, como a cessação ou suspensão da conta de um destinatário.

Ademais, o DSA cria obrigações para apresentar relatórios de transparência, anualmente, relativos aos serviços prestados pelas *big techs*, para os assuntos: atividades de moderação de conteúdo, quantitativo de decisões recebidas de autoridades categorizadas por conteúdo ilegal, quantitativo de notificações apresentadas a usuários, descrição qualitativa da motivação para moderação de conteúdo, tempo de atendimento, dentre outros.

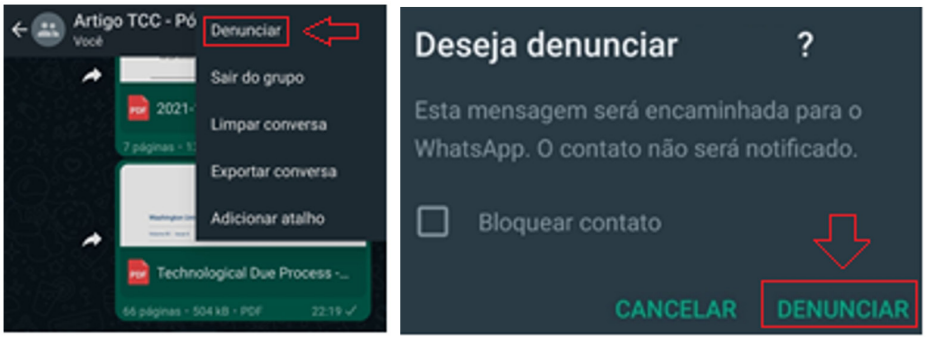
Nos Estados Unidos estão em discussão a lei que proíbe a publicidade de vigilância (Banning Surveillance Advertising Act) e a lei americana de inovação e escolha *online* (American Innovation and Choice Online Act – AICOA). Há também os Princípios de Santa Clara, de organizações civis, que concentram medidas em quantitativos de esforços para moderação de conteúdo, aviso claro aos usuários afetados e um processo robusto de apelações.[23]

[22] COMISSÃO EUROPEIA, [2023].
[23] THE SANTA CLARA PRINCIPLES, [2023].

3.2 Exemplo de ausência de transparência no tratamento de conteúdo digital

Há uma evidente falta de transparência na prestação de serviços digitais que realizam tratamento de conteúdo digital, sob responsabilidade de várias plataformas digitais e aplicativos de *big techs*. Todavia, este estudo se limita, como forma de exemplo, ao caso concreto do aplicativo de mensagens instantâneas WhatsApp, pois, no Brasil, ele é utilizado por cerca de 147 milhões de usuários, segundo o *site* Statista.[24]

Figura 1 - Telas do aplicativo móvel WhatsApp



Fonte: Whatsapp ([2023]).

O que mais chama atenção é essa ausência de transparência com o consumidor, e, apesar da denúncia ser registrada, não são informados qualquer protocolo de identificação da denúncia, prazo para atendimento, nenhuma informação sobre o trâmite interno de tratamento da denúncia é prestada.

É possível entender que essas questões técnicas indicadas violam o devido processo tecnológico, por desrespeitar a paridade de armas e ignorar a necessidade de transparência, vez que o usuário fica sem meios e informações adequadas para agir. De outra forma, quando o consumidor é banido ou tem seu acesso suspenso, devem ser respeitados os direitos de ampla defesa, contraditório, presunção inocência, pilares do devido processo tecnológico.

3.3 Proposta de eixos estruturantes para tratamento de conteúdo digital

Todas essas assimetrias de informações, fatos tecnológicos-jurídicos e desrespeitos a princípios básicos de direitos humanos e ao devido processo

[24] STATISTA, [2023].

tecnológico anteriormente citados podem configurar defeitos na prestação de serviço digital. Porém, o mais grave é o consumidor não ter ciência de como e quando seu conteúdo digital é acessado, armazenado, por quem é acessado e para quê.

As legislações deveriam se preocupar em criar obrigações para que o tratamento de conteúdo digital fosse realizado com rastreabilidade e transparência ao seu titular (consumidor), por meio de obrigação de existência de trilhas de auditoria, de modo que o seu titular pudesse em tempo real saber o que estaria ocorrendo com suas informações pessoais (dados e conteúdos digitais).

O controle de conteúdo digital deve ser de seu titular e não das *big techs*, ou seja, o consumidor deve ter o poder de controlar a sua privacidade; a inversão de valores e funções tolhe o direito humano à privacidade.

Seguindo a mesma perspectiva, Stefano Rodotà observa que as discussões sobre privacidade não podem se limitar ao direito ao esquecimento ou direito a ser deixado em paz, mas ter como centro de gravidade a capacidade de cada indivíduo controlar a utilização da informação que lhe diz respeito. O autor desperta ainda a atenção para a possibilidade de indivíduos e grupos controlarem o exercício de poderes com base na disponibilidade de informação, contribuindo assim para o estabelecimento de equilíbrios sociopolíticos mais adequados.[25]

Essa preocupação jurídica-científica de Rodotà representa o cenário contemporâneo experimentado pelos consumidores na prestação de serviços digitais pelas *big techs*, em que o exercício de poderes sobre a privacidade e a comunicação social – digitais – está nas mãos e manipulação daquelas e de outros Estados, sob seus interesses, objetivos de negócios e (geo)políticos, formas de controles antagônicas aos entendimentos erguidos nesta pesquisa.

O emérito professor ressalta que já não é possível considerar os problemas de privacidade apenas sob o pêndulo da confidencialidade e divulgação; entre o homem que é prisioneiro de seus segredos e o homem que não tem nada a esconder; entre a "casa-fortaleza", que exalta a privacidade e favorece o egocentrismo; a "casa-vitrine", que favorece as trocas sociais, e assim por diante. Ademais, acrescenta que essas são alternativas cada vez mais abstratas, pois refletem uma forma de encarar a

[25] No original: "Questo processo può essere forse schematizzato rilevando che si pone sempre più debolmente l'accento su definizioni della privacy come "diritto ad essere lasciato solo", a tutto vantaggio di definizioni il cui centro di gravità è rappresentato dalla possibilità di ciascuno di controllare l'uso delle informazioni che lo riguardano.

Non che quest'ultimo aspetto fosse assente dalle definizioni tradizionali: ma, in queste, esso serviva piuttosto a sottolineare, ad esaltare la componente individualitica, presentandosi come un mero strumento per realizzare il fine dell'essere lasciato solo; mentre oggi richiama soprattutto l'attenzione sulla possibilità di singoli e di gruppi di controllare l'esercizio dei poteri fondati sulla disponibilità di informazioni, concorrendo cosí allo stabilirsi di più adeguati equilibri socio-politici" (RODOTÀ, 2021, trad. nossa).

privacidade que negligencia a necessidade de expandir o próprio conceito, para além da dimensão estritamente individualista.[26]

Entendimento compartilhado também por este estudo, de forma especial, quando se defende a autonomia do consumidor em ter ou não o Estado presente nos seus conflitos com as *big techs* e, também, sobre a entrega do controle integral de acesso ao conteúdo digital personalíssimo ao titular consumidor, com transparência, o que podemos chamar de privacidade digital controlada por rastreabilidade.

Nesse sentido, a Anatel acompanha e recebe registros de conflitos (reclamações) do setor de telecomunicações (privado) por meio de multicanais de atendimento ao consumidor, de maneira presencial; por voz (1331), por meio de navegador de *internet* e, recentemente, por aplicativo móvel chamado "Anatel Consumidor", que permite a todos os usuários de serviços de telecomunicações reclamarem de forma fácil e amigável, fazer avaliações sobre a solução do conflito, acompanhar prazos e todos os passos da reclamação por meio de linha de tempo de tratamento e relatório de indicadores de desempenho, uma inovação que pode ser adaptada à realidade dos conflitos experimentados pelos consumidores na prestação de serviços digitais das *big techs*.

Essa prática regulatória de excelência reflete a abordagem de meios alternativos de solução de conflitos e disputa de resolução *online* (Online Dispute Resolution – ODR), de forma que empodera o consumidor e insere um terceiro imparcial (agentes públicos, órgão regulador) no acompanhamento e solução de conflitos de alta complexidade tecnológica.

Dessa forma, entende-se que há espaço para uma regulação mais participativa do consumidor na prestação de serviços digitais e no tratamento de conteúdo digital, que pode ser efetivada por meio de disputa de resolução *online*.

Repisa-se que conceder o poder de controlar integralmente as fases do tratamento de conteúdo digital ao titular-consumidor e ofertar a ele, por decisão autônoma, a opção de o Estado acompanhar ou não a sua reclamação ou denúncia, pode equilibrar o fosso digital de desigualdade experimentados pelos consumidores de serviços digitais, geralmente leigos, vulneráveis, hipossuficientes.

De outro modo, a partir da entrega desse controle integral aos acessos realizados aos seus dados e conteúdos personalíssimos, pode ser devolvida a igualdade processual tecnológica, com observância à paridade de armas, e proporcionar ao titular restringir (bloquear, requerer exclusão), permitir acesso, vender ou transferir seu conteúdo digital.

[26] No original: "(...) non è più possibile considerare i problemi della privacy solo seguendo il pendolo tra riservatezza e divulgazione; tra l'uomo prigioniero dei suoi segreti e l'uomo che non ha nulla da nascondere; tra la casa-fortezza, che glorifica la privacy e favorisce l'egocentrismo, e la casa-vetrina, che privilegia gli scambi sociali; e via dicendo. Queste tendono ad essere sempre più alternative astratte, poiché in esse si rispecchia un modo di guardare alla privacy che trascura proprio la necessità di dilatare questo concetto al di lá della dimensione strettamente individualistica in cui la sua vicenda d'origine lo ha sempre costretto" (RODOTÀ, 2021, trad. nossa).

Salgado e Saito, indicam que "proteger o direito à privacidade na era digital não significa pleitear o fim da coleta de dados pessoais, mas defender que tais práticas sejam realizadas em prol da transparência e da *accountability* (prestação de contas), a fim de diminuir a assimetria entre os polos da relação informacional".[27]

Nesse sentido, as pesquisadoras defendem a possibilidade de o usuário ter o conhecimento real das diferentes maneiras como seus dados serão utilizados e para quais finalidades eles estão sendo coletados, entendimentos jurídicos-científicos que corroboram os eixos estruturantes defendidos nessa pesquisa, como as trilhas de auditoria e a autonomia decisória no controle de acesso ao conteúdo digital personalíssimo pelo consumidor.

Portanto, diante da pesquisa, é possível depreender e propor quatro eixos estruturantes para assegurar o devido processo tecnológico no tratamento de conteúdo digital:

1 Elementos básicos de transparência e informação adequada a serem apresentados ao consumidor, exemplos: a existência de canais de atendimento multimeios funcionais, prazo de atendimento, número de protocolo de recebimento de reclamação ou denúncia, direito à notificação antecipada (presunção de inocência) e instâncias recursais que assegurem ampla defesa, contraditório;

2 Existência de trilhas de auditoria que controle o acesso ao tratamento de conteúdo digital – privacidade digital controlada por rastreabilidade;

3 Entrega de controle integral dos acessos realizados a dados e conteúdos personalíssimos aos titulares consumidores;

4 Fiscalização conciliatória *online*: uso de métodos autocompositivos (ex.: conciliação) combinados com transparência de ações, fiscalização ativa com a participação de agentes de Estado, por opção e autonomia do consumidor.

Figura 2 - Eixos estruturantes

[27] SALGADO; SAITO, 2020.

A fiscalização conciliatória *online* pode ser vista como uma regulação participativa, que entrega ao consumidor autonomia para decidir se o Estado deve ou não acompanhar os conflitos (reclamações, denúncias, pedido de informação) que surgem no tratamento de conteúdo digital entre aquele e as *big techs*.

O objetivo da fiscalização conciliatória é alcançar a melhor solução para o conflito e, por ser uma técnica com participação ativa do consumidor e possuir, como pilar, um terceiro imparcial, neutro, torna a relação e o diálogo entre as partes mais equilibrada.

Portanto, o agente público regulador (conciliador) pode esclarecer assuntos de alta complexidade técnica, regulatória e jurídica, facilitando aos consumidores um melhor entendimento para solução do conflito, diante das dificuldades com a falta de conhecimento tecnológico e de violações de direitos e deveres.

4 Considerações finais

A presente pesquisa abordou o conceito de devido processo tecnológico e a prestação de serviços de tratamento de conteúdo digital, indicou a necessidade de regulação do tema no Brasil a partir da lacuna regulatória existente na legislação brasileira e o direito comparado.

Em relação à exploração bibliográfica foi realizado estudo atualizado sobre os requisitos técnicos-jurídicos do tratamento de conteúdo digital, que possibilitou perceber a necessidade de o devido processo tecnológico ser respeitado pelas plataformas digitais, de modo a alcançar e empoderar os consumidores na garantia de seus direitos, em especial a privacidade e o controle de acesso ao uso de conteúdo digital.

Nesse sentido, reconhecer a deficiência de tutela à privacidade, a partir de violações provocadas por implementações de alta tecnologia (inteligência artificial, automação de decisões por algoritmos) e formas indiscriminadas de como se acessa o conteúdo digital gerado por terceiro, concedendo a seu titular o controle integral e a transparência de acesso ao tratamento de conteúdo digital, talvez seja o primeiro passo a ser dado pelas nações, preservando ou criando mecanismos de controle à privacidade.

É possível concluir que esse primeiro passo retomaria as liberdades de comunicação, expressão e de opinião na *internet*, a privacidade, tão essencial para desenvolver a personalidade de cada indivíduo e proteger a dignidade humana, endossada pela Declaração Universal dos Direitos Humanos, expressamente citada no art. 12º.

A partir deste estudo, é possível visualizar que existe uma clara mitigação da privacidade, que fica nítida quando analisamos a forma antiga de comunicação,

por voz, realizada por meio de serviço móvel pessoal (telefonia móvel) ou serviço de telefonia fixa, em que não havia controles de conteúdo digital e mapeamento em massa de perfis comportamentais.

A exceção para controle de conteúdo nesses meios tradicionais de comunicação somente ocorria em casos de interceptação das comunicações, para fins de investigação (criminal), devidamente autorizada por ordem judicial. Logo, esse paralelo demonstra como a privacidade de todo cidadão hiperconectado às plataformas digitais e aplicações, sob o lema do consentimento, está desprotegida no seio da *internet* e na prestação de serviços digitais sob responsabilidade das *big techs*.

O consentimento do consumidor para tratar seu conteúdo digital é uma figura jurídica criada para controlar o consumidor, que não poderia ser utilizada para legitimar excessos, retirar responsabilidades evidentes e violar direitos de várias dimensões. Dessa forma, é possível concluir que esse consentimento não pode ser visto como uma carta de alforria, uma justificativa jurídica para violação da privacidade e da dignidade humana.

Por conseguinte, o devido processo tecnológico e o tratamento de conteúdo de digital requerem a criação de um sistema normativo que proteja o cidadão hiperconectado, o insira no centro de soluções participativas e de controle.

Ao longo do estudo, também foi possível observar a importância do devido processo tecnológico no regramento de trilhas de auditoria, para garantir a rastreabilidade de uso e acessos ao conteúdo digital, assim como sugerir um modelo híbrido, intitulado de fiscalização conciliatória online, que pode ser um instrumento jurídico-tecnológico alternativo para solução dos inúmeros conflitos de tratamento (moderação) de conteúdo digital, com plena paridade de armas para as partes, que contempla a transparência e a autonomia de decisão do consumidor para que o Estado acompanhe seus conflitos com as *big techs*.

A pesquisa apresenta a proposição e enfatiza a importância de incorporar requisitos de devido processo tecnológico à prestação de serviços digitais (inteligência artificial, decisões automatizadas, moderação (tratamento) de conteúdo digital), por meio de quatro eixos estruturantes: 1) elementos básicos de transparência e informação adequada (canais, prazos e protocolos rastreáveis de atendimento), direito à notificação antecipada; instâncias recursais; 2) trilhas de auditoria que controle o acesso ao tratamento de conteúdo digital – privacidade digital controlada por rastreabilidade; 3) entrega de controle integral dos acessos realizados a dados e conteúdos personalíssimos aos titulares consumidores e 4) fiscalização conciliatória *online*.

Observado também a boa prática regulatória da Anatel, que viabiliza estrutura de atendimento ao consumidor de serviços de telecomunicações (privados) por meio de multicanais, que inclui aplicativo móvel e que entrega opções para o consumidor

avaliar a solução do conflito registrado, com todas as fases acompanhadas por linha de tempo e indicadores de desempenho com relatórios e transparência.

Por conseguinte, verifica-se a possibilidade de replicar essa experiência regulatória para as relações de consumo com as *big techs* e, considerando a peculiaridade dos conflitos de moderação (tratamento) de conteúdo digital, liberdades de expressão e de comunicação, a possibilidade de implementar meios alternativos de solução de conflitos e disputa de resolução online (Online Dispute Resolution – ODR) pode empoderar o consumidor, sem a natureza do Estado sensor e censurador, arranjo que reforça o princípio da autonomia da vontade do cidadão digital, portanto, uma alternativa plausível para que o Estado acompanhe os conflitos e não sobrecarregue o Poder Judiciário, observando os direitos do titular da informação (conteúdo digital) e sua escolha.

Durante o estudo foi possível realizar uma correlação entre a prestação de serviços de comunicação tradicionais (televisão, rádio) e a difusão digital de informações (comunicação social digital) prestada pelas *big techs*, realidade que demonstra particularidades comuns a ambas, pois há certa similitude de características da atividade econômica, que só as diferenciam em razão do conteúdo (digital) ser gerado por terceiros, disparidades tributárias e de obrigações, até porque a comunicação também é retransmitida e impulsionada em grandes blocos de difusão, comparável à uma rede retransmissora de televisão ou rádio.

Os resultados da pesquisa indicam ainda sobre a eventual atualização do art. 221 da Constituição Federal, propõe a criação de uma PEC, em razão do abismo regulatório diante do atual cenário de revolução tecnológica e de comunicação digital em curso, devido à prestação de serviços digitais com escassa transparência e segurança jurídica-concorrencial, frente às demandas sociais que clamam por um ambiente digital mais sadio, pacífico, sem esquecer da privacidade digital controlada por rastreabilidade e autonomia do consumidor.

A sugestão apresentada pelo achado científico que propõe uma PEC, pode viabilizar proteção em nível constitucional para a prestação de serviços digitais de comunicação social digital e de moderação de conteúdo realizadas pelas *big techs,* de modo a contemplar princípios fundamentais e básicos do Estado Democrático de Direito e refletir as políticas públicas consumeristas, de inclusão social, econômica e digital, a necessidade do desenvolvimento nacional tecnológico e científico, a alfabetização digital, a democratização dos meios de comunicação digital e as culturas nacional e regional digitais.

Ante todo o exposto, é notória a criticidade do devido processo tecnológico (*lato sensu*) e do tratamento de conteúdo digital para a privacidade (digital), a observância às liberdades de comunicação, expressão e de pensamento, cientes

de que esses são, de novo, novos desafios para sociedades atuais, globalmente conectadas e interdependentes.

Referências

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – Anatel. *Resolução nº 740, de 21 de dezembro de 2020*. Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776. Acesso em: 18 fev. 2023.

ALEMANHA. *Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)*, [2017]. Disponível em: https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2. Acesso em: 12 mar. 2023.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br. Acesso em: 6 fev. 2023.

BRASIL. Decreto Presidencial nº 52.795/63. Aprova o Regulamento de Serviços de Radiodifusão. *Diário Oficial da União*: Brasília, DF, 1963. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/antigos/d52795.htm. Acesso em: 8 fev. 2023.

BRASIL. Decreto nº 5.296, de 2 de dezembro de 2004. Regulamenta as Leis nos 10.048, de 8 de novembro de 2000, que dá prioridade de atendimento às pessoas que especifica. *Diário Oficial da União*: Brasília, DF, 2004. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/antigos/d52795.htm. Acesso em: 08 fev. 2023.

BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados – LGPD. *Diário Oficial da União*: Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 fev. 2023.

BRASIL. Lei 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais. *Diário Oficial da União*: Brasília, DF, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9472.htm. em: 16 fev. 2023.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor – CDC, que dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 18 fev. 2023.

CALDERON, Barbara. *Deep & Dark Web*. Rio de Janeiro: Alta Books, 2017.

COMISSÃO EUROPEIA. *Digital Services Act (DSA)*, [2023]. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package. Acesso em: 17 mar. 2023.

CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review.*, Washington, D.C., Issue 85, v. 1249, 2008. Disponível em: https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2. Acesso em: 11 nov. 2022.

CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, Washington, D.C., v. 89, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209. Acesso em: 24 abr. 2023.

GOMES, Marcus Lívio (coord.) *et al*. *Tributação da economia digital e das novas tecnologias*: com ênfase em tributos diretos. Belo Horizonte: Dialética, 2021.

HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*: desafios para o direito. 2. ed. Rio de Janeiro: Forense, 2022.

HUPFFER, Haide Maria; PETRY, Gabriel Cemin. (Des)controle digital de comportamento e a proteção ao livre desenvolvimento da personalidade. *International Journal of Digital Law*, Belo Horizonte, ano 2, n. 1, p. 111-132, jan./abr. 2021. DOI: 10.47975/IJDL/1hupffer.

KAYE, D. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Human Rights Council, 38 session, 2018. Disponível em: https://digitallibrary.un.org/record/1304394/files/A_72_350-AR.pdf?ln=en. Acesso em: 9 mar. 2023.

LÉVY, Pierre. *Cyberculture*. São Paulo: Editora 34, 1995.

NUNES, Dierle; PAOLINELLI, Camilla Mattos. Novos *designs* tecnológicos no sistema de resolução de conflitos: ODR, e-acesso à justiça e seus paradoxos no Brasil. *Revista de Processo*, v. 314, p. 395-425, abr. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos* (*1948).* Disponível em: https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese. Acesso em: 18 mar. 2023.

REPÚBLICA PORTUGUESA. *Carta Portuguesa de Direitos Humanos na Era Digital*, [2021]. Disponível em: https://dre.pt/dre/legislacao-consolidada/lei/2021-164870244. Acesso em: 18 fev. 2023.

RODOTÀ, Stefano. *Tecnologie e diritti*. Bologna: Società editrice il Mulino, 2021.

SALGADO, Eneida Desiree; SAITO, Vitoria Hiromi. Privacidade e proteção de dados: por uma compreensão ampla do direito fundamental em face da sua multifuncionalidade. *International Journal of Digital Law*, Belo Horizonte, ano 1, n. 3, set./dez. 2020, p. 117-137.

STATISTA. *Dossier on WhatsApp in Brazil*, [2023]. Disponível em: https://www.statista.com/study/88278/whatsapp-in-brazil/. Acesso em: 12 mar. 2023.

TAN, Pang-Ning et al. *Introduction to Data Mining*. 2nd. New York: Pearson Education, Inc., 2019.

THE SANTA CLARA PRINCIPLES. *On Transparency and Accountability in Content Moderation*, [2023]. Disponível em: https://santaclaraprinciples.org/. Acesso em: 17 mar. 2023.

VALENTE, Jonas Chagas. *Tecnologia, informação e poder das plataformas* online *aos monopólios digitais*. 2019. Tese (Doutorado em Ciências Sociais) – Instituto de Ciências Sociais, Universidade de Brasília, 2019. Disponível em: https://repositorio.unb.br/handle/10482/36948. Acesso em: 14 mar. 2023.

ZAKI, Mohammed J.; MEIRA JR., Wagner. *Data Mining and Machine Learning*: Fundamental Concepts and Algorithms. 2nd ed. Cambridge: Cambridge University Press, 2020.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

MONTENEGRO, Ricardo de Holanda Melo. O devido processo tecnológico na prestação de serviços digitais (tratamento de conteúdo digital) sob responsabilidade das *big techs*. *International Journal of Digital Law*, Belo Horizonte, ano 4, n. 1, p. 9-34, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.montenegro.

DOI: 10.47975/digital.law.vol.4.n.1.valle

Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT[I]

The challenges regarding the preservation of privacy and data protection in the face of the IoT equipment

Vivian Lima López Valle[*]
Pontifícia Universidade Católica do Paraná (Curitiba, Paraná, Brasil)
vivianclvalle@gmail.com
https://orcid.org/0000-0002-5793-2912

Bruna Gavron Barbosa[**]
Pontifícia Universidade Católica do Paraná (Curitiba, Paraná, Brasil)
brunagavron@hotmail.com
https://orcid.org/0009-0008-8723-9052

Recebido/Received: 03.03.2023/ March 3rd, 2023
Aprovado/Approved: 09.06.2023/ June 9th, 2023

Resumo: A Internet das Coisas poderá alterar significativamente o modo como as pessoas vivem. Entretanto, com a crescente utilização desses dispositivos, que já se encontram ou que estarão em breve no mercado, é necessária uma atenção aos riscos que eles podem trazer à privacidade como

[I] Como citar esse artigo/How to cite this article: VALLE, Vivian Lima López; BARBOSA, Bruna Gavron. Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT. *International Journal of Digital Law, Belo Horizonte*, v. 4, n. 1, p. 35-61, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.valle.

* Professora titular de Direito Administrativo da Pontifícia Universidade Católica do Paraná (Curitiba, Paraná, Brasil). Doutora e mestre em Direito do Estado pela Universidade Federal do Paraná. Especialista em Contratação Pública pela Universidade de Coimbra. Coordenadora do Curso de Direito da Pontifícia Universidade Católica do Paraná. Coordenadora do Curso de Especialização em Licitações e Contratos da Pontifícia Universidade Católica do Paraná. Diretora acadêmica do Instituto Paranaense de Direito Administrativo. Membro da Comissão de Gestão Pública da Ordem dos Advogados do Brasil, Seção Paraná. Advogada especializada em Direito Público. *E-mail*: vivianclvalle@gmail.com.

** Bacharela em Direito pela Pontifícia Universidade Católica do Paraná (Curitiba, Paraná, Brasil). Advogada. *E-mail*: brunagavron@hotmail.com.

direito fundamental dos usuários. Assim, o objetivo do presente artigo é demonstrar os desafios para preservação do direito à privacidade como princípio constitucional, frente à crescente conectividade dos dispositivos presentes no cotidiano dos indivíduos, visando à aplicação do princípio da privacidade, no âmbito da Internet das Coisas (IoT), e com base na Constituição Federal e na Lei Geral de Proteção de Dados.

Palavras-chave: LGPD. IoT. Privacidade. Tecnologia. Dados. iRobot.

The challenges regarding the preservation of privacy and data protection in the face of the IoT equipment

Abstract: The Internet of Things could significantly change the way people live. However, with the use of these devices that are already on the market, it is necessary to pay attention to the risks that can bring to privacy as the fundamental right of users. Thus, the objective of the article is to demonstrate the challenges for the preservation of the right to privacy as a constitutional principle, the growing connectivity of devices in the daily life of the base, applying the application of the principle of privacy in the scope of the Internet of Things (IoT), with basis on the Federal Constitution and on the General Data Protection Law.

Keywords: GDPR. IoT. Privacy. Technology. Data. iRobot.

Sumário: 1 Introdução – **2** A relevância da *internet* na sociedade de informação – **3** Os direitos fundamentais à privacidade e à intimidade na Constituição de 1988 – **4** O tratamento de dados por meio da Lei Geral de Proteção de Dados como forma de preservar o direito à privacidade – **5** A proteção da privacidade nos dispositivos IoT com base na Lei Geral de Proteção de Dados – **6** Caso iRobot – aquisição da iRobot pela Amazon – **7** Conclusões – Referências

1 Introdução

A proposta da presente pesquisa consiste em abordar os desafios na preservação da privacidade como princípio constitucional frente ao avanço da tecnologia, visando demonstrar a fragilidade dos equipamentos cada vez mais conectados e dependentes da internet, utilizando-se dos parâmetros resguardados pela Lei nº13.709/2018 (Lei Geral de Proteção de Dados).

O ponto inicial é o impacto causado pelo avanço da tecnologia, que expandiu celeremente a conectividade dos dispositivos eletrônicos e objetos diversos, causando uma enorme concessão de dados pelos seus usuários, uma vez que, para seu funcionamento, há uma vasta coleta e envio de dados que estes adquirem de seus ambientes. É certo que em uma sociedade de comunicação digital, desde as redes e mídias sociais à Internet das Coisas, também conhecida por IoT (Internet of Things, em inglês), a violação de sua privacidade tem colocado em risco o sistema constitucional com seus mecanismos de proteção dos direitos.

Em razão disso, tal estudo conceituará o direito à privacidade como direito fundamental resguardado pela Constituição Federal de 1988. Posteriormente, adentrará na aplicação deste no âmbito da Internet das Coisas (IoT), a qual descreve uma rede de objetos físicos incorporados a sensores, *software* e outras tecnologias, com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela

internet. Esses dispositivos variam de objetos domésticos comuns a ferramentas industriais sofisticadas.

Partindo dessa premissa, o estudo apontará os desafios para a aplicação do direito à privacidade na esfera da IoT frente aos dispositivos legais resguardados pela Lei Geral de Proteção de Dados, uma vez que ela permite o compartilhamento e coleta de dados com o mínimo de intervenção humana, de modo que tais sistemas podem digitais gravar, monitorar e ajustar cada interação entre itens conectados.

2 A relevância da *internet* na sociedade de informação

Ao longo do tempo, a sociedade passou por diversas formas de organização social. Cada mudança teve por fator determinante a estruturação de um elemento central que, ao seu desenvolvimento, estabeleceu o respectivo marco histórico.[1]

Na sociedade agrícola, o produto agrícola era o fator determinante para a economia por meio da prática do escambo (que de modo geral significa troca ou permuta), sendo a fonte de riqueza aquilo que provinha da terra. Na sociedade industrial, a fonte de riqueza sobreveio da criação das máquinas a vapor e da eletricidade, que modificou a produção nas fábricas.[2]

Em um terceiro momento, na sociedade dita sociedade pós-industrial, a prestação de serviço passou a impulsionar a economia, ou seja, mais importante era não mais o que se produzia, mas como poderia se ofertar os serviços.[3]

Já na sociedade atual, a forma de organização tem como seu elemento central a informação, sendo essa a impulsionadora da economia. Esse elemento se consolidou devido à acelerada evolução tecnológica, da qual decorrem vários mecanismos capazes de processar e transmitir informações em quantidade e velocidade inimagináveis. A relação social foi afetada por um amontoado de informações; não havia mais obstáculos físicos, como a distância, que pudessem interferir, o que também gerou uma nova compreensão de tempo-espaço.[4]

Sobre tal perspectiva, é possível dizer que a informação é o novo elemento estruturante responsável pela organização da sociedade, assim como foram a terra, as máquinas a vapor e a eletricidade e os serviços, formando a chamada sociedade da informação. E, ainda que essa nova forma de organização não se resuma ao ambiente virtual, as ferramentas que contribuem de forma mais abundante neste processo são a computação e a *internet*.

1 SILVA, 2009, p. 43.
2 BIONI, 2021, p 3.
3 BIONI, 2021, p. 3.
4 BIONI, 2021, p. 4.

Outro fator determinante na sociedade da informação é a alteração da plataforma na qual estas são sobrepostas. Antes, as informações eram descritas e armazenadas em papéis por meio de livros ou ficheiros. Após a descoberta dos *bits*, um sistema binário (1 e 0) que empregou uma linguagem compreensível aos computadores, passou-se a processar e armazenar informações, condensando-as em unidades menores, bem como possibilitou-se o uso de comandos pré-determinados, por exemplo, a utilização de palavras-chave com intuito de buscar informações. Com essa desmaterialização, logo todos os tipos de informações (áudio, vídeo, imagens...) também puderam ser digitalizadas, o que gerou um acúmulo de informações e novas plataformas, como *compact disk* (CD), *pendrive*, computadores pessoais, entre outros.[5]

Manuel Castells destacou, nos anos 1990, que a *internet* seria o canal de interconexão global mais importante, de modo que praticamente tudo estaria conectado a sistemas acessíveis a indivíduos e instituições, bem como afirmou que a caracterização da atual revolução tecnológica é a aplicação de novos conhecimentos e informações que geram dispositivos de processamento e comunicação da informação, de forma a se tornar um ciclo cumulativo de inovação – introdução de uma nova tecnologia – e seu uso.[6]

Com o avanço da tecnologia, o século 19 rege-se pelas múltiplas inovações das formas de comunicação na *web*, caracterizando-se pelo acesso instantâneo, pela praticidade dos aplicativos *mobile*, pela celeridade na transmissão de mensagens e, principalmente, pela enorme quantidade de dados pessoais e informações armazenadas.[7]

Essa realidade traz preocupação, uma vez que expandiu celeremente a conectividade dos dispositivos eletrônicos e objetos diversos, causando uma enorme concessão de dados pelos seus usuários, considerando-se que, para seu funcionamento, há uma vasta coleta e envio de dados que estes adquirem de seus ambientes.

É certo que, em uma sociedade de comunicação digital, desde as redes e mídias sociais à Internet das Coisas, a violação de sua privacidade tem colocado em risco o sistema constitucional com seus mecanismos de proteção dos direitos, uma vez que os usuários ficaram mais vulneráveis à violação e à quebra de sigilo de seus dados eletrônicos ou digitais. Essa vulnerabilidade cresceu junta à inovação tecnológica, sobretudo quanto à privacidade e à intimidade, que possibilitou a quebra da confidencialidade dos meios de comunicação e dados, pois, enquanto há uma grande circulação de informações pela rede, que ocasiona aumento de invasões

5 BIONI, 2021, p. 6.
6 CASTELLS, 1999, p. 69.
7 ÁVILA; WOLOSZYN, 2017.

de *e-mails* e correspondências, indesejáveis telefonemas a contatos pessoais do usuário da tecnologia, há também aplicativos capazes de assimilar quais as rotinas, as preferências comerciais e trajetos do cotidiano dos usuários.[8]

E, mesmo estando assegurado o sigilo dos dados, correspondências e comunicações por meio do sistema de proteção e defesa dos direitos humanos, sendo convencionais ou extraconvencionais, bem como tenha sido abarcado pelo texto constitucional, afirma Bobbio que a maior provocação atual é saber, com exatidão, de que forma garanti-los em meio ao sistema global digital identificado pela inexistência de limites materiais.[9]

3 Os direitos fundamentais à privacidade e à intimidade na Constituição de 1988

Os direitos à privacidade e à intimidade são duas grandes heranças dos ideais do liberalismo dos séculos 17 e 18, ambos relacionados às liberdades individuais e, por isso, resguardados no âmbito constitucional de diversos países e na maioria dos documentos que versam sobre a proteção aos direitos humanos.

No início, o direito à vida privada adquiriu seus contornos por meio da defesa da propriedade, em que o domicílio era o elemento principal compreendido como o espaço onde o indivíduo estaria protegido de terceiros e do Estado. Entretanto, com o avanço das tecnologias, o sujeito ficou mais propício a ser exposto de modo inabitual, o que tornou necessário uma compreensão mais robusta do significado do direito à vida privada. Assim, a privacidade deixou de ser compreendida apenas na esfera da propriedade, passando a ser considerada também um direito à personalidade.

Os direitos de personalidade então previstos na Constituição Federal de 1988 em seu art. 5º, em especial nos incisos X, XI e XII, os quais respectivamente tratam da proteção ao direito à vida privada, à intimidade, à inviolabilidade do domicílio, ao sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas.

A Declaração Universal dos Direitos do Homem, por meio de seu art. 12, prevê que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

Na mesma linha, estabelece a Convenção Europeia para Proteção dos Direitos Humanos e das Liberdades Fundamentais,[10] de 1950, por meio de seu art. 8º,

8 ÁVILA; WOLOSZYN, 2017, p. 168.
9 BOBBIO, 2004, p. 25 citado por ÁVILA; WOLOSZYN, 2017, p. 170.
10 COUNCIL OF EUROPE, 1950.

a Carta de Direitos Fundamentais da União Europeia,[11] em seu art. 8º, o Pacto Internacional de Direitos Civis e Políticos,[12] a proteção da privacidade, em seu artigo 17, e a Convenção Americana de Direitos Humanos, assinada pelos países membros da Organização dos Estados Americanos,[13] em 1969, em São José da Costa Rica, por meio do art. 11.

Verifica-se que os direitos à privacidade e à intimidade restam protegidos por variados regulamentos, tanto regionais quanto internacionais, de modo que é de competência de cada Estado-membro a discriminação destes em seu ordenamento jurídico e a definição da forma como será efetivada tal proteção. Entretanto, considerando a dicotomia trazida pela Constituição Federal de 1988 ao preceituar a privacidade e a intimidade, se faz necessária uma abordagem mais minuciosa de tais termos.

O direito estadunidense, o qual dispõe sobre o *right to privacy*, não distingue a privacidade da intimidade, ou direito ao segredo do direito à reserva da doutrina italiana. Trata apenas de forma genérica o direito à privacidade, o qual não deixa de ser delimitado e compreendido devidamente na doutrina norte-americana, sendo uma preocupação jurisprudencial, a qual pode ser demonstrada por meio da Quarta Emenda à Constituição dos Estados Unidos. Esta proíbe a busca e apreensão sem causa razoável e mandado judicial amparado em causa provável, e sua origem se deve a um artigo escrito por dois advogados que problematizaram a crescente e potencial invasão do governo e da mídia na vida das pessoas.[14] Em princípio, o entendimento americano sobre a privacidade desdobra-se da propriedade, limitando ao Estado o poder de invadi-la, controlá-la ou ainda de dispô-la.

A doutrina brasileira se aproxima, em parte, dessa concepção do direito estadunidense, sem distinguir, de forma clara, a privacidade da intimidade, de forma que, quando realizada tal distinção, irrelevante materialmente, tornando-se mera questão de aprofundamento material. Essa mesma linha é seguida pelos doutrinadores José Afonso da Silva,[15] Gonet Branco[16] e Luiz Avolio.[17]

Tércio Sampaio Ferraz Jr. destaca que a privacidade se rege pelo princípio da exclusividade, o qual se baseia em três atributos: a solidão ou o estar só, o segredo ou o direito de exigir o sigilo e a autonomia, ou o direito de dispor sobre si mesmo, como sendo o centro das informações. A intimidade, por sua vez, garante sobretudo o estar só, trata-se de um aprofundamento da definição de privacidade;

11 EUROPEAN UNION, 2000.
12 BRASIL, 1992a.
13 BRASIL, 1992b.
14 GARCIA, 2018, p. 6.
15 SILVA, 1989. p. 183.
16 GONET BRANCO, 2009, p. 420.
17 AVOLIO, 2012, p. 24.

ou seja, com base no âmbito da privacidade, a intimidade é o mais exclusivo dos direitos e está contido no princípio da privacidade.[18]

Ao passo que Ferraz Júnior, em sua doutrina, trata do direito à privacidade com base no direito estadunidense, Paulo José da Costa Junior[19] popularizou no Brasil a teoria das esferas do direito alemão. Essa descreve a privacidade como sendo dividida em camadas, em que a primeira camada e a mais ampla representa a esfera privada, e nela estão contidos os comportamentos e acontecimentos que o indivíduo não quer que se tornem de domínio público; já na segunda, contida no interior da primeira, está a intimidade, uma esfera confidencial da qual fazem parte indivíduos em que a pessoa deposita certa confiança e com quem mantém uma intimidade; por fim, a terceira e última camada, localizada no centro, é a esfera do segredo.

Por meio dessa teoria, é possível distinguir intimidade da vida privada, bem como diferenciá-las do segredo. Isso se justifica pois a vida privada, como esfera de maior amplitude, é o direito de impedir que fatos da vida particular cheguem ao conhecimento do público. Já a intimidade, em sentido lato, remete ao direito de excluir do saber de outros informações sensíveis do indivíduo, como dados sobre vida sexual, política e religiosa, geralmente compartilhados apenas com pessoas mais íntimas e de forma reservada. Quanto à última esfera, a do segredo, ou intimidade em sentido estrito, ela compreende informações sobre o sentimento, sonhos e emoções do indivíduo, as quais geralmente não são divulgadas a terceiros e podem ser compartilhadas com amigos mais íntimos.[20]

Apesar de as correntes doutrinárias não realizarem clara distinção entre a vida privada e a intimidade, na Constituição Federal de 1988, é expressamente prevista tal dicotomia. Devido a isso, importante é buscar compreendê-la, porém sem desconsiderar que ainda há uma área cinzenta entre os princípios da vida privada e da intimidade, em virtude da sua proximidade.

Essa distinção pode ser mais bem compreendida com o suporte literário de George Orwell, por meio da distopia *1984*, criada pelo autor em 1949, na qual não há privacidade. O protagonista Winston consegue sair da vigilância do chamado "Grande Irmão" apenas em momentos de fuga, ou quando se aproveita de falhas dos sistemas de vigilância. Isso demonstra que a privacidade pode ser facilmente mitigada pelo poder estatal; basta que haja vigilância absoluta em todos os lugares, o que impede que um indivíduo fique só ou sem que alguém o observe por um instante.

[18] FERRAZ JÚNIOR, 1993, p. 439.
[19] GARCIA, 2018, p. 9.
[20] VIEIRA, 2007, p. 30.

Apesar de essa mitigação da privacidade afrontar necessariamente a intimidade das pessoas, uma vez que impede o seu livre desenvolvimento, a violação da intimidade não está ligada apenas à privação de determinado espaço sem que haja interferência de terceiros, ou ao sigilo de aparelhos pessoais, mas também ao pensamento próprio, à crítica, à noção do indivíduo sobre si e sobre o mundo, suas emoções, sentimentos, personalidade, relacionamentos íntimos, enfim, sua dignidade.

Nesse sentido, a intimidade adquire uma amplitude semântica que vai além do direito de estar só ou do direito à propriedade, como dito anteriormente. Resulta sua violação em exposição, que traz consigo a vergonha, impotência e medo. A própria possibilidade de virem a público os pensamentos, interesses, gostos e sexualidade do indivíduo sem o seu devido consentimento atinge o livre desenvolvimento de sua personalidade e de seu modo de ser na sociedade.

De forma resumida, a privacidade está ligada historicamente à proteção da propriedade e do direito de não ser incomodado por meio de seus bens, enquanto a intimidade se relaciona à proteção do livre desenvolvimento e da personalidade. A diferenciação proposta excede a sintonia entre os princípios; entretanto, considera-se que essa distinção conceitual está mais evidente em sua definição constitucional, além de conter mais potencial sob um viés político e crítico quanto à livre consciência e aos direitos civis, o que supera a origem patrimonialista.

4 O tratamento de dados por meio da Lei Geral de Proteção de Dados como forma de preservar o direito à privacidade

Tais princípios ainda podem ser compreendidos por meio de diferentes dimensões, as quais são citadas na obra de Bart Willem Schermer: o corpo, a mente, o domicílio, o comportamento íntimo, as comunicações, a vida familiar e os dados pessoais. Contudo, considerando o objeto do presente artigo, limitar-nos-emos à abordagem dos dados pessoais.[21]

Os dados pessoais são, segundo a Lei Geral de Proteção de Dados (LGPD), toda informação relacionada à pessoa natural identificada ou identificável (art. 5º, inciso I), ou seja, todas as informações codificadas de uma determinada pessoa que, ao serem tratadas, gera um informação pessoal,[22] o que abarca endereço, Código de Endereçamento Postal (CEP), número de telefone, profissão, data de nascimento, números indicadores da documentação em geral, nome de familiares, cidade natal, número do cartão de crédito, dados bancários, endereço eletrônico,

[21] SCHERMER, 2007, p. 76.
[22] ZANON, 2018, p. 21.

salário, mensagens de texto, fotos e vídeos, endereço de Internet Protocol (IP), entre outros.

Sem dúvida, a questão sobre o tratamento de dados pessoais eleva-se em importância devido ao avanço das novas tecnologias de comunicação. Por meio da Emenda Constitucional nº115, foi incluído, na Constituição Federal de 1988, o inciso LXXIX ao art. 5º, o qual prevê que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais", podendo ainda do esvaziamento dos próprios princípios da privacidade e da intimidade verificar que estes também protegem os dados pessoais, com a finalidade de não permitir condutas invasivas, ou seja, não permitir o acesso total aos dados pessoais pelo Estado ou por terceiros, de modo a ignorar o sentido principiológico dos dispositivos.

Até mesmo na administração pública foi introduzida uma nova perspectiva sobre o potencial gerencial, econômico e de direção das atividades públicas, decorrentes do movimento global em torno da disseminação de ferramentas de tecnologia da informação (TICs) e dos instrumentos digitais de preservação e armazenamento de dados, que possuem cada vez mais capacidade. Tal concepção levou à observação de que os dados podem se transformar em informações úteis, não sendo apenas dados isolados ou "crus" (*raw data*), trazendo à administração pública o dever de adotar medidas de proteção e segurança aos indivíduos, enquanto titulares dos dados e de seus próprios agentes, responsáveis pelo tratamento das informações.[23]

A chamada Quarta Revolução Industrial permitiu a fusão dos ambientes físico, digital e biológico, possibilitando relações jurídicas e interações inimagináveis no século 20. Tal revolução exige uma regulação eficiente capaz de, ao mesmo tempo, afastar as vicissitudes causadas pelo uso indevido, mal-intencionado, discriminatório, direcionado e estandardizado dos algoritmos e não impedir as inovações disruptivas e seu potencial transformador.[24]

Atualmente, praticamente todos os dados de uma pessoa estão, de alguma forma, registrados. Exemplo, os celulares, que guardam diversas informações sobre seus usuários, o Google, o Facebook, os bancos, os registros das conversas via WhatsApp, capazes de traçar perfil detalhado da vida e dos relacionamentos pessoais da pessoa, o conteúdo armazenado em computadores pessoais etc. Com base nisso, não resta dúvida de que o acesso a essas informações é capaz de criar uma narrativa vasta e arriscada acerca do indivíduo.

Egon Bockmann Moreira indica a necessidade de se constituir direitos fundamentais para humanos digitais, citando a existência de uma minuta da Carta dos Direitos Digitais da União Europeia que expande a percepção de direitos

[23] CRISTÓVAM; HAHN, 2020, p. 7.
[24] VALLE; GALLO, 2020, p. 78.

fundamentais para o mundo digital. O autor discorre sobre a *persona* digital em uma dimensão existencial ligada à dimensão de dados, informações digitalizadas e perfis que o indivíduo analógico assume no ambiente virtual, bem como sobre a interação da Inteligência Artificial (IA) algorítmica com ela. As perguntas pertinentes sobre tal assunto são: essa nova configuração do humano digital necessita de proteção distinta e de direitos fundamentais? a *persona* digital faz jus a proteção autônoma na condição de direito fundamental como um ser digitalizado? o posicionamento de Moreira inclina-se ao fato de a *persona* digital possuir autonomia diferenciada, e é merecedor de proteção de métricas que desconhece.[25]

As expressões "dados" e "informações" são comumente usadas como sinônimas, porém, são distintas. Dados refere-se a um estado primitivo da informação; são, segundo Bruno Bioni,[26] fatos brutos que se tornam algo inteligível quando processados e organizados, do qual pode se extrair uma informação. O inciso IV do art. 5º da LGPD conceitua banco de dados como sendo um "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico", o que envolve, em sua operação, a entrada (*input*) e a manipulação de dados e a saída (*output*) de uma informação, bem como seu gerenciamento, do qual se extrai conhecimento. Quanto à expressão "informação", ela é definida como sendo um dado ou conjunto de dados, processados ou não em um suporte apto a gerar conhecimento; pode ser uma imagem, som, documento eletrônico ou físico, ou ainda um dado isolado.[27]

Com base em tais definições, verifica-se que o banco de dados não é reduzido a um repositório de informações, mas trata-se de uma ferramenta que permite a criação de uma interface que possibilita a manipulação, análise e o descobrimento de informações para tomada de decisões. Isso possibilita a identificação e determinação do perfil do potencial consumidor, bem como seus hábitos e demais informações essenciais à tomada de decisão de forma tática e estratégica. É a chamada mineração de dados ou *data mining*, em que apenas alguns dados são valiosos, o que torna necessária a realização de uma seleção destes, uma vez que os dados considerados úteis não são mais identificados como dados, mas sim como informação por conter aspectos úteis e valor agregado, de modo que a mineração busca descobrir padrões, segmentar informações ou buscar correlações entre dados existentes.

Ainda, a LGPD traz conceitos distintos para "dados pessoais", "dados pessoais sensíveis" e "dados anonimizados". Em seu art. 5º, incisos I, II e III, classifica-os da seguinte forma:

[25] MOREIRA, 2019.
[26] BIONI, 2019, p. 35.
[27] VIEIRA, 2007, p. 157.

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Com tal distinção, nota-se que os dados pessoais sensíveis são aqueles que necessitam de maior proteção e sigilo, podendo sua coleta e utilização ocorrerem com ou sem consentimento explícito do titular, se abrangido em uma das hipóteses descritas no inciso II do art. 11 da Lei nº 13.709/2018.

A LGPD é aplicada para todas as operações de manipulação de dados feitas por pessoa natural ou física, independentemente do meio, do país de sua sede ou país onde estejam situados os dados, desde que essa operação de tratamento de dados seja realizada em território nacional com objetivo de ofertar ou fornecer serviços ou bens ou o tratamento de dados individuais localizados em território nacional. Exclui-se de tal aplicação o tratamento de dados pessoais com finalidade meramente particular ou não econômico, bem como para questões de defesa nacional, segurança pública, atividades de investigação e repressão de infrações penais, fins jornalísticos, artísticos e acadêmicos (arts. 3 e 4 da lei).

Entre os princípios norteadores de tal lei, os quais estão dispostos no art. 6º, estão os princípios da necessidade (inciso III), o qual limita o tratamento ao mínimo necessário para determinada finalidade, sem que haja excesso; livre acesso (inciso IV), que garante aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento; transparência (inciso VI), que garante aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento; segurança (inciso VII), que visa À utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; prevenção (inciso VIII), que prevê a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; não discriminação (inciso IX), que impossibilita a realização do tratamento para fins discriminatórios ilícitos ou abusivos; responsabilização e prestação de contas (inciso X), que exigem a demonstração pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como a eficácia dessas medidas. Esses princípios garantem o respeito aos direitos dos titulares, bem como geram

diretrizes a serem seguidas pelos agentes de tratamento, como o consentimento do titular e o legítimo interesse.

O tratamento dos dados é toda operação que coleta, utiliza, reproduz, transmite, distribui, processa, armazena, elimina e transfere dados, conforme demonstra o Quadro 1:

Quadro 1 - Tratamento de dados

DADOS PESSOAIS	
FASE DO CICLO DE TRATAMENTO	OPERAÇÕES DE TRATAMENTO - LGPD, ART. 5º, X
Coleta	Coleta, produção, recepção.
Retenção	Arquivamento e armazenamento.
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação.
Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão.
Eliminação	Eliminação.

Fonte: Comitê Central de Governança de Dados. Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD).

Para tal tratamento, a lei prevê a figura dos agentes de tratamento, os quais são o controlador, o operador e o encarregado pelo tratamento de dados. O controlador é o responsável pelas decisões referente ao tratamento dos dados coletados. O operador é quem realiza o tratamento dos dados pessoais em nome do controlador. Para atuação de ambos os agentes, a LGPD estabelece atribuições e limites, bem como os requisitos ao tratamento dos dados, conforme dispõem os arts. 7º e 11º da lei. Já o encarregado é a pessoa indicada pelo controlador e operador para operar como meio de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Tudo isso é necessário para segurança e sigilo dos dados, de maneira que a segurança da informação não é uma preocupação apenas das empresas ou do próprio Estado que coletam e processam os dados, mas também dos titulares, que estão, hoje, mais atentos, considerando os possíveis impactos de seus dados em posse de outros. A Lei nº 13.709/2018 evidenciou a responsabilidade dos agentes de tratamento e previu que estes devem adotar medidas de segurança para garantir que os dados pessoais não sejam obtidos por acessos não autorizados ou por situações acidentais ou ilícitas que visem a alteração, perda, destruição, comunicação ou outra forma de tratamento inapropriado ou ilícito. Assim, deve

ser mantida a garantia da segurança da informação até mesmo posteriormente ao tratamento realizado.

Ocorrendo incidentes de segurança que possibilitem risco ou dano significativo aos titulares, é dever do operador comunicar de maneira imediata a ANPD, descrevendo os fatos ocorridos, as informações sobre os indivíduos (titulares) afetados, os riscos ligados ao incidente e as medidas que serão tomadas a fim de reverter os efeitos do prejuízo. De forma breve, destaca-se que a ANPD é um órgão do governo inerente à presidência da República, ao qual compete fiscalizar e executar o que prevê a LGPD, regulamentar e fiscalizar as operações de tratamento dos dados, bem como aplicar as penalidades ao descumprimento da lei.

Quanto ao modelo regulatório, uma das principais características da LGPD, a qual foi herdada da RGPD (Regulamento Geral de Proteção de Dados), é a adoção do *ex-ante*, o qual impõe que, para o tratamento de dados pessoais, antes mesmo de ser realizada a coleta ou outra ação que envolva o primeiro, deve ser o agente de tratamento capaz de justificar tais atos, com base em uma das hipóteses de tratamento previstas no art. 7º da LGPD. Tal modelo *ex-ante* parte, ainda, da premissa de que todo dado pessoal ou toda informação ligada à pessoa natural identificada ou identificável é relevante sob aspecto jurídico, o que se deve ao aumento do processamento ubíquo e automatizado dos dados, fato que traz a necessária regulamentação das diversas formas de tratamento de dados pessoais.[28]

Assim, verifica-se que a LGPD possui como principal objetivo proteger os direitos fundamentais de liberdade e privacidade dos indivíduos, concentrando regras sobre o uso adequado de dados pessoais, aplicado a todos os setores, gerando um cenário com mais segurança jurídica, padronização de regulamento e ações que visem garantir a proteção no tratamento dos dados coletados, implementando um ambiente de desenvolvimento tecnológico, a partir de normas flexíveis e adequadas ao cuidado de negócios que se baseiam no uso de dados pessoais. Por meio dessa lei, o Brasil se torna ainda apto a gerenciar dados advindos de outros países que exigem níveis de segurança de dados. A redação da LGDP contém 65 artigos que abrangem diversas situações que resguardam os direitos dos titulares dos dados, bem como normas que devem ser observadas em operações que visem ao tratamento de dados pessoais pelos controladores e operadores.

[28] ZANETTI DE OLIVEIRA; FREITAS, 2022, p. 95.

5 A proteção da privacidade nos dispositivos IoT com base na Lei Geral de Proteção de Dados

A segurança de dados e da privacidade do usuário é um dos temas mais importantes em se tratando de uma rede de dispositivos. Desse modo, se faz necessária a adoção de medidas de segurança e de gerência de dados que possibilitem mitigar ataques e preservar a integridade das informações, uma vez que, dependendo do caso concreto, pode haver dados sensíveis armazenados ou em trânsito.

A evolução natural das coisas, com o passar do tempo, torna o produto ou equipamento mais simples passível de armazenar cada vez mais informações e de modo mais inteligente, por meio de recursos avançados de interação e interface homem-máquina. Assim, , por meio da inclusão digital, o acesso a esses dispositivos são expandidos para diversas classes da sociedade. E devido a toda essa interação, acessibilidade, mobilidade e facilidade de transposição de conteúdo digital de diversos equipamentos torna a segurança da informação um desafio, para que seja mantido o sigilo dos dados do usuário titular de tais conteúdos *online*, os quais, agora, podem ser armazenados em uma *smart* TV, micro-ondas, uma geladeira, entre outros, objetos esses que interagem com outros usuários à sua volta, bem como com o próprio fabricante.

Mas o que vem a ser a IoT? A IoT (sigla do termo em inglês Internet of Things, ou, em português, Internet das Coisas) refere-se à capacidade de que objetos usados no cotidiano do ambiente real interliguem-se com a *internet*, de modo a comunicarem-se, reportar informações sobre seu estado e funcionamento. De modo geral, a IoT relaciona-se com a ampla gama de dispositivos conectados à *internet* passíveis de se comunicarem com outros dispositivos e redes, de captar e transmitir dados e receber e executar ordens.[29]

Campos Pataca cita[30] que a Internet das Coisas pode ser classificada como uma terceira geração da *internet* a que se está habituado hoje, também chamada de Web 3.0, a qual compreende a capacidade de os objetos também se conectarem com a *internet* e de se comunicarem tanto entre si quanto com máquinas e sistemas de informações, bem como com as pessoas. Enquanto a primeira geração foi aquela fundada na digitalização da informação, a segunda inseriu indivíduos, maciçamente, como criadores de conteúdos, sobretudo por meio das mídias sociais.

De forma básica e sem nos aprofundarmos nos significados mais técnicos, a arquitetura da IoT se divide em camadas, e cada uma possui função necessária ao funcionamento do sistema. Elas podem ter de três a cinco camadas, as quais,

[29] PATACA, 2021, p. 208.
[30] PATACA, 2021, p. 208.

de forma básica, são: camada de percepção, de rede e de aplicação. A primeira é a camada física, em que há sensores para detectar e coletar informações sobre o ambiente, bem como parâmetros físicos e identificar objetos inteligentes do ambiente. A segunda é a camada responsável pela conexão com outros objetos inteligentes, dispositivos de rede e servidores, usados também para transmissão e processamento de dados do sensor. A terceira camada é responsável pela entrega dos serviços específicos ao usuário, sendo definidas nesta as aplicações nas quais a IoT pode ser implantada, como em casas e cidades inteligentes, entre outros.[31]

Se divididas em cinco camadas, essas são definidas em: percepção, transporte, processamento, aplicação e camadas de negócios. A função das camadas de aplicação e percepção permanece a mesma da arquitetura com três camadas. Quanto às demais, essas possuem os seguintes papéis: a camada de transporte repassa dados do sensor da camada de percepção para camada de processamento e vice-versa, usando redes como Bluetooth, *wireless*, *near-field communication* (NFC) [comunicação por campo de proximidade], *radio frequency identification* (RFID) [identificação por radiofrequência] etc. A de processamento (também chamada de *middleware*) armazena, analisa e processa enormes quantidades de dados advindos da camada de transporte, pode gerenciar e fornecer diversos serviços para camadas inferiores, bem como possui tecnologias, como banco de dados, computação em nuvem e módulos de processamento de *big data*. A quinta e última camada é a camada de negócios que gerencia todo sistema IoT, abrange aplicativos, modelos de negócios e lucros e a privacidade dos usuários.[32]

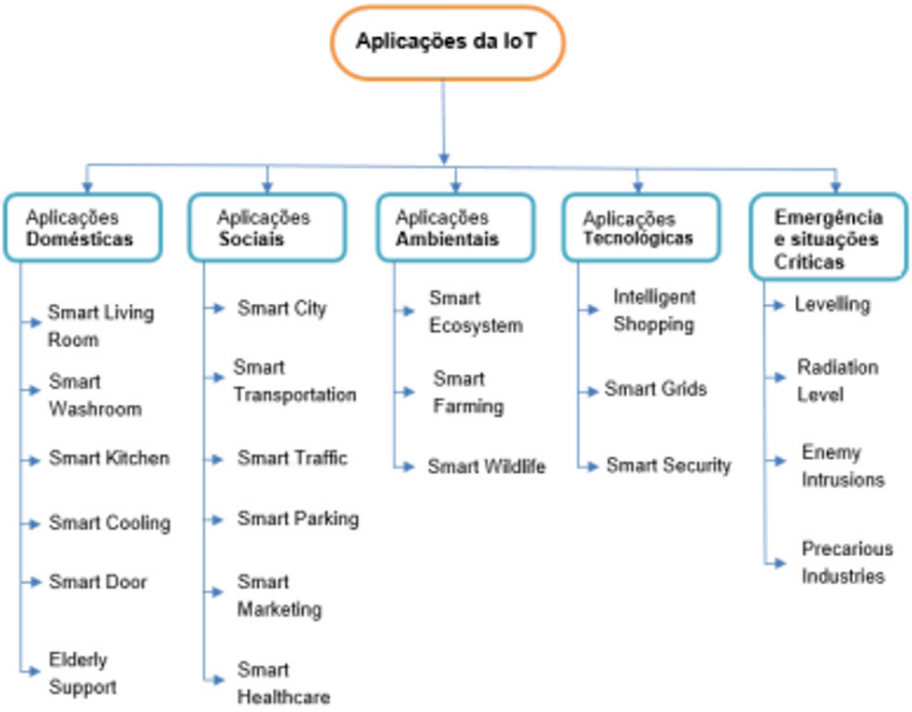
Quanto à comunicação da Internet das Coisas, essa utiliza, para tal, os protocolos de comunicação, os quais protegem e garantem a segurança dos dados trocados entre os dispositivos conectados. Geralmente, os dispositivos são conectados por meio de uma rede Internet Protocol (IP); entretanto, o Bluetooth e RFID, por exemplo, permitem que haja uma conexão local dos dispositivos, o que difere em potência, alcance e memória. Esses protocolos podem ser divididos, de forma ampla, em protocolos de rede e protocolos de dados. Os protocolos de dados IoT são utilizados para conectar dispositivos de baixa potência, fornecendo comunicação com o *hardware*, sem que haja conexão com a internet, usando uma rede com fio ou celular. São exemplos deles: Message Queuing Telemetry Transport (MQTT) [Transporte de Telemetria de Enfileiramento de Mensagens]; Constrained Application Protocol (CoAP) [Protocolo de Aplicação Restrita]; Advanced Message Queuing Protocol (AMQP) [Protocolo Avançado de Enfileiramento de Mensagens] etc. Já os protocolos de rede IoT são utilizados para conectar dispositivos via rede,

[31] SETHI; SARANGI, 2021, p. 2.
[32] SETHI; SARANGI, 2017, p. 3.

normalmente usados pela *internet*. São exemplos destes: *wi-fi*, Bluetooth, ZigBee, entre outros.[33]

De modo geral, a IoT é uma renovação tecnológica que, cada vez mais, contribuirá para otimização e automação de tarefas cotidianas e poderá trazer informações relevantes para benefício público e para empresas privadas, o que torna seus produtos e serviços prestados mais assertivos. Essa conexão virtual de dados, indivíduos, processos e coisas podem alcançar diversos domínios práticos, como domínio doméstico, social, ambiental, emergencial, incluídas aqui situações críticas e tecnológicas, conforme demonstra a figura a seguir:

Figura 1 - Principais áreas de aplicação da IoT



Fonte: *Revista de Direito, Estado e Telecomunicações* (2021).

Devido a toda essa conexão dos dispositivos IoT à rede, a segurança se torna a preocupação principal, uma vez que aumenta a possibilidade de ataques, *malwares* e invasões de *hackers*; trata-se de um risco potencial, mas sim um risco real. O crescimento e o uso da IoT dependem principalmente do aspecto de segurança,

[33] PATACA, 2021, p. 208.

uma vez que medidas de segurança devem controlar as ações tanto dos usuários quanto dos objetos. De modo paralelo, considerando-se que os dispositivos são caracterizados por recursos computacionais restritos, não basta a utilização de mecanismos de segurança convencionais, e, devido à heterogeneidade e às diversas interconexões dos dispositivos, gera-se uma grande quantidade de dados difíceis de gerenciar.

Os ataques que podem ocasionar a captação ou acesso aos dados dos usuários é a grande preocupação, uma vez que a rotina diária, dados gerais de saúde, hábitos, entre outros, são informações que podem ser inferidas até mesmo de dados não críticos. Nessa mesma linha, Allhoff e Henschke[34] abordam que, por meio dessa coleta de dados, é possível construir um perfil dos usuários, por exemplo, casas inteligentes, as quais podem mostrar rotina, hábitos de consumo e diversas informações, que muitas vezes são repassadas ao fabricante (nem sempre criptografadas). Isso demonstra que não apenas o mercado pode ter acesso a tais dados, mas *hackers* também podem fazer uso para fins nefastos.

De acordo com Barati,[35] as leis de proteção de dados surgiram com fundamento em fornecer o direito de privacidade de dados, de modo a não permitir que empresas que tratam dados os forneçam a outras empresas sem a devida permissão de seus titulares. Por essa razão, antes da realização do processamento de dados, a LGPD determina que haja o consentimento dos usuários, proibindo qualquer coleta de dados sem autorização e dando aos usuários pleno direito de manipular seus dados por meio de dispositivos inteligentes, ou por qualquer outro meio pelo qual possam acessar seus dados.

A Lei Geral de Proteção de Dados não traz definições quanto à proteção dos equipamentos, apenas faz alusão às boas práticas de segurança, deixando como responsabilidade do agente responsável controlar os dados a criação de mecanismos capazes de proteger os equipamentos. Podem eles criar normas de segurança, desenvolver os padrões técnicos, estabelecer métodos de supervisão dos dados, entre outros procedimentos técnicos e administrativos capazes de estabelecer um tratamento de acordo com a LGPD.

A criação e o uso de boas práticas de segurança de dados sempre foram recomendados; entretanto, requerem investimentos financeiros em recursos humanos e tecnológicos, o que[36] levou à sua adoção por poucas organizações. No entanto, a LGPD surgiu estabelecendo tais práticas em formato de lei, prevendo penalidades, como o recebimento de multas. A observação destas ainda é importante para evitar que haja vazamento de dados dos usuários. São diversos os setores em

[34] ALLHOFF; HENSCHKE, 2018, p. 59.
[35] BARATI, 2020.
[36] POHLMANN, 2020.

que pessoas mal-intencionadas invadem em busca de dados pessoais. Exemplo é a área da saúde, na qual os dados são alvo, pois podem ser vendidos na *dark web* com mais facilidade.[37]

Dessa forma, a interseção entre a privacidade e a IoT inicia-se por meio da percepção de que os dispositivos IoT podem coletar enormes quantidades de dados de seu usuário e de que esses dados são passíveis de serem analisados e compartilhados.[38] Exemplo foi o caso da Target,[39] amplamente divulgado, em que a empresa explorou hábitos de compra de determinada cliente, prevendo que esta estava gestante e enviando-lhe uma mala com diversos itens de bebê para sua residência. Ocorre que a usuária estava cursando o ensino médio e, embora estivesse grávida, sua família não tinha conhecimento do fato. Ou seja, a descoberta da gravidez se deu em razão da mala direta. A Target utilizou dados estatísticos por meio da análise de dados com base nas compras da cliente e, em pouco tempo, padrões úteis surgiram. Percebe-se, nesse caso, que a empresa estava coletando dados significativos da usuária, certamente vinculados ao seu cartão de crédito, e utilizou tais informações para traçar o perfil da cliente, prevendo, acertadamente, que ela estava grávida. A criação de perfil do usuário pode se mostrar uma boa prática de negócios, porém possivelmente invasiva, sem o consentimento do cliente.[40]

Logo, deve-se reconhecer que a IoT, devido a sua riqueza de sensores e comunicações integradas, oportuniza a reunião de um grande número de informações pessoais, a qual pode afetar, de forma significativa, a privacidade do indivíduo. Esse risco aumenta quando, junto à IoT, aplica-se a Inteligência Artificial.

A IA também possui capacidade de adquirir, processar e interpretar uma enorme quantidade de dados e decidir com base na interpretação destes dados. Considerando essa característica de coleta de dados, o que aumenta sua capacidade de observar o comportamento humano, há uma preocupação com relação à privacidade do indivíduo.[41]

Por meio da conectividade de vários sistemas de IA, que analisam dados e identificam *links* entre eles, a IA pode ser utilizada para transformá-los em grandes conjuntos de dados não mais anônimos, mesmo que não incluam dados pessoais por si mesmos.[42]

Assim, a IA passa a conseguir executar funções que antes apenas humanos conseguiriam, o que torna os indivíduos cada vez mais sujeitos às decisões ou

37 RILEY, 2019.
38 WEBER, 2015 citado por ALLHOFF; HENSCHKE, 2018, p. 58.
39 A Target é uma varejista de mercadorias em geral com lojas em todos os 50 estados dos EUA e no distrito de Columbia.
40 ALLHOFF; HENSCHKE, 2018, p. 58.
41 GABARDO; MENENGOLA; SANMIGUEL, 2023, p. 4.
42 GABARDO; MENENGOLA; SANMIGUEL, 2023, p. 5.

assistência da IA, as quais, por vezes, são difíceis de compreender e contestar, de forma eficaz, se necessário. O risco de tais decisões à sociedade se dá pela possibilidade de estas representarem, assim como nos humanos, discriminação, violação da privacidade, efeitos adversos nos processos democráticos e vigilância em massa (HEDLUND, 2022).[43]

Para proporcionar maior segurança jurídica aos usuários e desenvolvedores, é necessário regulamentação precisa que trate desses riscos e proteja os direitos e garantias fundamentais, uma vez que essa insegurança jurídica, consequência da ausência regulatória, pode prejudicar o uso da tecnologia e, com isso, causar danos irreversíveis aos que investem em IA.[44]

6 Caso iRobot – aquisição da iRobot pela Amazon

Um caso importante que envolve IoT foi a aquisição pela Amazon do iRobot, fabricante do robô aspirador Roomba.[45] Tais robôs são aspiradores que funcionam por meio de sensores que detectam obstáculos, escadas e paredes, além de medirem as distâncias em que devem trabalhar e possuírem tecnologia que os permite retornarem sozinhos aos seus locais de recarga, sem que seja necessário que o usuário realize algum comando.[46]

Os sensores de obstáculos ficam na parte do para-choque; o robô é capaz de identificar objetos pelo caminho, como mesas e cadeiras, desviando sem colidir com eles. Os sensores de escada (ou *cliff sensors*, para identificar "penhascos") são utilizados para evitar que o robô não se quebre em quedas, emitindo sinais infravermelhos pelo aspirador inteligente, que permanece todo tempo buscando identificar a superfície. Uma vez que não localize, imediatamente muda de direção. Da mesma forma, por meio de infravermelhos, detectam as paredes e conseguem acompanhar essas ao longo das bordas, mas em uma distância que evite o impacto.

Além dos sensores, o robô tem capacidade de mapear todos os ambientes da casa, o que auxilia o funcionamento do aspirador *smart*. Essa tecnologia integrada dos dispositivos utiliza câmeras digitais acopladas no dispositivo, ou *lasers* de detecção. Por meio de tais funcionalidades, coleta dados, combina informações e constrói algo parecido com um mapa mental do ambiente a ser limpo, sendo tal sistema também conhecido como Vision Simultaneos Localization and Mapping (VSLAM) [Localização Simultânea Visual e Mapeamento]. Assim, a função de limpeza do robô se torna mais eficiente e precisa, pois toda a planta do local

43 GABARDO; MENENGOLA; SANMIGUEL, 2023, p. 7.
44 EUROPEAN COMMISSION, 2020.
45 ALVES, 2022.
46 GIANTOMASO, 2018.

permanece armazenada no *software*, o que possibilita que o próprio equipamento defina trajetórias mais ordenadas, movendo-se em linhas retas.

Ainda, por meio da conexão via *wi-fi*, o robô é compatível com a Amazon, Alexa e Google Assistente, bem como é equipado com câmeras que permitem o mapeamento das casas (ou outros locais onde estejam), de modo a conhecer o tamanho dos cômodos e os móveis presentes em cada um, o que permite que a Amazon faça crescer seu grande banco de dados sobre comportamento humano.

Um dos *sites* que trouxe a notícia de tal aquisição e abordou as funcionalidades da tecnologia, o Yahoo Finanças, optou pelo título da matéria a seguinte frase: "Amazon compra empresa e fica ainda mais 'espiã'", citando ainda uma fala do CEO da iRobot em que este afirma que havia anunciado, em entrevista, que

> a última atualização de *software* do Roomba faria com que ele tivesse um conhecimento mais aprofundado do mapa da sua casa e dos seus hábitos. O robô, em vez de bater nas paredes constantemente, é capaz de memorizar onde os móveis e objetos de decoração estão de modo a eventualmente não colidir com nada, nem mesmo, com o seu dono.[47]

Com isso, a Amazon se tornou capaz de, por meio de dados adquiridos por tal dispositivo, ver dentro da residência daqueles que o adquirissem, tomando conhecimento da localização de cada cômodo da casa e dos móveis que nela estão, de possíveis obras em andamento e muito mais.

O Yahoo Finanças ainda expôs fala da diretora da divisão Alexa Smart Home, Marja Koopmans, para a qual a próxima fronteira na Inteligência Artificial não é mais informação, e sim mais contexto. Ela informou que o iRobot fornece resquícios desse contexto e, devido à utilização de armazenamento em nuvem, é capaz de compartilhar facilmente as informações com outros dispositivos. Nas palavras de Marja, "conseguimos entender a expressão 'vá para a cozinha e me pegue uma cerveja' por uma década. Mas se eu não sei onde fica a cozinha, e não sei onde fica a geladeira, e não sei como é uma cerveja, realmente não importa se eu entendo suas palavras".[48]

Verificada a capacidade do novo robô, o qual já está disponível no mercado, mostra-se válida uma abordagem não exaustiva da política de privacidade da empresa iRobot responsável pela criação do Roomba, bem como da política de privacidade adotada pela Amazon, a qual adquiriu a empresa e realiza a venda de tal equipamento.

47 AMAZON..., [2022a].
48 AMAZON..., [2022a].

A política de privacidade do iRobot estabelece que: 1) o controlador de dados, para fins das leis de proteção de dados aplicáveis, é o iRobot Corporation; 2) os dados coletados são informações do próprio usuário, de terceiros, de aplicativos e de alguns robôs; 2.1) as informações pessoais que o usuário fornece, como nome, *e-mail*, usuário e senha, histórico de compras, entre outros, também são armazenados, porém, separadamente dos dados do robô, desidentificados, com acesso restrito apenas a quem precisar; 3) a iRobot recebe informações de terceiros sobre o usuário, em situações em que o *login* realizado pelo titular dos dados é realizado por meio de rede social ou serviço de autenticação de terceiros, ou ainda podem adquirir tais informações quando ocorrer interação com as contas em rede social da empresa, por meio de ações como "curtir" ou "seguir". Essas mesmas informações são ainda utilizadas para que a iRobot consiga operar, manter e fornecer ao usuário recursos e as funcionalidades de seu serviço.[49]

Quanto ao robô, informam que: 1) sua tecnologia inteligente possibilita que transmitam dados sem fio para o serviço, os quais são armazenados em um estado desidentificado, separado das informações identificáveis; 2) ao registrar-se o robô, é armazenado o nome dado a ele pelo usuário, bem como as informações coletadas por este sobre o ambiente no qual é implantado, como sinal *wi-fi*, movimento do robô pelo ambiente, a fim de criar "mapa" do local de seu domínio, da existência e dos tipos de objeto (cadeira, mesa, geladeira, entre outros) ou obstáculos encontrados; 3) as imagens das câmeras dos robôs são coletadas a partir do consentimento do usuário; contudo, elas não ficarão visíveis à iRobot, apenas em caso em que, novamente, haja o consentimento do compartilhamento das imagens com a empresa; 4) as informações não são transmitidas pelos robôs enquanto não forem registrados *online* e conectados à rede *wi-fi* ou Bluetooth ou à *internet*, por qualquer outro método.[50]

Já a política de privacidade da Amazo volta-se ao comportamento do usuário quanto consumidor, de modo que estabelece o seguinte: 1) os dados informados são armazenados quando o usuário acessa o *site*, aplicativo ou outros serviços disponibilizados, sendo alguns opcionais e outros coletados de forma automática por meio dos *cookies*;[51] 2) ocorre compartilhamento de dados com terceiros em casos em que a Amazon entende que a liberação é apropriada ao cumprimento da lei, ou para executar as condições de uso e demais acordes, bem como para

[49] IROBOT CORPORATION, 2022.

[50] IROBOT CORPORATION, 2022.

[51] Os *cookies* são pequenos arquivos criados por sites visitados e que são salvos no computador do usuário, por meio do navegador. Estes armazenam diferentes informações e dados do usuário, como login, sua forma de navegar, quanto tempo permaneceu na página, que páginas do site foram visitadas e informações digitadas em algum formulário do *site*. *Cookies* são também comumente relacionados a casos de violação de privacidade na *web*.

proteger os direitos, propriedade ou segurança da Amazon, dos usuários ou terceiros, incluindo-se, aqui, a troca de informações com outras empresas e organizações para proteção de fraude e redução de riscos de crédito; 3) quanto ao acesso aos dados pelo usuário, o titular pode escolher não fornecer as informações, mesmo quando necessárias para realização da compra, e pode ainda adicionar ou atualizá-las, casos em que a Amazon conserva uma cópia da versão anterior em seu arquivo.[52]

Em ambas as políticas de privacidade, cita-se o necessário consentimento do usuário para que sejam os dados, em sua maioria, coletados, o que demonstra concordância com o texto legal da LGPD, o qual prevê tal consentimento, em seus arts. 5º, inciso XII, 7º, inciso I, e 14, inciso 1º. Entretanto, é evidente que, com o advento da IoT, ainda que seja ela arquitetada dentro das normas estabelecidas na LGPD, há uma mitigação do princípio da privacidade, se se considerar que sempre haverá vulnerabilidade nos dispositivos e uma enorme coleta de dados para o funcionamento deles, uma vez que, em sua essência, a IoT aplica algoritmos de Inteligência Artificial e ainda cruza informações por meio do *machine learning*, com a finalidade de gerar estatísticas capazes de detectar padrões e comportamentos dos usuários.

7 Conclusões

Conforme abordado anteriormente, a sociedade atual tem como seu elemento central a informação, tendo em vista o desenvolvimento do capitalismo, em que a informação assume cada vez mais um papel relevante, fazendo nascer uma nova forma de organização da sociedade, tanto no aspecto social quanto político e econômico. Nesse cenário, a informação tornou-se uma riqueza em todos os setores, intensificando-se no uso da tecnologia, a qual facilitou a coleta, produção, processamento, transmissão e armazenamento de dados.

Segundo a LGPD, todos os usuários possuem direito à privacidade e proteção de seus dados pessoais perante empresas públicas e privadas. Ocorre que tal contexto se mostra como um desafio à IoT, uma vez que tais dispositivos coletam uma gama de informações de seus usuários, aplicando algoritmos de inteligência artificial e cruzando tais informações de modo a gerar estatísticas capazes de detectar padrões no comportamento humano. Nesse contexto, os maiores desafios verificados da IoT são: adotar métodos para autorização da coleta do uso dos dados dos usuários pela empresa responsável; especificar padrões seguros para transmissão de dados; promover armazenamento seguro dos dados, bem como adotar procedimento que eliminem informações do usuário quando findada a relação

[52] AMAZON, [2022b].

entre este e a empresa prestadora do serviço. Isso considerando a capacidade restrita dos dispositivos IoT, tanto de memória como de processamento, uma vez que se trata de objetos do cotidiano.

Além disso, essa "onipresença" da IoT traz questionamentos significativos sobre a privacidade dos indivíduos e em como tratar essa diversidade de requisitos para segurança dos serviços. Isso demonstra o necessário desenvolvimento de soluções de segurança adaptáveis, centradas no usuário, como por meio do gerenciamento de perfis e políticas de segurança e de privacidade. Busca-se, assim, preservar a autonomia dos usuários, a fim de que estes permaneçam no controle de suas próprias informações.

Como um dos meios possíveis para se garantir a autonomia, pode-se pensar na adoção mais clara e efetiva das políticas de privacidade. Mas não uma política de privacidade impositiva, em que o indivíduo tem suas opções reduzidas apenas ao "aceito" ou "não aceito" tais termos, o que influencia a prestação do serviço de determinado equipamento. Mas sim adotar, por exemplo, o método de *checklist*, em que os tópicos sobre o tratamento dos dados, tantos os necessários ao funcionamento de determinado dispositivo quanto aqueles usados apenas para aperfeiçoar a prestação de serviços, poderiam ser lidos em tópicos e habilitados ou desabilitados pelo usuário, conforme sua preferência. Claro que os dados indispensáveis ao funcionamento do equipamento permaneceriam sendo coletados e tratados dentro da lei, o que deve aparecer de forma clara ao usuário; porém, aqueles dados não essenciais poderiam ter coleta desabilitada pelo usuário. Tal modelo de *checklist* ainda proporcionaria uma leitura mais agradável e menos cansativa ao indivíduo.

Ainda, tendo em vista as boas práticas de segurança, as quais a LGPD buscou prever, bem como ocorre com a Regulamento Geral de Proteção de Dados (RGPD) aplicado na Europa, cita-se aqui a importância da adoção do *privacy by design* e do *privacy by default*, os quais destacam a importância de ser considerada a privacidade desde os estágios iniciais do *design* e durante todo o processo de desenvolvimento do produto, do serviço e dos processos que envolverão o tratamento dos dados pessoais e, junto ao *design*, considerar também as opções que o sistema ou serviço disponibilizarão ao indivíduo, demonstrando a quantidade de dados pessoais que serão por ele compartilhados, devendo ser as configurações padrão as mais favoráveis à privacidade.[53]

A insuficiência do espectro normativo analógico como função ordenadora capaz de conceder respostas aos problemas, ora referenciado, reivindica uma

[53] ALVES; PEIXOTO; ROSA, 2021, p. 13.

construção teórica robusta e intensa sobre a regulação digital, capaz de definir um regime jurídico próprio, instrumentos de cautela e prevenção contra uso inadequado e antidemocrático dos dados, plataformas e máquinas robôs para direcionamento de escolhas públicas e privadas.[54]

Com isso, verifica-se a necessidade de regulamentação dos procedimentos de segurança a serem aplicados pelos responsáveis pelo tratamento dos dados pessoais, a fim de que haja garantia da integridade, da disponibilidade, da autenticidade, do sigilo das informações, sendo esses os quatro pilares da segurança da informação, os quais devem ser observados junto aos princípios relacionados à proteção dos dados pessoais, bem como dos direitos resguardados aos titulares dos dados, como os direitos à oposição, à informação, ao acesso e à eliminação.

Referências

ALLHOFF, Fritz; HENSCHKE, Adam. The Internet of Things: foundational ethical issues. *Internet Of Things*, v. 1-2, p. 55-66, set. 2018. DOI: http://dx.doi.org/10.1016/j.iot.2018.08.005.

AMAZON compra empresa e fica ainda mais 'espiã'. *Yahoo! Finanças*, [2022a]. Disponível em: https://br.financas.yahoo.com/noticias/amazon-quer-espionar-dentro-de-sua-casa-231348602.html?_guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADgR39pmzRQ_Azs9kGp5mTN4E5BbjJ4YCiBt8_tq8A5DgksR_isyVbdS4Bz7iFTJPgbLNA4mjS5HBYaBMIc8ctQ1xD5oTjcVdWZbUSX5YD89JWI2_npX5ikq-886qa2ufM0hzKnFgHRobR3f8rWyi2mGIkvuBijggZOzmczf3HwG&guccounter=2. Acesso em: 30 out. 2022.

AMAZON. Notificação de Privacidade da Amazon, [2022b]. Disponível em: https://www.amazon.com.br/hz/cs/help?nodeId=GX7NJQ4ZB8MHFRNJ. Acesso em: 30 out. 2022.

ALVES, David; PEIXOTO, Mario; ROSA, Thiago. *Internet Das Coisas (IoT)*: segurança e privacidade dos dados pessoais. Rio de Janeiro: Alta Books, 2021. 256 p.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. *Revista de Investigações Constitucionais*, v. 4, n. 3, p. 167-200, set./dez. 2017.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019. 328 p.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. São Paulo: Grupo GEN, 2021. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 29 out. 2022.

BRASIL. Decreto nº 592, de 6 de julho de 1992. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Pacto Internacional Sobre Direitos Civis e Políticos. *Diário Oficial da União*: Brasília, DF, 6 jul. 1992a. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 01 out. 2022.

[54] VALLE; GALLO, 2020, p. 78.

BRASIL. Decreto nº 678, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Convenção Americana Sobre Direitos Humanos. *Diário Oficial da União*: Brasília, DF, 9 nov. 1992b. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 01 out. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09 set. 2022.

BRASIL. Ministério Público Federal. Secretaria de Cooperação Internacional. *Tratados de direitos humanos*: Sistema Internacional de Proteção aos Direitos Humanos. Convenção Europeia para a Proteção dos Direitos humanos e das Liberdades Fundamentais, v. 4, Brasília, 2016.

BARATI, Masoud *et al*. GDPR Compliance Verification in Internet of Things. *IEEE Access*, v. 8, 29 jun. 2020. Disponível em: https://ieeexplore.ieee.org/document/9127459. Acesso em: 22 out. 2022.

CASTELLS, Manuel. *A sociedade em rede*. Tradução: Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 2013. 355 p.

COUNCIL OF EUROPE. Europe Court of Human Rights. *Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais* (1950), 4 nov. 1950. Disponível em: https://www.echr.coe.int/documents/d/echr/convention_por. Acesso em 07 set. 2022.

CRISTÓVAM, José Sérgio da Silva; HAHN, Tatiana Meinhart. Administração pública Orientada por Dados: Governo Aberto e Infraestrutura Nacional de Dados Abertos. *Revista de Direito Administrativo e Gestão Pública*, v. 6, n. 1, p. 1-24, jan./jun. 2020. DOI: http://dx.doi.org/10.26668/IndexLawJournals/2526-0073/2020.v6i1.6388.

EUROPEAN UNION. *Charter Of Fundamental Rights Of The European Union*, 7 dez. 2000. Disponível em: http://data.europa.eu/eli/treaty/char_2016/oj. Acesso em: 7 set. 2022.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da* USP, São Paulo, v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 25 out. 2022.

FROM, Danieli Aparecida; REZENDE, Denis Alcides. Modelo de Prestação de Serviços Públicos Municipais Conectados por meio da Internet das Coisas no Contexto da Cidade Digital Estratégica. *Contribuciones A Las Ciencias Sociales*, p. 15-28, 6 jul. 2021.

FORNASIER, Mateus de Oliveira. A aplicabilidade da Internet das Coisas (IoT) entre os direitos fundamentais à saúde e à privacidade. *Revista de Investigações Constitucionais*, Curitiba, v. 6, n. 2, p. 297-321, maio/ago. 2019.

FINANÇAS, Redação. Amazon compra empresa e fica ainda mais 'espiã'. *Yahoo Finanças*, 7 ago. 2022. Disponível em: https://br.financas.yahoo.com/noticias/amazon-quer-espionar-dentro-de-sua-casa-231348602.html?guccounter. Acesso em: 23 out. 2022.

GABARDO, Emerson; MENENGOLA, Everton; SANMIGUEL, Nancy Nelly González. A proposta europeia de regulação da Inteligência Artificial. *Sequência Estudos Jurídicos e Políticos*, v. 43, n. 91, 2023. DOI: 10.5007/2177-7055.2022.e91435. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/91435. Acesso em: 15 abr. 2023.

GARCIA, Rafael de Deus. Os direitos à privacidade e à intimidade: origem, distinção e dimensões. *Revista da Faculdade de Direito do Sul de Minas*, Pouso Alegre, v. 34, n. 1, p. 1-26, 2018. Disponível em: https://revista.fdsm.edu.br/index.php/revistafdsm/article/view/257. Acesso em: 24 out. 2022.

GONET BRANCO, Paulo Gustavo. Direitos fundamentais em espécie. *In:* GONET BRANCO, Paulo Gustavo. *Curso de direito constitucional*. 4. ed. São Paulo: Saraiva, 2009.

GIANTOMASO, Isabela. Entenda como funciona a tecnologia do robô aspirador de pó. *Techtudo*, 5 jul. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/07/entenda-como-funciona-a-tecnologia-do-robo-aspirador-de-po.ghtml. Acesso em: 23 out. 2022.

IROBOT CORPORATION. Política de Privacidade. *iRobot*, 2022. Disponível em: https://www.irobot.com.br/Legal/Privacy-Policy. Acesso em: 30 out. 2022.

LAFER, Celso. *A reconstrução dos direitos humanos um diálogo com o pensamento de Hannah Arendt*. São Paulo: Schwarcz, 1991. 406 p. Disponível em: https://mpassosbr.files.wordpress.com/2013/03/a-reconstruc3a7c3a3o-dos-direitos-humanos-celso-lafer.pdf. Acesso em: 28 set. 2022.

MOREIRA, Egon Bockmann. Direitos Fundamentais para Humanos Digitais. *Gazeta do Povo*, 19 ago. 2019. Disponível em: https://www.gazetadopovo.com.br/vozes/egon-bockmann-moreira/direitos-fundamentais-para-humanos-digitais/. Acesso em: 5 outubro de 2022.

PATACA, Campos Calenga. A Internet das Coisas: Tipologias, Protocolos e Aplicações. *The Law, State and Telecommunications Review*, v. 13, n. 2, p. 198-220, 2021. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/32773. Acesso em: 22 out. 2022.

PORTELA, Irene Maria; MOTTA, Ivan Dias da; ABAGGE, Yasmine de Resende. O uso dos dados pessoais nas políticas públicas de combate à covid-19. *Revista Jurídica*, v. 4, n. 61, p. 70-90, out. 2020. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/4478/371372683. Acesso em: 15 out. 2022.

SCHERMER, Bart Willem. *Software agents, surveillance, and the right to privacy*: a legislative framework for agent-enabled surveillance. Leiden: Imprensa da Universidade de Leiden, 2007. 241 p. Disponível em: https://hdl.handle.net/1887/21094. Acesso em: 10 out. 2022.

SILVA, Daniel Pereira Militão. *Desafios do ensino jurídico na pós-modernidade*: da sociedade agrícola e industrial para a sociedade da informação. 2009. 280 f. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2009.

SPIECKER DE OLIVEIRA, Nairobi *et al*. Segurança da Informação para Internet das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). *Revista Eletrônica de Iniciação Científica em Computação*, São Leopoldo, v. 17, n. 4, 2019. Disponível em: https://seer.ufrgs.br/reic/article/view/88790. Acesso em: 09 out. 2022.

SETHI, Pallavi; SARANGI, Smruti R. Internet of Things: architectures, protocols, and applications. *Journal Of Electrical and Computer Engineering*, v. 2017, p. 1-25, 2017.

URQUHART, Lachlan; LODGE, Tom; CRABTREE, Andy. Demonstrably doing accountability in the internet of things. *International Journal of Law and Information Technology*, v. 27, n. 1, p. 1-27, 2019. DOI: https://doi.org/10.1093/ijlit/eay015.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2007. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.D76AACD6&lang=pt-br&site=eds-live. Acesso em: 3 out. 2022.

VALLE, Vivian Cristina Lima López; GALLO, William Ivan. Inteligência Artificial e Capacidades Regulatórias do Estado no Ambiente da administração pública Digital. *A&C – Revista de Direito Administrativo & Constitucional*, Belo Horizonte, v. 20, n. 82, p. 67-86, out./dez. 2020

ZANETTI DE OLIVEIRA, Dânton Hilário; FREITAS, Cinthia Obladen de Almendra. *Big Data e os limites à livre iniciativa no âmbito da Lei Geral de Proteção de Dados Pessoais.* 2022. 198 f. Dissertação (Mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2022. Disponível em: https://archivum.grupomarista.org.br/pergamumweb/vinculos/0000a6/0000a635.pdf. Acesso em: 3 out. 2022.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

VALLE, Vivian Lima López; BARBOSA, Bruna Gavron. Os desafios quanto a preservação da privacidade e da proteção de dados em face dos equipamentos IoT. *International Journal of Digital Law*, Belo Horizonte, ano 4, n. 1, p. 35-61, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.valle.

DOI: 10.47975/digital.law.vol.4.n.1.tedrus

Hipótese de tratamento de dados sensíveis: dado biométrico e relação de trabalho[I]

Sensitive data processing hypothesis: biometric data and work relationship

Rafael Tedrus Bento*
Pontifícia Universidade Católica de São Paulo (São Paulo, São Paulo, Brasil)
rafaeltedrus@gmail.com
https://orcid.org/0000-0003-2677-5595

Recebido/Received: 19.02.2023/ February 19th 2023
Aprovado/Approved: 09.06.2023/ June 9th 2022

Resumo: Este artigo busca responder à seguinte questão: O art. 74, §2º, da CLT constitui hipótese para o tratamento de dado biométrico? Ou, como há três opções, o dado biométrico precisa de consentimento específico? Para tanto, far-se-á uma busca legislativa, jurisprudencial e acadêmica sobre entendimentos relacionados ao art. 74, §2º, da CLT e à LGPD e os princípios norteadores das áreas em questão, buscando-se, inclusive, entendimentos junto à União Europeia como método de abranger a pesquisa.

Palavras-chave: LGPD. Dado biométrico. Consentimento. Dado sensível. Tratamento de dados.

Sensitive data processing hypothesis: Biometric data and work relationship

Abstract: This article seeks to answer the following question: art. 74, §2, of the CLT, constitutes a hypothesis for the treatment of biometric data? Or, since there are three options, does biometric data need specific consent? Therefore, a legislative, jurisprudential and academic search will be carried out on understandings related to art. 74, §2, of the CLT, the LGPD, and the guiding principles of the areas in question, even seeking understandings with the European Union as a method of covering the research.

Keywords: LGPD. Biometric data. Consent. Sensitive data. Processing data.

[I] Como citar esse artigo/How to cite this article: BENTO, Rafael Tedrus. Hipótese de tratamento de dados sensíveis: dado biométrico e relação de trabalho. *International Journal of Digital Law*, Belo Horizonte, v. 4, n. 1, p. 63-75, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.tedrus.

* Doutorando em Direito pela Pontifícia Universidade Católica de São Paulo (São Paulo-SP, Brasil). Mestre em Direitos Humanos e Desenvolvimento Social pela Pontifícia Universidade Católica de Campinas (PUC Campinas), com período integrado ao Mestrado em Direito da União Europeia da Universidade do Minho (UMinho). Especialista em Direito do Trabalho pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Especialista em Direito Empresarial pelo INSPER. *E-mail*: rafaeltedrus@gmail.com.

Sumário: 1 Introdução – **2** Por existirem dois outros meios de controle de ponto, seria o tratamento de dado biométrico cumpridor do princípio da necessidade? – **3** O General Data Protection Regulation e o dado biométrico – **4** Conclusão – Referências

1 Introdução

A relação de trabalho é uma verdadeira fonte de dados pessoais, e, em relação à proteção desses dados nas relações empregatícias, um dos pontos mais agudos é o atinente à categoria dos dados pessoais sensíveis.[1]

A Constituição Federal do Brasil de 1988 protege os direitos da personalidade do trabalhador e a sua condição de dignidade: "Art. 5º (...) X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação."

No tocante ao tema da proteção dos dados pessoais sensíveis nas relações empregatícias, uma questão que se destaca é o tratamento dos dados biométricos para fins de registro de ponto. No cenário brasileiro, o mais corriqueiro é que esse controle se dê por meio da impressão digital, com o objetivo de conceder maior fidedignidade em relação à realidade da jornada e a veracidade daquele que a está marcando. Além disso, possibilita garantir o real cumprimento da jornada, bem como de obrigações dela decorrentes, a exemplo da hora extra.[2]

O art. 74 da CLT estipula a necessidade de registro de ponto, admitindo que tal controle se dê por meio manual, mecânico ou eletrônico.[3] A Portaria nº 1.510/2009, do então Ministério do Trabalho, por sua vez, autorizou o registro de ponto biométrico de empregado, trazendo os requisitos para sua validade, mas sem mencionar expressamente a possibilidade de controle biométrico. O regulamento foi revogado pela Portaria MPT nº 671/21, que também não disciplinou de forma específica o modelo de controle biométrico, apenas trouxe as diretrizes gerais de validade dos registros.[4]

O modelo de controle biométrico, embora permitido para simplificar e garantir maior segurança ao controle da jornada, ganhou novos contornos com a entrada em vigor da Lei nº 13.709/18 (LGPD), que dispôs sobre o regime jurídico pátrio do

1 MOREIRA, 2010.

2 JÚNIOR; FERREIRA, 2020.

3 "Art. 74. O horário de trabalho será anotado em registro de empregados.
(...)
§2º Para os estabelecimentos com mais de 20 (vinte) trabalhadores será obrigatória a anotação da hora de entrada e de saída, em registro manual, mecânico ou eletrônico, conforme instruções expedidas pela Secretaria Especial de Previdência e Trabalho do Ministério da Economia, permitida a pré-assinalação do período de repouso."

4 BRASIL, 2021.

tratamento de dados pessoais. A LGPD, em seu artigo 5º, II, classificou os dados biométricos como dados pessoais sensíveis. Assim, levantou-se o questionamento sobre a verdadeira necessidade do seu uso no ambiente de trabalho e sua compatibilidade com a LGPD.[5]

O tratamento de tais dados exige um rigor mais acentuado, isso porque eles, diferentemente dos outros, disciplinam informações que podem gerar discriminações sobre a pessoa a quem se refere.[6] Frisa-se que biometria não se restringe à impressão digital; pode ser extraída a partir da íris, face, voz ou até mesmo da deambulação.[7]

---

5 PINHEIRO; BOMFIM, 2020.

6 "Seção II

Do Tratamento de Dados Pessoais Sensíveis

"Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o §5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

I - a portabilidade de dados quando solicitada pelo titular; ou

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

§5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários."

7 PINHEIRO; BOMFIM, 2020.

No Brasil, não há manifestação expressa Autoridade Nacional de Proteção de Dados Pessoais (ANPD) abordando o tratamento dos dados biométricos. Entretanto, encontramos julgamento proferido pelo Tribunal Superior do Trabalho sobre o tema:

> (...) 2. JORNADA DE TRABALHO. HORAS EXTRAS. Segundo o Tribunal de origem, havia o registro de ponto via biometria pelo reclamante e o consequente recebimento do respectivo recibo diário da jornada de trabalho cumprida; documentos esses que atestavam a existência de horas extras laboradas pelo reclamante, a denunciar, portanto, que não havia a marcação inflexível da jornada de trabalho. Assim, diante desse contexto, não há se cogitar em contrariedade à Súmula nº 338, I, do TST. (...).[8]

A Academia, também, admite o uso de controles biométricos para registro de jornadas, justificando a sua utilização pelo cumprimento de obrigação legal. Nesse sentido, lecionam Vólia Bomfim Cassar e Iuri Pinheiro que não seria necessário o consentimento do empregado para a utilização dos dados biométricos, pelo fato de o controle da jornada pelo empregador decorrer de uma obrigação legal, conforme já exposto, o que estaria respaldado com base no artigo, 11, II, "a", da LGPD:

> O tratamento do dado biométrico para fins de jornada estaria, assim, assegurado pelo cumprimento de obrigação legal pelo controlador (art. 11, II, a, da LGPD). Além disso, o registro biométrico também pode ser utilizado para outras formas de controle de acesso e segurança na empresa, o que também se legitimaria mesmo sem o consentimento do titular pela alínea "g" do mesmo dispositivo para "garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.[9]

Dessa forma, a CLT, ao atribuir ao empregador o encargo de controle de jornada, faz com que o tratamento dos dados biométricos para fins de registro de ponto se enquadre na base jurídica do cumprimento de obrigação legal. Assim, sempre que obrigado por lei ou regulamento administrativo, o controlador poderá tratar os dados pessoais sem consentimento do titular.

Importante salientar que a LGPD justifica o tratamento diante de finalidades expressas e claras, além de impor que cada tratamento deverá ter sua base legal, indicando 10 fontes utilizáveis, em seu art. 7º, quais sejam, (i) consentimento;

[8] BRASIL, 2021.
[9] PINHEIRO; BOMFIM, 2020.

(ii) cumprimento de obrigação legal ou regulatória; (iii) execução de políticas públicas; (iv) estudo por órgão de pesquisa; (v) execução de contrato; (vi) exercício regular de direito em processo judicial administrativo ou arbitral; (vii) proteção da vida; (viii) tutela da saúde; (ix) legítimo interesse; (x) proteção ao crédito.

No caso analisado, a base legal que justifica essa utilização dispensa a necessidade de consentimento do empregado, e, portanto, não é necessário que o empregador colete o consentimento de cada empregado para utilizar o dado biométrico para o fim declarado. Nesse cenário, destaca-se o exposto por Lilian de Souza Castelani:

> O Princípio que pode suscitar dúvidas sobre a legitimidade de utilização desse tipo de dado é da Necessidade ou Minimização, já que existem outros meios supostamente menos invasivos e que permitem o controle de ponto (folha manual ou cartão magnético).
> Conquanto seja possível, de fato, assinalar a jornada por outros meios diversos da biometria, não há meio tão eficaz quanto este para assegurar a integridade dos horários lançados nos respectivos registros e a autoria.
> E a fidedignidade desses registros é essencial e extremamente saudável para ambas as partes, evitando alegações de desvirtuamento da jornada pela existência, por exemplo, de controle paralelo e permitindo a justa e real apuração do saldo de horas.
> O tratamento do dado biométrico para fins de jornada estaria, assim, assegurado pelo cumprimento de obrigação legal pelo controlador (art. 11, II, a, da LGPD).[10]

Cabe ressaltar que o uso da biometria, seja para registro de ponto, seja para acesso à empresa, garante direitos fundamentais, como o da própria integridade física, que sobrepor-se-á em relação aos de caráter infraconstitucional.

No ambiente de trabalho, o uso de dado biométrico do empregado pode não se limitar apenas à questão de registro de jornada, sendo frequentemente utilizado para permitir o acesso à empresa e considerado um mecanismo de segurança do ambiente empresarial, em que somente pessoas autorizadas poderiam adentrar o local. Isso seria legítimo mesmo sem o consentimento do titular pela alínea "g" do mesmo dispositivo; ou seja, nesse caso, a base legal adequada tampouco seria o consentimento do empregado, uma vez que a legislação teria autorizado o uso do dado sensível sem autorização do seu titular para os casos de "garantia da prevenção à fraude e a segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos", nos termos do artigo 11, "g", da LGPD.

[10] PINHEIRO; BOMFIM, 2020.

É imperioso destacar que, mesmo nessas hipóteses excepcionais, não deve existir abusos; os dados deverão ser utilizados com a finalidade estrita para a qual foram colhidos, com a criação de mecanismos para o tratamento e proteção, sob pena de violação aos ditames da Lei Geral de Proteção de Dados.

Em síntese, o consentimento do trabalhador para tratamento dos dados biométricos em caso de registro de ponto não é necessário, mas ele deve ser informado das operações realizadas com tais dados, atentando-se ao fundamento da autodeterminação informada (art. 2º, inciso II, da LGPD) e ao princípio da transparência (art. 6º, inciso VI, da LGPD). O ideal, inclusive, é que tal fato seja definido em cláusula contratual ou adento ao contrato de trabalho, constando, ainda, na política de tratamento de dados interna da empresa.

2 Por existirem dois outros meios de controle de ponto, seria o tratamento de dado biométrico cumpridor do princípio da necessidade?

O princípio da necessidade, previsto no artigo 6º, III, da LGPD, consubstancia-se na limitação da realização do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Segundo Marcio Pestana, o princípio da necessidade é "a necessidade, ao seu turno, poderá ser compreendida como a adoção de um meio que, a par de preencher o requisito de adequação à finalidade almejada, seja o menos gravoso para o indivíduo e para o interesse público".[11]

Pela regra contida na LGPD, a realização do tratamento de dados ocorrerá se e quando o atingimento de determinada finalidade se mostrar relevante. No caso, somente deverão ser tratados os dados pertinentes, isto é, aqueles que se mostrem imprescindíveis para que o objetivo previamente traçado seja atingido. Ainda, a manipulação desses dados deve ser instruída pela proporcionalidade, não havendo excessos.

A lógica do princípio da necessidade que norteia a LGPD traz um questionamento acerca da utilização dos dados biométricos para fins de controle de jornada, uma vez que existem outros métodos menos invasivos de controle de ponto, como o registro em folha de ponto manual ou por meio de cartão magnético.

Contudo, esses meios citados não são tão eficazes de assegurar a integridade dos horários lançados e a autoria da marcação quanto o ponto eletrônico por biometria. Segundo Pinheiro e Volia, "a fidedignidade desses registros é essencial e

[11] PESTANA, 2014.

extremamente saudável para ambas as partes, evitando alegações de desvirtuamento da jornada pela existência, por exemplo, de controle paralelo e permitindo a justa e real apuração do saldo de horas".[12]

Portanto, é importante ressaltar que, a veracidade das informações obtidas pelos dados biométricos é essencial para ambas as partes, evitando alegações de desvirtuamento da jornada.

Diante do contexto mencionado, é possível afirmar que a utilização dos dados biométricos vem se mostrando há anos como a forma mais eficaz, confiável e segura de controle de ponto, evitando e diminuindo alegações de desvirtuamento da jornada pela existência de outros meios de controle, assegurando a integridade dos horários registrados e a autoria em relação à marcação.

O tratamento de dados biométricos é cumpridor do princípio da necessidade, ao passo que os demais meios não se apresentam de forma tão eficaz para atingir o fim declarado.

Entretanto, no caso concreto, deverá ser observada a intenção do empregador, de modo que deve restar inequívoco que os dados obtidos estão sendo utilizados com a finalidade estrita para os quais foram colhidos. Essa necessidade de estar sempre demonstrado que o tratamento dos dados se dê com uma finalidade estritamente necessária, adequada e proporcional, traz para os empregadores o ônus de comprovar que estão tomando todas as medidas adequadas com o objetivo de equilibrar a intenção de se chegar a uma finalidade e o respeito à liberdade dos empregados e titulares dos dados fornecidos.

Em síntese, é imperiosa a adoção de medidas para segurança desses dados biométricos coletados. Dessa forma, evitando a violação de direitos de personalidade dos empregados e inadequação à norma protetora dos dados pessoais.

3 O General Data Protection Regulation e o dado biométrico

O General Data Protection Regulation (GDPR) é o regulamento do direito da União Europeia sobre tratamento de dados pessoais. O regulamento é um componente importante da abordagem centrada no ser humano e uma bússola para o uso da tecnologia e nas transições digitais que caracterizam a formulação de políticas da União.[13]

Ele foi elaborado por meio de um processo legislativo complexo e duradouro. Em sua origem, os formuladores de políticas europeias iniciaram um processo que envolveu uma série de consultas a especialistas, o que gerou uma profunda

[12] PINHEIRO; BOMFIM, 2020.
[13] TZANOU, 2019.

sofisticação regulatória sobre como as práticas de informação podem ser manipuladas para escapar das metas regulatórias.[14]

O regulamento consiste em um documento de quase 100 páginas. A extensão e complexidade da norma decorre do número de direitos para titulares de dados, dentre eles o direito ao esquecimento, o direito à portabilidade de dados pessoais e o direito de resistir à criação de perfis automatizados. No mesmo sentido, o número de funções atribuídas aos controladores de dados pessoais (encarregados de dados, no caso da União Europeia) foi significativamente alargadas por meio da introdução de um dever de responsabilidade, deveres relativos às avaliações de impacto de proteção de dados, o dever de nomear um oficial de proteção de dados pessoais e uma obrigação de notificação após a ocorrência de uma violação sobre os dados pessoais.[15]

No que tange aos dados biométricos, é relevante destacar que o Regulamento Geral de Proteção de Dados, em seu art. 4 (14), define que dados biométricos são aqueles "dados pessoais resultantes de um tratamento técnico específico relativo às características físicas ou comportamentais de uma pessoa singular que permitem confirmar a identificação única, tais como imagens faciais ou dados de impressões digitais, entre outros".

A respeito do tratamento de dados no trabalho, o Grupo de Trabalho (*Working Party*) 29,[16] em seu Parecer nº 02/2017, concluiu favoravelmente à utilização da biometria no caso de controle de ponto, desde que os dados fossem tratados exclusivamente para essa finalidade. E alerta que, "embora tais sistemas possam constituir uma importante componente de uma pista de auditoria de um empregador, colocam também o risco de proporcionar um nível de conhecimento e controle invasivo das atividades do empregado no local de trabalho".[17]

Ainda em seu Parecer nº 3/2012 sobre a evolução das tecnologias biométricas, o órgão consultivo desaconselhou, veementemente, um armazenamento centralizado de dados biométricos, pois usualmente há fraqueza quando oferecem um único ponto de destino/exploração.[18] Embora reconheça-se que, para fins específicos e na presença de necessidades objetivas, um banco de dados centralizado com dados biométricos pode ser considerado admissível, o uso de modelos criptografados em

[14] HOOFNAGLE; VAN DER SLOOT; BORGESIUS, 2019, p. 68.
[15] HOOFNAGLE; VAN DER SLOO; BORGESIUS, 2019, p. 73.
[16] Cumpre ressaltar que o Grupo de Trabalho do artigo 29 (WP29) foi um órgão consultivo da Comissão Europeia para prestar assessoria sobre temas ligados à proteção de dados pessoais. O órgão foi substituído pelo Conselho Europeu de Proteção de Dados (EDPB), a partir da entrada em virgo do Regulamento Geral de Proteção de Dados da UE (Regulamento (EU) 2016/679).
[17] EUROPEAN COMISSION, [2017].
[18] "O Grupo de Trabalho alerta para os riscos decorrentes da utilização de dados biométricos para efeitos de identificação em grandes bases de dados centralizadas, devido às consequências potencialmente nocivas para as pessoas a que os dados se referem" (EUROPEAN COMISSION, [2017]).

mídia de propriedade exclusiva do titular dos dados (ou seja, cartões inteligentes ou dispositivos semelhantes) é considerado geralmente preferível. Nesse caso, uma chave de criptografia específica para os dispositivos de leitura deve ser usada como uma proteção eficaz para proteger os dados pessoais biométricos contra acesso não autorizado.[19]

Dessa forma, podemos indicar que o princípio da proteção de dados desde a concepção dos sistemas de tratamento (*privacy by design*) até a criação de meios de contenção de defeitos das operações (*privacy by default*") são os definidores finais deste tópico, como forma práticas da execução e processamento de dados pessoais de forma segura e razoável.[20] Tendo em vista que a conformidade é parcialmente responsabilidade do controlador, os controladores devem inserir garantias legais e verificações para garantir que o processamento de dados pessoais (inclusive os biométricos) esteja e permaneça em conformidade com a lei de proteção de dados pessoais e seu princípios.[21]

Na prática, podemos ressaltar que tribunal da Alemanha entendeu que o controle de jornada mediante uso de dados biométricos pode ser considerado excessivo, ensejando aplicação de sanções. Nesse sentido, a Corte de Apelação do Trabalho na Alemanha julgou ilegal o uso de sistema de marcação de jornada por meio de biometria.[22] No presente caso, a reclamante era funcionária de uma clínica de radiologia e anteriormente, a empresa utilizava um sistema de registo do tempo de trabalho baseado em formulários em papel, que o empregado preenchia sempre que chegava e saía do escritório.

Porém, em julho de 2018 a companhia decidiu implementar um novo sistema que utiliza as terminações e ramificações das bordas papilares da impressão digital humana dos funcionários para sua identificação e registro do tempo de trabalho. Um funcionário se recusou a ter suas impressões digitais digitalizadas como forma de registrar as horas de trabalho e continuou a registrar suas horas de trabalho em papel.

A empresa emitiu dois avisos ao funcionário, o segundo informando que o funcionário seria demitido caso não iniciasse imediatamente o novo sistema. Em resposta, o funcionário entrou com uma ação no Tribunal de Berlim, alegando que, se fosse obrigado a usar suas impressões digitais como meio de registrar suas horas de trabalho, seus direitos pessoais seriam violados. Em conclusão, o

[19] "O Grupo de Trabalho concorda que a tecnologia da cifragem biométrica é um domínio fértil para a investigação e está suficientemente amadurecida para a integração em medidas políticas, o desenvolvimento de protótipos e a apreciação de pedidos" (EUROPEAN COMISSION, [2012]).
[20] WALDMAN, 2018, p. 160-161.
[21] VICENTE; CASIMIRO, 2020, p. 12.
[22] ALEMANHA. 2019.

tribunal concordou com os argumentos do empregado, em julgamento datado de 16 de outubro de 2019.

A empresa recorreu, mas o tribunal de apelação confirmou o julgamento inicial. Considerou que, no caso em questão, o uso de impressões digitais para registrar o tempo não era necessário e manteve o caso. O registro de dados, no caso, constituía dados biométricos na acepção do art. 9(1) RGPD, e estes pertenciam a categorias especiais de dados pessoais. Assim, o tratamento desses dados no contexto das circunstâncias laborais só seria admissível se o tratamento fosse necessário para efeitos do exercício de direitos ou cumprimento de obrigações legais decorrentes da relação de trabalho, e se não existissem motivos para presumir que o trabalhador tinha um direito legítimo superior interesse em excluir tal processamento.

Ainda, sobre o tema da possibilidade de utilização do consentimento do empregado para fins da relação de trabalho, a Lei Geral de Proteção de Dados brasileira não trouxe disposição específica quanto ao uso do consentimento. Já no âmbito da União Europeia, vale registrar que o Grupo de Trabalho do Artigo 29 disponibilizou guia que traz a preocupação jurídico do uso do consentimento no tratamento de dados pessoais de empregados, visto que há claro desequilíbrio de poder em contexto laboral, nos seguintes termos:

> Por conseguinte, o GT29 considera problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos seus trabalhadores atuais ou futuros com base no consentimento, uma vez que é improvável que esse consentimento seja dado de livre vontade. Relativamente à maior parte deste tratamento de dados no local de trabalho, o fundamento legal não pode nem deve ser o consentimento dos trabalhadores [artigo 6.º, n.º 1, alínea a)], devido à natureza da relação entre empregador e trabalhador.[23]

Nesse mesmo sentido, o GDPR traz, em suas justificativas iniciais, o "Considerando 43",[24] o qual indica que o consentimento não terá fundamento jurídico válido quando houver desequilíbrio entre o titular dos dados e o responsável pelo seu

[23] EUROPEAN COMISSION, [2016].

[24] A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade, se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

tratamento. Já o "Considerando 155"[25] informa acerca do direito do Estado-membro ou das convenções coletivas das categorias poderem prever regras para o tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente no que respeita às condições em que os dados pessoais podem ser tratados no contexto laboral, em especial, com base no consentimento do empregado.

Dessa forma, observa-se que o tratamento de dados pessoais, no contexto laboral, detém necessárias preocupações adicionais, em especial sobre o uso de dados sensíveis e, também, na hipótese de tratamento sob o uso do consentimento do empregado, em decorrência da especial disparidade de poder sobre os entes. Adiciona-se que a União Europeia entende que, caso haja disposição legal nacional ou regulamentação setorial, é possível a utilização desses itens, desde que formulado com salvaguardas específicas sobre o tema.

4 Conclusão

A privacidade da pessoa abrange o direito de manter privadas as funções e características do corpo (como códigos genéticos e biometria). O corpo humano tem uma forte dimensão simbólica, como resultado da integração do corpo físico e da mente, e é intrínseco aos valores culturais da sociedade.[26] Pensa-se que a privacidade da pessoa conduz a sentimentos individuais de liberdade e ajuda a apoiar uma sociedade democrática ajustada.[27]

A relação entre empregador e empregado é marcada pela vulnerabilidade deste em decorrência da relação de subordinação, de forma que se pode questionar se esse consentimento foi dado espontaneamente.

Salienta-se que os princípios da necessidade e da transparência devem ser os nortes para a criação e implementação de salvaguardas específicas sobre o tema, para que, assim, seja possível o tratamento de dados pessoais, com a inserção de hipótese de tratamento legal e justa. Inclusive, caso o consentimento seja uma das formas de obtenção da autorização para tratamento dos dados, faz-se necessário que as informações fornecidas permitam ao titular determinar as consequências do consentimento, com a possibilidade de sua exclusão a qualquer momento.

---

[25] O direito do Estado-membro ou as convenções coletivas (incluindo "acordos setoriais") podem prever regras específicas para o tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente no que respeita às condições em que os dados pessoais podem ser tratados no contexto laboral, com base no consentimento do assalariado, para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas por lei ou por convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no trabalho, de saúde e segurança no trabalho, e para efeitos de exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

[26] MORDINI, 2011.

[27] FINN; WRIGHT; FRIEDEWALD, 2013.

Por esse exposto, as organizações são obrigadas a obter o consentimento explícito dos indivíduos antes de coletar, usar ou compartilhar seus dados pessoais e devem informar os indivíduos sobre a finalidade da coleta de dados, por quanto tempo os dados serão mantidos e quem terá acesso a eles. As organizações também devem implementar medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acesso, alteração ou destruição não autorizados.

Referências

AGUIAR, Antonio Carlos. A Lei Geral de Proteção de Dados e seus impactos no direito do trabalho. *Revista Ltr: Legislação do Trabalho*, São Paulo, v. 82, n. 6, p. 655-661, jun. 2018.

ALEMANHA. Tribunal Regional de Berlim. *Processo: 229 Ca 5451/19*, 2019. Disponível em: http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/portal/t/279b/bs/10/page/sammlung.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=JURE200011045&doc.part=L&doc.price=0.0#focuspoint. Acesso em: 16 maio 2023.

BRASIL. *PORTARIA/MTP nº 671, de 8 de novembro de 2021*. Disponível em: https://in.gov.br/en/web/dou/-/portaria-359094139. Acesso em: 16 maio 2023

CONI JÚNIOR, Vicente Vasconcelos; PAMPLONA FILHO, Rodolfo. A *Lei Geral de Proteção de Dados e seus reflexos nas relações jurídicas trabalhistas*. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

EUROPEAN COMISSION. *Guidelines on Consent under Regulation 2016/679* (wp259rev.01), [2016]. Disponível em: https://ec.europa.eu/newsroom/article29/items/623051/en. Acesso em: 17 maio 2023.

EUROPEAN COMISSION. *Opinion 3/2012 on developments in biometric Technologies*, [2012]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. Acesso em: 16 maio 2023.

EUROPEAN COMISSION. *Opinion 2/2017 on data processing at work*, [2017]. WP249. Disponível em: https://ec.europa.eu/newsroom/article29/items/610169. Acesso em: 16 maio 2023.

FINN, Rachel L.; WRIGHT, David; FRIEDEWALD, Michael. Seven Types of Privacy. *In.* GUTWIRTH, Serge, LEENES, Ronald, DE HERT, Paul and POULLET, Yves. (ed.) *European Data Protection*: Coming of Age. London: Springer, 2013. p. 14-69.

HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, v. 28, p. 65-98, 2019.

JUNIOR, Carlos Augusto Pinto de Vasconcellos; FERREIRA, Victor Silva. Impacto da Lei Geral de Proteção de Dados Pessoais nas relações de trabalho: a necessidade de implantação do programa de integridade (*compliance*). *UERJ Labuta*, 21 mar. 2020. Disponível em: https://uerjlabuta.com/2020/03/21/impacto-da-lei-geral-de-protecao-de-dados-pessoais-nas-relacoes-detrabalho-a-necessidade-de-implantacao-do-programa-de-integridade-Compliance/. Acesso em: 16 maio 2023.

LIMA, Ana Paula Moraes Canto D. *LGPD Aplicada*. São Paulo: Grupo GEN, 2021.

MAIA, Daniel Azevedo de Oliveira. *As hipóteses autorizativas de Tratamento de Dados Pessoais nas Relações de Trabalho sob a ótica da LGPD e do GDPR*. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

MARTINS, Sergio Pinto. *Direito do trabalho*. 39. ed. São Paulo: Saraiva, 2023.

MORDINI, Emilio. Whole body imaging at airport checkpoints: The ethical and political context. *In:* VON SCHOMBERG, René. *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies fields*. Luxembourg: Publications Office of the European Union, 2011. p. 165-209.

MOREIRA, Teresa Coelho. *A Privacidade dos trabalhadores e as novas tecnologias de informação e comunicação*: contributo para um estudo dos limites do poder de controlo electrónico do empregador. Coimbra: Almedina, 2010.

OLIVEIRA, Ricardo. LGPD: *Como evitar as sanções administrativas*. São Paulo: Saraiva, 2021.

PESTANA, Marcio. *Direito administrativo brasileiro*. 4. ed. São Paulo: Atlas, 2014.

PINHEIRO, Iuri; BOMFIM, Vólia. *A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho*. *Instituto Trabalho em Debate*, 1 out. 2020. Disponível em: http://trabalhoemdebate.com.br/artigo/detalhe/a-lei-geral-de-protecao-de-dados-e-seus-impactos-nas-relacoes-de-trabalho. Acesso em: 9 maio 2023.

TEIXEIRA, Tarcísio, e RUTH Maria Guerreiro. *Lei Geral de Proteção de Dados Pessoais (LGPD)*: Comentada Artigo por Artigo. São Paulo: Saraiva, 2022.

BRASIL. Tribunal Superior do Trabalho (8. Turma). RRAg-1995-55.2016.5.06.0144. Relatora: Min. Dora Maria da Costa. *DEJT*, 26 nov. 2021.

TZANOU, Maria. *Personal Data Protection and Legal Developments in the European Union*. Hershey: IGI Global, 2019.

VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet (org.). *In:* VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. *Ius Comparatum* – Global Studies in Comparative Law. Berlin: Springer, 2020. p. 4-44.

WALDMAN, Ari Ezra. Privacy, notice, and design. *Stanford Technology Law Review*, v. 21, p. 129-183, 2018.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

BENTO, Rafael Tedrus. Hipótese de tratamento de dados sensíveis: dado biométrico e relação de trabalho. *International Journal of Digital Law*, Belo Horizonte, ano 4, n. 1, p. 63-75, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.tedrus.

DOI: 10.47975/digital.law.vol.4.n.1.diaz

La Inteligencia Artificial: Una herramienta que revoluciona la compra pública[I]

Artificial Intelligence: A tool that revolutionizes public procurement

Juan Francisco Diaz Colmachi[*]
Universidad Andina Simón Bolívar (Quito, Ecuador)
jfranciscodiaz85@gmail.com
https://orcid.org/0000-0002-0114-9267

Recebido/Received: 04.02.2023/ February 4th 2023
Aprovado/Approved: 14.06.2023/ June 14th 2023

Resumen: La inteligencia artificial en la administración y en la contratación pública particularmente es inminente. Es necesario estar preparados para esta vinculación que se ve venir de manera rauda. Existen ventajas y posibles riesgos que son necesarios alertarlos previo a que la tecnología llegue a cubrir de manera completa aquellas actuaciones donde los sistemas tecnológicos logren realizar actividades que tradicionalmente han sido realizados por lo humanos, en este artículo intentamos plantear una problemática sobre la que es necesaria discutir con el fin de que la administración este a la altura de asumir los nuevos retos y sobre todo de manera oportuna, preservando el bien común y sobre todo el derecho de los ciudadanos a adecuados servicios públicos.

Palabras-clave: Inteligencia Artificial. Contratación pública. Machine learning. Contratos. Administración pública.

Abstract: Artificial intelligence in administration and public procurement in particular is imminent. It is necessary to be prepared for this connection that can be seen coming quickly. There are advantages and possible risks that need to be alerted before the technology fully covers those actions where technological systems manage to carry out activities that have traditionally been carried out by humans. In this article we try to raise a problem on which it is necessary discuss so that the Administration is up to the task

[I] Como citar esse artigo/How to cite this article: COLMACHI, Juan Francisco Diaz. La Inteligencia Artificial: Una herramienta que revoluciona la compra pública. *International Journal of Digital Law*, Belo Horizonte, v. 4, n. 1, p. 77-85, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.diaz.

[*] Profesor de Maestría en la Universidad Andina Simón Bolívar (Quito, Ecuador). Doctorando en Derecho por la Universidad de Valladolid. Maestría en Derecho Administrativo por la Universidad Andina Simón Bolívar Abogado por la Universidad Central del Ecuador. Coordinador Nacional del Observatorio de Contratación Pública de Ecuador (ObTCP). Miembro de la Asociación Internacional de Derecho Administrativo (AIDA) del Instituto de Estudios de Derecho Administrativo y Social (IDEAS) de la Asociación Mexicana de Derecho Administrativo (AMDA). Miembro colaborador del Observatorio de Contratación Pública de España (ObCP) y de la Red Iberoamericana de Contratación Pública Públicas (REDICOP). *E-mail*: jfranciscodiaz85@gmail.com.

of assuming the new challenges and above all in a timely manner, preserving the common good and above all the right of citizens to adequate public services.

Keywords: Artificial intelligence. Public procurement. Machine learning. Contracts. Public administration.

Sumario: **1** Antecedentes – **2** La Inteligencia Artificial – **3.** Aplicación de la Inteligencia Artificial – **4** La Inteligencia Artificial en la contratación pública – **5** Conclusiones – **6** Referencias

1 Introducción

Hay un antes y un después de la administración pública con y sin el uso de la tecnología en su quehacer diario que comenzó hace aproximadamente 25 años. Esto provocó el cambio del correo tradicional por el correo electrónico, papeles por documentos digitales, pasando de firmas manuscritas a firmas electrónicas. Salir de los trámites presenciales para el uso de software, facilitando el trabajo de los servidores; evitando la presencia física de personas en las oficinas, solicitando autorizaciones, permisos o pagando impuestos. Si hacemos una evaluación hoy, una conclusión anticipada nos permite afirmar que sin tecnología los gobiernos no podrían realizar adecuadamente su trabajo. A pesar de esta evolución, se sigue esperando una Administración más ágil, más inclusiva, menos burocrática, incluso menos corrupta, especialmente en los países latinoamericanos, sin que el rol del ciudadano haya cambiado significativamente.

Es importante evidenciar cuál es el problema en nuestros países latinoamericanos, con respecto a la prestación de los servicios públicos. Por citar un ejemplo en Ecuador, sus ciudadanos han calificado en 2022 con 5,6 puntos sobre 10 servicios públicos del país, la peor calificación desde 2017,[1] entendiendo por servicios públicos seguridad, salud, educación, transporte, trámites, permisos, obtención de documentos, pagando impuestos.

Una solución a estos problemas es la implementación de un verdadero Gobierno Electrónico, entendido como "Las actividades de las administraciones pueden ejecutarse mediante el uso de nuevas tecnologías y medios electrónicos, respetando las leyes, salvaguardando la inalterabilidad e integridad de las actuaciones y garantizando los derechos de las personas";[2] dentro del gobierno electrónico definitivamente resalta la ya bastante difundida inteligencia artificial (IA por sus siglas). Las palabras más usadas en español, según la Real Academia de la Lengua Española en 2022, es "Inteligencia Artificial" (IA),[3] que se contrasta

1 Disponible en: https://www.primicias.ec/noticias/economia/servicios-publicos-calificacion-baja-ecuatorianos/.
2 DÍAZ, 2021, p. 128
3 MORALES, 2022.

con la palabra “Metaverso”, que se encuentra entre las 25 palabras más usadas en inglés.[4] Concluyendo que estos nuevos espacios creados por la Tecnología en una especie de mundo paralelo no deben ser ajenos a la administración pública, siendo necesario estudiarlos y debatirlos, para otorgar al ciudadano un nuevo rol.

2 La Inteligencia Artificial

Como todos sabemos, la IA se está convirtiendo rápidamente en una de las tecnologías más transformadoras de nuestro tiempo, con el potencial de revolucionar muchos aspectos de nuestras vidas. En el sector público, la IA se aplica para tener gobiernos más eficientes, efectivos y receptivos a las necesidades de los ciudadanos. ¿Qué es la IA? La Inteligencia Artificial (IA) es un campo de estudio y desarrollo de tecnología que busca replicar la capacidad humana de razonamiento, aprendizaje y toma de decisiones en sistemas informáticos.

Por ser tan reciente hay muy poca bibliografía, sin embargo hemos encontrado algunos intentos de definirla como el de “La simulación de procesos de inteligencia humana por parte de máquinas, especialmente sistemas informáticos” conforme el diccionario de Oxford, por otro lado encontramos que es “La capacidad de una máquina para imitar la inteligencia humana y realizar tareas que normalmente requieren de la intervención humana, como el reconocimiento de voz, la toma de decisiones, la comprensión del lenguaje natural y el aprendizaje”. Según John McCarthy, uno de los pioneros en el campo de la IA. Stuart Russell y Peter Norvig autores del libro *Inteligencia Artificial: Un enfoque moderno* lo consideran como “La ciencia y la ingeniería de hacer que las máquinas sean inteligentes, especialmente mediante la programación de algoritmos que les permitan aprender de los datos, razonar, tomar decisiones y resolver problemas”.

Estas definiciones reflejan la idea central de la IA, que es la capacidad de las máquinas para realizar tareas de manera autónoma o asistida, imitando o superando la inteligencia humana en determinados dominios. La IA abarca una amplia gama de enfoques y técnicas, como el aprendizaje automático (*machine learning*), el procesamiento del lenguaje natural (NLP), la visión por computadora y la robótica, que para efectos de la administración pública se puede aprovechar la analítica y estadística para toma de decisión y predicción a fin de tener una administración pública mucho más eficiente.

[4] LINDREA, 2022.

3 Aplicación de la Inteligencia Artificial

Una de las mayores ventajas de la IA en la administración pública es su capacidad para procesar grandes cantidades de datos de forma rápida y precisa. Esto significa que las agencias gubernamentales pueden analizar grandes cantidades de información en tiempo real, lo que les permite tomar decisiones basadas en datos que se basan en pruebas sólidas. En el campo del transporte, la IA se puede utilizar para optimizar el flujo de tráfico y mejorar la eficiencia de los sistemas de transporte público.

Un área en la que la IA tiene el potencial de tener un impacto significativo es en el cuidado de la salud. La IA se puede utilizar para analizar los datos de los pacientes y ayudar a los proveedores de atención médica a realizar mejores diagnósticos y decisiones de tratamiento. Por ejemplo, en el campo de la radiología, la IA se puede utilizar para analizar imágenes médicas y ayudar a los radiólogos a identificar problemas potenciales que pueden haberse pasado por alto durante las revisiones manuales. Otro beneficio de la IA en la administración pública es su capacidad para automatizar tareas rutinarias, lo que libera a los trabajadores del gobierno para que se centren en cuestiones más complejas e importantes. Los *chatbots* impulsados por IA pueden manejar consultas básicas de servicio al cliente, mientras que los sistemas más avanzados pueden ayudar a procesar el papeleo y hacer predicciones sobre tendencias futuras. Esto puede ayudar a las agencias gubernamentales a operar de manera más eficiente y eficaz, al mismo tiempo que mejora la calidad de los servicios que se brindan a los ciudadanos.

En relación a esto, en Ecuador anualmente se destinan cerca de diez millones de dólares, equivalentes a casi el 10% del Producto Interno Bruto (PIB), para cubrir salarios de medio millón de funcionarios en un país de 17 millones de habitantes un número importante. Si bien es cierto la IA puede ser una amenaza para los trabajos mecánicos y de asistencia porque reemplazaríamos a los seres humanos con tecnología, el beneficio será directo para los ciudadanos, obligará a los funcionarios a superarse y beneficiará a la economía del país.

El profesor Christopher Pissarides, de la London School of Economics y Premio Nobel de economía en el año 2010, mencionó que podríamos pasar a una semana de cuatro días fácilmente implementando IA,[5] esto de la mano con que un reciente informe de Goldman Sachs que estimó que trescientos millones de personas podría perder sus trabajos y ser reemplazadas por IA.[6] Siendo una amenaza para

[5] Disponible en: https://www.xataka.com/empresas-y-economia/palabra-premio-nobel-chatgpt-aliado-inesperado-semana-cuatro-dias.

[6] Disponible en: https://www.infobae.com/america/mundo/2023/03/30/goldman-sachs-estima-que-la-inteligencia-artificial-afectara-a-300-millones-de-empleos-en-las-economias-avanzadas/.

los trabajos mecánicos y de asistencia porque sustituiríamos al ser humano por tecnología al ser más efectivo y más económico para las empresas

Para aprovechar todo el potencial de la IA en la administración pública, es importante que tengamos una fuerza laboral capacitada que sea capaz de desarrollar e implementar estas tecnologías. Esto requerirá una inversión significativa en educación y capacitación, así como asociaciones entre agencias gubernamentales, instituciones académicas y empresas del sector privado.

Otra área en la que se puede utilizar la IA para mejorar la administración pública es en el campo de la respuesta ante desastres. La IA se puede utilizar para analizar datos de múltiples fuentes, incluidas las redes sociales y las imágenes satelitales, para ayudar a los primeros en responder a identificar áreas que pueden estar en alto riesgo durante un desastre. Esto puede ayudar a salvar vidas, prevenir daños a la propiedad y aún más en los países sudamericanos que frecuentemente experimentan terremotos, erupciones e inundaciones, podría ser de gran ayuda. Sin embargo, también existen desafíos asociados con la incorporación de la IA en la administración pública. Uno de los mayores desafíos es el potencial de la IA para perpetuar las desigualdades y los sesgos existentes, especialmente si los algoritmos que impulsan estas tecnologías se entrenan con datos sesgados.

4 La Inteligencia Artificial en la contratación pública

La Inteligencia Artificial (IA) ya es una herramienta poderosa y transformadora en diversos ámbitos de la sociedad. Uno de los campos en los que la IA ha encontrado una aplicación significativa es en la compra pública por parte de los gobiernos. La compra pública se refiere a la adquisición de bienes y servicios por parte de las entidades gubernamentales para satisfacer las necesidades de la sociedad y llevar a cabo sus funciones. En este artículo, exploraremos cómo la Inteligencia Artificial se podría convertir en una herramienta fundamental en el proceso de compra pública de los gobiernos, y cómo impactar positivamente la eficiencia, la transparencia y la toma de decisiones en este ámbito, intentando mostrar los beneficios y desafíos asociados con su implementación.

Empecemos ¿Como mejoramos la eficiencia en la compra pública? La adopción de la Inteligencia Artificial en la compra pública permite la automatización de numerosas tareas y procesos, lo que conlleva una mejora significativa en la eficiencia de estos procedimientos. Los algoritmos de aprendizaje automático pueden analizar grandes volúmenes de datos y automatizar tareas repetitivas, como el procesamiento de solicitudes de las áreas requirentes y la generación de informes que demandan tiempo importante a los funcionarios. Esto reduce la carga de trabajo administrativo y permite a los funcionarios de compras dedicar más tiempo a tareas estratégicas.

Además, la IA facilita la optimización de los procesos de adquisición. Los sistemas de IA pueden utilizar técnicas de análisis de datos y algoritmos de optimización para mejorar la planificación de la compra, identificar proveedores potenciales, realizar comparaciones de precios y condiciones, y agilizar el proceso licitatorio. Esto conduce a una mayor eficiencia en la selección de proveedores y en la obtención de los bienes y servicios necesarios para los gobiernos.

Con respecto a la transparencia, este es un principio fundamental en la compra pública, ya que garantiza la igualdad de oportunidades y la justa competencia entre proveedores. La IA puede desempeñar un papel crucial en el aumento de la transparencia en este ámbito. Por un lado, los sistemas de IA pueden rastrear y auditar todas las transacciones y decisiones de compra, proporcionando un seguimiento y una visibilidad más efectiva de todo el proceso. Esto ayuda a prevenir y detectar posibles casos de corrupción, asegurando que las acciones de los funcionarios de compras sean transparentes y estén sujetas a escrutinio público efectivo en tiempo real e inclusivo pasando de la sanción a la prevención.

Definitivamente la transparencia es la antítesis de la corrupción,[7] sin embargo, conocemos que no es el único antídoto, por lo que de manera complementaria a lo que la IA puede hacer en la contratación pública, es necesario sumar, políticas, leyes y sobre todo una cultura política y social que mantenga alejadas las malas prácticas de los procedimientos de contratación.

Por otro lado, la aplicación de la IA en la evaluación de ofertas puede garantizar que los criterios de selección sean objetivos y se apliquen de manera justa a todos los proveedores. Los algoritmos de IA pueden analizar y comparar las propuestas de los proveedores, asegurando que se realice una evaluación imparcial y transparente. Esto disminuye el riesgo de favoritismos y promueve una compra pública basada en la calidad y la competitividad. Incluir criterios de IA donde ganan las mejores ofertas, limita la discrecionalidad de los servidores públicos, evolucionando a compras inteligentes y para ello será necesario invertir en desarrollo tecnológico.

La IA tiene el potencial de mejorar la toma de decisiones en la compra pública al proporcionar información y análisis basados en datos. Los algoritmos de IA pueden analizar grandes conjuntos de datos y extraer patrones y tendencias, brindando a los funcionarios de compras una visión más clara de las opciones disponibles y las posibles implicaciones de sus decisiones. Al utilizar la IA, los gobiernos pueden tomar decisiones más informadas sobre qué proveedores seleccionar, qué precios y condiciones son más favorables, y qué estrategias de adquisición son más eficientes. Además, los sistemas de IA pueden ayudar a predecir y mitigar riesgos en el proceso de compra, permitiendo una gestión más efectiva de posibles

[7] DÍAZ, 2022.

problemas y contingencias. A esto se suma el hecho de poder obtener mejores precios, diferentes alternativas, una planificación mucho más real de los objetos de contratación que se requieren para satisfacer adecuadamente las necesidades ciudadanas.

A pesar de los beneficios que la IA ofrece en la compra pública, también plantea desafíos y consideraciones éticas que deben abordarse de manera adecuada. Uno de los desafíos es el sesgo algorítmico. Los algoritmos de IA se basan en datos históricos, y si estos datos contienen sesgos o prejuicios ocultos, los algoritmos pueden perpetuarlos en sus decisiones. Esto podría resultar en una selección desigual de proveedores o en la exclusión de ciertos grupos. Es fundamental abordar este sesgo algorítmico mediante la recopilación de datos imparciales y la implementación de mecanismos de control y supervisión adecuados. también es importante contar con un marco regulatorio adecuado y actualizado, que permita a quien parametrizan las condiciones y la información mantener altos niveles de responsabilidad a fin de evitar discrecionalidad, mantener objetividad y evitar favoritismos en las adjudicaciones

Otro desafío importante es la seguridad y privacidad de los datos. La implementación de la IA en la compra pública requiere el acceso a grandes cantidades de información sensible, como datos financieros y personales de proveedores. Es crucial establecer protocolos de seguridad y protección de datos para evitar filtraciones o mal uso de la información, caso contrario se convertiría en un riesgo potencial. Además, es esencial considerar el impacto socioeconómico de la adopción de la IA en la compra pública. Si bien la automatización puede mejorar la eficiencia, también puede tener implicaciones en el empleo y en la relación con los proveedores tradicionales. Los gobiernos deben abordar estas cuestiones y establecer políticas y programas que mitiguen cualquier impacto negativo.

5 Conclusiones

La Inteligencia Artificial se avizora como una herramienta valiosa en la compra pública de los gobiernos, mejorando la eficiencia, la transparencia y la toma de decisiones informadas. La automatización de tareas, la optimización de procesos y la capacidad de análisis de datos de la IA ofrecen grandes oportunidades para mejorar los procedimientos de compra y lograr un uso más efectivo de los recursos públicos.

Es fundamental abordar los desafíos y consideraciones éticas asociados con la implementación de la IA en la compra pública. La eliminación de sesgos algorítmicos, la protección de datos y la gestión adecuada del impacto socioeconómico son aspectos clave que deben tenerse en cuenta. Con una adopción responsable y una

gestión adecuada, la IA puede ser una herramienta poderosa para promover una compra pública eficiente y transparente, beneficiando así a la sociedad en general.

Para abordar estos desafíos, es importante que abordemos el uso de la IA en el gobierno con precaución y tengamos reglas y regulaciones claras para garantizar que estas tecnologías se usen de manera ética y responsable. Esto requerirá una estrecha colaboración entre las agencias gubernamentales, las empresas de tecnología y los ciudadanos, así como un compromiso con la educación y capacitación continuas para los trabajadores del gobierno.

Finalmente, cabe preguntarse si el papel del ciudadano también ha evolucionado con estos cambios. Desde la perspectiva de la administración pública, se ha puesto a disposición del público información accesible a través de la web, lo que nos hace preguntarnos si es suficiente por cuestiones de transparencia pensando en un verdadero gobierno abierto. La tecnología ha acercado la administración pública a los hogares. Sin embargo, vemos que es necesario no solo estar cerca, sino involucrar a las personas en las decisiones que toman los gobiernos en nombre del "bien común", no solo el día de las elecciones, sino en la toma de decisiones sobre aspectos que puedan beneficiarlos o afectarlos, tales como nuevas infraestructuras, cambios viales, nuevos trámites, licencias o requisitos y atención de servicios.

Referencias

CUGUERÓ-ESCOFET, N.; GUASCH, X. Artificial intelligence in public procurement: How to prevent corruption in contracting authorities. *Digital Policy, Regulation and Governance*, v. 20, Issue 6, p. 534-553, 2018. Disponible en: https://www.emerald.com/insight/content/doi/10.1108/DPRG-03-2018-0016/full/html. Accesso el: 12 feb. 2023.

DÍAZ, Juan Francisco. La utopía de los trámites administrativos electrónicos. *In:* BARRERA, Teresita Rendón Huerta (ed.). *Construyendo uma agenda del derecho administrativo em la pospandemia del Covid-19*. 1. ed. Guanajuato: LITO-GRAPO, S.A. de C.V., 2021.

DÍAZ, Juan Francisco. *La corrupción en la compra pública*. Pamplona: Editorial Aranzadi, 2022.

EUROPEAN COMMISSION. *Artificial Intelligence in the public sector*. Joint Research Centre Science for Policy Report, 2019. Disponible en: https://ec.europa.eu/jrc/en/publication/artificial-intelligence-public-sector. Accesso el: 12 feb. 2023.

KATTEL, R.; MITRAKOVIĆ, M. Artificial Intelligence in Public Procurement: A Comparative Study of Six Countries. *Government AI Readiness Index Report*, v. 4, Issue 1, p. 32-45, Apr. 2020. Disponible en: https://www.researchgate.net/publication/340518149_Artificial_Intelligence_in_Public_Procurement_A_Comparative_Study_of_Six_Countries. Accesso el: 9 feb. 2023

LINDREA, Brayden. *'Metaverse' a top 3 contender for Oxford's Word of the Year*, 23 nov. 2022. Disponible en: https://cointelegraph.com/news/metaverse-a-top-3-contender-for-oxford-s-word-of-the-year. Accesso el: 15 jan. 2023.

MORALES, Manuel. La palabra del año son dos: inteligencia artificial según la FundéuRAE. *Diario el País de España*, 29 dic. 2022. Disponible en: https://elpais-com.cdn.ampproject.org/c/s/elpais.com/cultura/2022-12-29/la-palabra-del-ano-son-dos-inteligencia-artificial-segun-la-fundeurae.html?outputType . Accesso el: 20 jan. 2023.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (OCDE). *Artificial Intelligence in Society*. Paris: OECD Publishing, 2020. Disponible en: https://www.oecd-ilibrary.org/science-and-technology/artificial-intelligence-in-society_9789263499602-en. Accesso el: 4 feb. 2023.

WALKER, R.; GOLDSMITH, S. Using artificial intelligence in public procurement. *Harvard Kennedy School*, 2020. Disponible en: https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/egov/files/Using%20AI%20in%20Public%20Procurement.pdf. Accesso el: 10 feb. 2023.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

COLMACHI, Juan Francisco Diaz. La Inteligencia Artificial una herramienta que revoluciona la compra pública. *International Journal of Digital Law*, Belo Horizonte, ano 4, n. 1, p. 77-85, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.diaz.

DOI: 10.47975/digital.law.vol.4.n.1.becerra.

Avances de la administración colombiana en la era digital[I]

Advances of the Colombian administration in the digital age

Augusto Hernández Becerra[*]
Universidad Externado de Colombia (Bogotá, DC, Colombia)
hernandezaugusto@hotmail.com
https://orcid.org/0000-0002-4929-1916

Recebido/Received: 02.04.2023/ March 02nd, 2023
Aprovado/Approved: 18.06.2023/ June 18th, 2023

Resumen: El estudio expone la forma como las políticas de modernización informática en la administración pública colombiana se han extendido a dominios tan diversos como la seguridad y privacidad de los datos, la automatización de trámites en línea, la gestión documental y de los contratos estatales, el control de las transacciones y la administración de los impuestos. Inicialmente se refieren los principales hitos de la digitalización de la administración en Colombia, y posteriormente se analiza cómo la digitalización ha conducido a la administración hacia las fronteras de la Inteligencia Artificial. La recolección de fuentes acude a la investigación de tipo bibliográfico, en la cual se registran fuentes normativas nacionales y literatura nacional e internacional sobre administración pública y digitalización de las organizaciones. Se concluye que en Colombia se han dado grandes pasos para avanzar hacia el gobierno digital, y se previene sobre los riesgos de la aplicación de la Inteligencia Artificial en los procedimientos administrativos cuando se trata de decidir sobre derechos humanos.

Palabras-clave: Gobierno digital. Transparencia. Gobierno abierto. Inteligencia Artificial. reforma administrativa.

Abstract: The article exposes the way in which the computer modernization policies in the Colombian public administration have extended to domains as diverse as data security and privacy, the automation of online procedures, document management and state contracts, the control of transactions and the administration of taxes. Initially, the main milestones of the digitization of the administration in Colombia are referred to, and later it is analyzed how digitization has led the administration towards the frontiers of artificial intelligence. The collection of sources goes to bibliographic research, in which national regulatory sources and national and international literature on public administration and digitization of organizations are recorded. It is concluded that in Colombia great steps have been taken to advance towards digital government, and it is warned about the risks of the application of artificial intelligence in administrative procedures when it comes to deciding on human rights.

[I] Como citar esse artigo/How to cite this article: BECERRA, Augusto Hernández. Avances de la administración colombiana en la era digital. *International Journal of Digital Law*, Belo Horizonte, v. 4, n. 1, p 87-106, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.becerra.

[*] Doutor em Direito e professor-pesquisador pela Universidade Externado de Colombia.

Keywords: Digital government. Transparency. Open government. Artificial Intelligence. Administrative reform.

Sumario: 1 Introducción – **2** Hacia la digitalización de la administración de Colombia – **2.1** Las primeras leyes – **2.2** Creación del Ministerio de Tecnologías de la Información y las Comunicaciones – **2.3** La reforma de los procedimientos administrativos en 2011 – **2.4** Leyes contra la corrupción – **2.5** Legislación sobre publicidad de los actos oficiales – **2.6** Legislación sobre transparencia – **2.7** La política de Gobierno o Estado abierto – **3** En las fronteras de la Inteligencia Artificial – **4** Conclusiones – Referencias

> "La aceleración de las innovaciones digitales debe ser aprovechada aún más por los países, para que la prestación de los servicios sea más rápida y eficaz. Es el tiempo de dar un salto cualitativo y empezar a trabajar con más intensidad en el uso del big data y la Inteligencia Artificial para predecir, analizar y evaluar, tanto en la formulación como en la directa prestación de servicios públicos."[1]

1 Introducción

La organización, los procesos y los procedimientos de la administración pública contemporánea han sido objeto de profundas y aceleradas transformaciones por efecto de la incorporación de medios tecnológicos avanzados que contribuyen a incrementar la eficiencia en la provisión de bienes y servicios públicos y en el desempeño de las funciones estatales. Esta es la oleada de reformas que ha colocado a la administración pública en la "era digital".

Al implementar medios tecnológicos avanzados en los campos de la información y la comunicación, los sistemas electrónicos de gestión, las plataformas en línea, las aplicaciones móviles y otras herramientas digitales, las administraciones públicas han logrado automatizar tareas, agilizar trámites, optimizar la comunicación interna y externa, y desarrollar nuevas capacidades institucionales y modelos de servicio público.

De otra parte, el uso de la informática contribuye a garantizar la transparencia en la administración pública. La digitalización de documentos y procesos y su publicidad, permiten un mejor acceso y disponibilidad de la información para los ciudadanos, facilitan la lucha contra la corrupción, promueven la rendición de cuentas, viabilizan la participación ciudadana en la toma de decisiones y promueven una gestión pública más democrática y colaborativa.

En el presente artículo se describe la forma como el Estado colombiano, en sintonía con las tendencias internacionales, ha venido haciendo ese recorrido hacia la digitalización de la administración, y de qué manera las políticas de modernización

[1] CLAD, 2020.

informática le han llevado a dominios tan diversos como la seguridad y privacidad de los datos, la automatización de trámites en línea, la gestión documental y de los contratos estatales, el control de las transacciones y la administración de los impuestos.

El presente artículo se compone de dos partes. La primera describe los principales hitos de la digitalización de la administración en Colombia. La segunda analiza la última etapa de una evolución tecnológica que ha llevado la administración a las fronteras de la Inteligencia Artificial.

2 Hacia la digitalización de la Administración de Colombia

Al terminar el siglo pasado, la administración colombiana dio unos primeros pasos, tímidos e inseguros, dirigidos a la introducción de herramientas informáticas en algunos de sus procedimientos internos y a su aplicación en trámites de los ciudadanos ante la administración, especialmente en lo relacionado con peticiones, quejas, reclamos, recursos, sugerencias y denuncias.

Un claro indicio de esta tendencia fue la creación del Ministerio de Tecnologías de la Información y las Comunicaciones en 2009. Poco después se dio un paso gigantesco para sumergir a toda la administración en la dimensión digital con la expedición del Código de Procedimiento Administrativo y de lo Contencioso Administrativo en 2011, que normalizó los actos administrativos electrónicos y los expedientes administrativos electrónicos, y consagró el derecho de toda persona a relacionarse con la administración pública utilizando medios electrónicos.

Por aquellos años sucesivas leyes contra la corrupción, sobre publicidad de los actos oficiales y sobre transparencia, coincidieron en acudir a la estrategia informática como medio para dar mayor eficacia a dichas medidas, pues evidentemente las tecnologías digitales no solo masifican la publicidad de la actividad estatal y facilitan el acceso del público a los documentos estatales, sino que, bajo tales condiciones, mejoran los controles y se restringe significativamente la corrupción administrativa.

Más recientemente, a raíz del ingreso de Colombia a la OCDE en 2020, el gobierno adoptó políticas públicas consonantes con las recomendaciones del organismo, enfocadas principalmente a garantizar el acceso ciudadano a la información pública, desarrollar una cultura de integridad pública, consolidar la capacidad institucional de lucha contra la corrupción y la cultura de la legalidad, impulsar iniciativas de innovación pública para consolidar los objetivos de un Estado Abierto y aplicar los Principios de la OCDE sobre Inteligencia Artificial.

2.1 Las primeras leyes

En Colombia se comenzó a legislar para impulsar la modernización administrativa mediante la introducción de la tecnología informática desde la década de los años 1990. Inicialmente la Ley nº 527 de 1999, autorizó la utilización de medios electrónicos para la sustanciación de las actuaciones,[2] la expedición de los actos administrativos, los documentos, contratos y en general los actos derivados de la actividad precontractual y contractual. Esta Ley nº dispuso, además, que para el trámite, notificación y publicación de tales actos podrían utilizarse soportes, medios y aplicaciones electrónicas.

Posteriormente la Ley nº 962 de 2005 abrió la posibilidad de que la administración,[3] en sus trámites y procedimientos, empleara medios electrónicos, al disponer que los organismos y entidades de la Administración Pública debían poner en conocimiento de los ciudadanos los medios tecnológicos de que dispusieren para atender los trámites y procedimientos de su competencia. Así mismo facultó a las entidades estatales para tramitar las actuaciones administrativas mediante la utilización de "soportes, medios y aplicaciones electrónicas". De otra parte, la Ley nº facultó también a los ciudadanos para presentar peticiones, quejas, reclamaciones o recursos, "mediante cualquier medio tecnológico o electrónico del cual dispongan las entidades y organismos de la Administración Pública".

2.2 Creación del Ministerio de Tecnologías de la Información y las Comunicaciones

La Ley nº 1341 de 2009 transformó el tradicional Ministerio de Comunicaciones en el moderno Ministerio de Tecnologías de la Información y las Comunicaciones, y le asignó la función de coordinar en la administración pública la implementación de la Estrategia de Gobierno en Línea, cuyo objeto ha sido desarrollar un Estado más eficiente, transparente y participativo y habilitarlo para prestar mejores servicios mediante el aprovechamiento de las tecnologías informáticas y comunicativas.

Esta Ley nº determina el marco general de las políticas públicas que rigen el sector de las Tecnologías de la Información y las Comunicaciones, el uso eficiente de las redes y del espectro radioeléctrico, así como las atribuciones del Estado para intervenir, regular y garantizar el libre acceso de todos los habitantes a la Sociedad de la Información. A través del nuevo ministerio el gobierno promueve el uso de

[2] "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."

[3] "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos."

las Tecnologías de la Información y las Comunicaciones, con el fin de fomentar el crecimiento y la competitividad del país.

El sector se modernizó sensiblemente con la Ley nº 1978 de 2019, que introdujo algunas modificaciones a la Ley nº 1341 con el objeto de modernizar el marco institucional, focalizar las inversiones para el cierre efectivo de la brecha digital y potenciar la vinculación del sector privado en el desarrollo de los proyectos asociados. Con estas nuevas medidas se quiso generar seguridad jurídica a las inversiones y facilitar el despliegue de infraestructura de alto costo, enfocando la inversión en la conexión a Internet de la población vulnerable y de escasos recursos, y en las zonas rurales y apartadas del país.

2.3 La reforma de los procedimientos administrativos en 2011

A pesar de que las leyes eran ya suficientemente claras, el Estado permaneció dubitativo ante el desafío cultural de las TICs durante algunos años, hasta la expedición de la Ley nº 1437 de 2011, mediante la cual se adoptó el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. En virtud del principio de celeridad, definido por esta Ley nº en el artículo 3º numeral 13, las autoridades quedaron obligadas a incentivar el uso de las tecnologías de la información y las comunicaciones, a efecto de que los trámites administrativos se adelantaran diligentemente, "dentro de los términos legales y sin dilaciones injustificadas". Lo que hasta entonces era para el Estado una opción se convirtió en regla general para todos los procedimientos administrativos.

La importancia de la Ley nº 1437 para la modernización del Estado radica en que impuso a la administración la obligación de "adoptar medios tecnológicos para el trámite y resolución de peticiones, y permitir el uso de medios alternativos para quienes no dispongan de aquellos" (artículo 7º numeral 8), como también el deber de contar con una sede electrónica (artículo 60) que le permita realizar sus procedimientos y trámites administrativos a través de medios electrónicos (artículo 63). En consonancia con todo ello, esta Ley nº autorizó que los trámites administrativos pudieran realizarse a través de medios electrónicos, y dispuso que, para garantizar la igualdad de acceso a la administración, la autoridad debía asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros medios (artículo 53).

La Ley nº 1437 dejó completamente estructurado el procedimiento administrativo electrónico: las autoridades pueden notificar sus actos a través de medios electrónicos (artículo 56), así como emitir válidamente actos administrativos por medios electrónicos (artículo 57) y organizar todas las actuaciones en expedientes

electrónicos (artículo 59). De otra parte, la Ley nº reconoció en el artículo 54 a todas las personas, y no solo a los ciudadanos, un nuevo derecho, propio de la era tecnológica que estamos viviendo, y que dice así: "Toda persona tiene el derecho de actuar ante las autoridades utilizando medios electrónicos."

El artículo 67 de esta ley, que describe la forma como se deben realizar las notificaciones personales, prevé que estas puedan hacerse "por medio electrónico". Se trató en su momento de un cambio muy notable frente a los procedimientos tradicionales, pues la presencia física de la persona, que siempre se exigió para poder realizar la notificación personal de los actos administrativos, y por esa razón se llama así, fue reemplazada, gracias a la magia del internet, por un nuevo tipo de "presencia", la presencia virtual. A partir de allí se desarrollará la gran trasformación cultural de nuestros días, asociada con el fenómeno de la virtualidad, que es la nueva forma de relación interpersonal en numerosos actos de la vida pública y privada.

La utilización de medios electrónicos en los procedimientos administrativos precipitó cambios cualitativos en el funcionamiento general del Estado, pues comenzaron a desaparecer las ventanillas atendidas por funcionarios, las filas de ciudadanos a la espera de realizar sus diligencias, las tradicionales congestiones en las oficinas públicas y las habituales demoras en los trámites oficiales de papel, sellos y firmas.

2.4 Leyes contra la corrupción

Durante algo más de veinte años el Congreso ha expedido leyes motivadas en la intención explícita de combatir la corrupción, mediante la estrategia combinada de transparencia, publicidad, participación ciudadana y utilización creciente de medios informáticos avanzados.

El Código Penal,[4] por supuesto, regula en el Título XV los delitos contra la Administración Pública, que describen conductas directamente asociadas con la corrupción. La Ley nº 850 de 2003, "Por medio de la cual se reglamentan las veedurías ciudadanas", las faculta para vigilar tanto la gestión de las autoridades y entidades públicas como el manejo de los recursos públicos, y en desarrollo de sus funciones formular recomendaciones, quejas y denuncias.

Ley nº 1474 de 2011, conocida como "Estatuto Anticorrupción", dicta medidas para prevenir y erradicar la corrupción pública y privada, endurece las penas relacionadas con los delitos contra la Administración Pública, crea una Comisión Nacional para la Moralización, y establece políticas institucionales y pedagógicas

[4] Ley nº 599, de 2000, "por la cual se expide el Código Penal".

de transparencia. Esta normatividad fue reforzada por la Ley nº 1712 de 2014,[5] que amplía las categorías existentes de personas naturales y jurídicas obligadas, crea nuevos deberes y obligaciones estatales en materia de publicación de información y consolida el sistema de acceso a la información pública.

La Ley nº 2195 de 2022, de transparencia, que ha sido precedida por otras leyes que tratan sobre la misma materia, enfatiza la prevención de actos de corrupción, refuerza la coordinación entre las entidades del Estado responsables de reprimir la corrupción y procurar el resarcimiento de los daños ocasionados. La ley, además, diseña programas de transparencia y ética empresarial, obligatorios para todos los sectores y personas jurídicas de derecho público y derecho privado, y establece un régimen sancionatorio más severo para las empresas, sus representantes y directivos por actos de corrupción.

La Ley nº 2.294 de 2023, "por la cual se expide el Plan Nacional de Desarrollo 2022-2026 'Colombia Potencia Mundial de la Vida'", faculta en el artículo 200 al gobierno nacional para formular una Estrategia Nacional de Lucha Contra la Corrupción, que tendrá como principales componentes la garantía de los derechos humanos, la protección al denunciante, el derecho al acceso a la información pública, el fortalecimiento de la veeduría ciudadana y la transparencia en la contratación y la gestión pública.

El anterior plan nacional cuatrienal de desarrollo, contenido en la Ley nº 1955, de 2019, para el periodo 2018-2022, quizá de manera más contundente proclamó como uno de sus objetivos un "Pacto de cero tolerancia a la corrupción y a la falta de transparencia", y asignó a la Secretaría de Transparencia, como estrategia para prevenir los riesgos de corrupción, la formulación e implementación de la Política Pública relacionada con "Transparencia, Integridad, Legalidad y Estado Abierto".

La Estrategia Nacional de Lucha Contra la Corrupción anunciada en el artículo 200 de Ley nº 2294, de 2023, tiene un sabor continuista, pues remite evidentemente a la caudalosa legislación existente en materia de protección de los derechos humanos, acceso a la información pública, veedurías ciudadanas, transparencia en la contratación y lucha contra la corrupción.

El uso de tecnología digital para combatir la corrupción ha sido un tema relevante en los últimos años en América Latina, Colombia incluida. De ahí la creación de plataformas para presentar en línea denuncias de corrupción en forma segura y anónima, y la implementación de sistemas de compras públicas electrónicas para reducir la corrupción en los procesos de adquisición de bienes y servicios. Las políticas de gobierno abierto y de datos abiertos también se han generalizado,

[5] "Por medio de la cual se crea la Ley nº de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."

pues fomentan la transparencia y permiten a los ciudadanos hacer un seguimiento efectivo de los recursos y las decisiones gubernamentales. Incluso se están usando ya técnicas avanzadas de Inteligencia Artificial y análisis de datos para identificar patrones y detectar posibles casos de corrupción.[6]

2.5 Legislación sobre publicidad de los actos oficiales

El deber de publicidad de los actos oficiales, así como el coetáneo derecho ciudadano de recabar información relativa a informaciones o documentos oficiales, respaldado en la explícita consagración constitucional del derecho de petición, son instituciones que cuentan con antecedentes antiguos dignos de mencionar en la legislación colombiana. Así, por ejemplo, la Ley nº 149, de 1888, reguló en el artículo 357 el derecho ciudadano de acceso a la información, y el artículo 334 de la Ley nº 4, de 1913, reiteró la garantía del derecho de petición.

Posteriormente el Decreto nº 2.733. de 1959. reglamentó el procedimiento que debía seguirse para garantizar el derecho de petición, a propósito del cual aseveró que su efectivo ejercicio obraba "en provecho común de los gobernados y de los gobernantes". Años más tarde el Decreto nº 1, de 1984, consagró y reguló entre otros principios el de publicidad de todos los actos del Estado, además del derecho a la información. La Ley nº 57. de 1985. robusteció el principio de publicidad de los actos y documentos oficiales y el derecho de petición. La Constitución de 1991 reitera estos principios, además de los de prevalencia del interés general, igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y participación.[7]

La citada Ley nº 1.437, de 2011, consagra, al lado del principio de transparencia, el de publicidad, que es instrumento y condición necesaria de aquella. Si la administración no estuviera sujeta al deber de informar, los ciudadanos difícilmente podrían tener noticias de su actividad, como requiere el principio de transparencia. El artículo 3º de esta ley nº fija el principio de publicidad de las actuaciones y procedimientos administrativos en los siguientes términos:

> (...) 9. En virtud del principio de publicidad, las autoridades darán a conocer al público y a los interesados, en forma sistemática y permanente, sin que medie petición alguna, sus actos, contratos y resoluciones, mediante las comunicaciones, notificaciones y publicaciones que ordene la ley, incluyendo el empleo de tecnologías que permitan difundir de manera masiva tal información de conformidad con lo dispuesto en este Código. Cuando el interesado deba asumir

[6] CAF, 2022.

[7] A propósito de los partidos y movimientos políticos, el artículo 107 de la Constitución establece que estarán sujetos a los principios rectores detransparencia y moralidad, entre otros.

> el costo de la publicación, ésta no podrá exceder en ningún caso el valor de la misma.

La disposición transcrita transforma el principio de publicidad en un deber estatal de permanente información sobre sus actividades y, en especial, de sus decisiones. Las autoridades deben, por tanto, dar a conocer "sus actos, contratos y resoluciones". Quiere la ley que esta función difusiva de lo que hace la administración sea constante y sistemática, es decir, que no se produzca simplemente como reacción a requerimientos de los ciudadanos, ni que los datos oficiales fluyan solo como respuesta a las demandas particulares, sino que las autoridades los suministren sin restricción y espontáneamente.[8]

El derecho de acceso a la información o a los documentos que se encuentren en poder de las autoridades no puede ser desconocido ni condicionado discrecionalmente por estas. En relación con esta importante cuestión ha precisado la Corte Constitucional que únicamente es legítima una restricción del derecho de acceso a la información pública o el establecimiento de una reserva sobre determinadas informaciones o documentos cuando lo autorice expresamente la Constitución o la ley.[9]

6 Legislación sobre transparencia

El derecho de acceso a la información y, por ende, la aplicación de los principios de transparencia y publicidad, contribuyen al control ciudadano sobre las agencias estatales al obligarlas a publicitar y explicar las decisiones adoptadas y el uso que le han dado al poder y a los recursos públicos, y son por tanto valiosos instrumentos para combatir la corrupción y dar eficacia al principio de legalidad.[10]

En consonancia con el artículo 74 de la Constitución, relativo al derecho a la información, según el cual "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley", la actividad entera del Estado debe ser visible para todos los ciudadanos, como si se desarrollara dentro de una urna de cristal. Nada que sea de interés público, y ninguna de las conductas de los funcionarios que se origine en el ejercicio de sus atributos, puede permanecer vedado al conocimiento de la sociedad.

Del acceso a la información y a la circulación de datos, en la sociedad democrática, se predican dos reglas de oro, de una u otra manera consagradas en las Constituciones: la información sobre el Estado es (o debe ser) pública, en

[8] Es lo que la Ley nº de Transparencia 1712 de 2014 denomina en el artículo 3º "principio de la divulgación proactiva de la información".
[9] COLOMBIA, 2006.
[10] COLOMBIA, 2010.

tanto que la información sobre las personas es privada o reservada. La primera se rige por el principio de transparencia, la segunda por el derecho denominado de *habeas data*.

La reserva sobre la información relativa al Estado es excepcional. En cambio, la reserva sobre la información de las personas es la regla general. Es por estas razones que únicamente la Ley nº puede indicar en qué casos la información pública es reservada, y cuándo la información privada puede trascender al conocimiento de terceras personas.

La Ley nº 1.581. de 2012, sobre protección de datos personales o *habeas data*, consagra el principio de transparencia en los siguientes términos:

> e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Por las dos vías, la de la publicidad de la información pública, y la privacidad de los datos personales, se defienden las libertades públicas y, por ende, la democracia. No seríamos libres si el Estado pudiera, legalmente, ocultar al público sus maquinaciones o mentirle sobre lo que ocurre en sus oficinas. Tampoco sería posible la libertad si los poderes de escrutinio y vigilancia estatales estuvieran legitimados para invadir la vida privada de las personas o para extenderse a las reconditeces de nuestro pensamiento.

Aun cuando el principio de transparencia solo será objeto de regulación explícita en leyes de reciente expedición, hizo precoz aparición en la Ley nº 80, de 1993, Estatuto General de Contratación de la Administración Pública, que en el artículo 23 lo incluyó entre los principios de la contratación administrativa. El artículo 24 de esta Ley nº enuncia fugazmente el principio de transparencia para hacerlo consistir en la regla conforme a la cual "La escogencia del contratista se efectuará siempre a través de licitación o concurso públicos".

La transparencia irrumpió en leyes posteriores con notable énfasis y reiteración. Así, por ejemplo, la Ley nº 1.437, de 2011, "por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo", aborda la transparencia como principio y la instrumenta mediante varios mecanismos que buscan darle eficacia.

La Ley nº 1.474, de 2011,[11] estatuto anticorrupción, regula prolijamente la eficiencia y la transparencia en el Título I, que con detalle fija las condiciones y

[11] "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública."

requisitos que se aplican a las distintas modalidades de selección de los contratistas y a los distintos tipos de contratos, da renovado impulso a la contratación pública electrónica y reorganiza e integra los distintos sistemas de información, registro y gestión contractual pública. Esta ley, además, impone a las entidades públicas la obligación de publicar información veraz, responsable, ecuánime, suficiente y oportuna sobre los proyectos de pliegos de condiciones y estudios previos, con el propósito de permitir a todos los interesados formular observaciones a su contenido.

Mediante el Decreto nº 4.170, de 2011, el gobierno nacional creó la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, entidad descentralizada que impulsa políticas públicas orientadas a la organización y articulación de los partícipes en los procesos de compras y de contratación pública, con el fin de lograr una mayor eficiencia, transparencia y optimización de los recursos del Estado. En cumplimiento de esta misión, la Agencia administra el *Sistema Electrónico de Contratación Pública – SECOP*, que es una plataforma transaccional por medio de la cual compradores y proveedores pueden realizar, enteramente en línea, el proceso de contratación con el Estado.[12]

Por su parte, el Decreto nº 19, de 2012,[13] estatuto antitrámites, invoca en sus considerandos la transparencia como principio afín al postulado de buen gobierno y a los principios de eficiencia, equidad, eficacia, economía y moralidad pública, como medios necesarios para racionalizar los trámites, procedimientos y regulaciones.

También la Ley nº 1551, de 2012, proclama en el literal f) del artículo 4º, sobre principios rectores del ejercicio de la competencia municipal, los principios de responsabilidad y transparencia, en virtud de los cuales los municipios asumirán las competencias a su cargo "garantizando su manejo transparente".[14] Agrega la norma que, en desarrollo de este principio, las autoridades municipales promoverán el control ciudadano de las actuaciones de la administración "a fin de prevenir la ocurrencia de actos de corrupción relacionados con la ejecución del presupuesto y la contratación estatal".

La Ley nº 1.712, de 2014, "Por medio de la cual se crea la Ley nº de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones",[15] impuso a todas las entidades públicas, entre otras, las obligaciones de : poner a disposición del público, en la página web, toda la información institucional y proveer apoyo y asistencia en relación con trámites y

12 COLOMBIA, [2023].

13 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública."

14 "Por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios."

15 El Decreto nº 1.081, de 2015, reglamenta la Ley nº 1.712, de 2014, establece los lineamientos para la implementación del derecho de acceso a la información pública y dispone sobre la clasificación de la información, los procedimientos de solicitud de información y las excepciones al acceso a la información.

servicios que se presten por medios electrónicos y presenciales; desarrollar criterios diferenciales de accesibilidad que permitan a poblaciones específicas acceder a la información pública en sus diversos idiomas y lenguas, así como a la población en condición de discapacidad; publicar las contrataciones en curso con un vínculo al sistema electrónico para la contratación pública; asegurar que sus sistemas de información electrónica estén alineados con la estrategia de *Gobierno en Línea*.[16]

El diseño, promoción e implementación de la política pública de acceso a la información pública está a cargo de la Secretaría de Transparencia de la Presidencia de la República, el Ministerio de Tecnología de la Información y Comunicaciones, el Departamento Administrativo de la Función Pública (DAFP), el Departamento Nacional de Planeación (DNP), el Archivo General de la Nación y el Departamento Administrativo Nacional de Estadística (DANE).[17]

4.7 La política de Gobierno abierto o Estado abierto

La teoría del gobierno abierto o del Estado abierto propone modernizar la administración pública para, por medio de las tecnologías de la información y las comunicaciones, lograr objetivos de eficiencia, transparencia, lucha contra la corrupción, participación ciudadana y consolidación del sistema democrático.

El modelo de gobierno abierto o de Estado abierto viene a ser una de las más recientes iniciativas globales de reforma de la administración, promovida al unísono por el gobierno de los Estados Unidos, la ONU, el CLAD, la CEPAL y la OCDE, además de organismos multilaterales de crédito, e instituciones académicas, científicas y empresariales. El concepto de gobierno abierto recoge experiencias, buenas prácticas, políticas públicas y normas que han demostrado ser eficaces para mejorar la gestión gubernamental, relegitimar las instituciones democráticas y apuntalar el estado de derecho, mediante el uso intensivo de las tecnologías de la información y las comunicaciones, y el diseño y ejecución de políticas de transparencia y participación ciudadana.

Entre los principales antecedentes de esta doctrina pueden citarse: (i) la Alianza para el Gobierno Abierto (AGA) (Open Government Partnership – OGP), nacida en 2007 como una idea del Presidente de los Estados Unidos, Barack Obama, que se formalizó en 2011 para convertirse en una iniciativa multilateral que agrupa a gobiernos e instituciones de la sociedad civil; (ii) la Agenda 2030 adoptada por la Asamblea General de las Naciones Unidas en septiembre de 2015, integrada por

[16] BECERRA, 2022.

[17] Entre muchas otras páginas web sobresalen en las políticas de gobierno en línea y transparencia: http://www.anticorrupcion.gov.com, http://www.contratacionenlinea.com, www.colpensiones.gov.com, www.defensajuridica.gov.com, http://www.atencionyreparacion.gov.co, http://www.portalterritorial.gov.com, http://www.banrep.gov.com, http://www.creg.gov.co, http://www.dps.gov.com etc.

17 objetivos para el desarrollo sostenible (ODS), entre los cuales se destaca el objetivo 16, que plantea una reforma del Estado para una gestión pública eficaz,[18] mediante la transparencia, el acceso a la información, la rendición de cuentas públicas, la participación ciudadana y la colaboración para la innovación.

De acuerdo con la OCDE, las estrategias de Gobierno Abierto son necesarias para recuperar la confianza de los ciudadanos y promover la democracia y el crecimiento".[19] La OCDE enumera como reformas necesarias de gobierno abierto, las siguientes: (i) Constituciones nacionales, (ii) libertades de expresión, información y prensa, (iii) leyes de participación ciudadana, (iv) leyes de libre acceso a la información pública, (v) leyes de transparencia, (vi) leyes de integridad, (vii) leyes de rendición de cuentas, (viii) leyes sobre archivos nacionales.

Por su parte la CEPAL sostiene que el gobierno abierto es una "nueva forma de gobernar" para, con y a través de los ciudadanos, que fortalece la nueva "ecuación entre el estado, el mercado y la sociedad." Según la visión de este organismo, el gobierno abierto reconfigura el Estado y fortalece la democracia porque sintoniza con la cultura digital, la cual prefiere compartir, dialogar y concertar, antes que imponer la autoridad, mediante el uso de formatos de colaboración, reciprocidad y conocimiento compartido.[20]

Por su parte el CLAD promovió la Carta Iberoamericana de Gobierno Abierto,[21] que fue adoptada en Cartagena de Indias en 2016. La Carta señala como finalidad del gobierno abierto la concreción del derecho de los ciudadanos a un buen gobierno, que se traduce en bienestar y prosperidad, mejores servicios públicos, calidad de vida, fortalecimiento de la democracia, confianza en la administración pública, y respeto a la dignidad humana y a la diversidad cultural. Para tales efectos la Carta consagra cuatro pilares del gobierno abierto, similares a los postulados por la Agenda 2030: (i) transparencia y acceso a la información pública, (ii) rendición de cuentas públicas, (iii) participación ciudadana y, (iv) colaboración e innovación pública y ciudadana.

A la idea inicial de "apertura" del gobierno se ha ido agregando una concepción más amplia, en el sentido de que las innovaciones técnicas y los avances democráticos de dicha apertura no pueden limitarse a la esfera de la rama ejecutiva o de la administración pública, sino que deben trascender a la totalidad de los organismos del Estado en sus diversas ramas y funciones. Es por esta razón que se prefiere hablar no de gobierno abierto sino de Estado abierto.[22]

---

18 "Objetivo 16. Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas."
19 OCDE, 2016.
20 CEPAL, 2017.
21 CLAD, 2016.
22 CEPAL, 2017.

Colombia, al igual que otros países democráticos, había implementado iniciativas que ahora se rotulan como de *gobierno abierto*, antes de que se popularizara esta noción, como ya antes se ha relatado. De la adopción del modelo de Estado abierto en Colombia se han ocupado, de una parte, el Plan Nacional de Desarrollo, que se expide por Ley nº cada cuatro años, y de otra parte el Consejo Nacional de Política Económica y Social (CONPES), que es la máxima autoridad nacional de planeación y organismo asesor del gobierno en todos los aspectos relacionados con el desarrollo económico y social del país. El CONPES actúa por medio de documentos en los cuales el gobierno formula y decide la política pública que orienta toda su actividad administrativa.[23]

Es así como en el documento CONPES nº 4.070, de 2021, denominado "Lineamientos de política para la implementación de un modelo de Estado Abierto", el gobierno reconoce la insuficiente articulación de normas, actores institucionales y sociedad alrededor de la construcción de confianza pública en el marco de la transición hacia un Estado abierto. En consecuencia, propone lineamientos de política pública para poner en marcha un modelo de Estado Abierto que promueva un mejor desempeño de la administración pública basado en la confianza, y deja constancia de que, con esta política, se da cumplimiento a los acuerdos internacionales derivados del ingreso del país a la OCDE y se avanza hacia el cumplimiento de la Agenda 2030.

Al definir la política de Estado Abierto el documento CONPES 4070 fija como objetivos específicos cinco ejes, a saber: (i) fortalecer la garantía del derecho de acceso a la información pública, (ii) desarrollar la cultura de integridad pública, (iii) consolidar la capacidad institucional de lucha contra la corrupción y la cultura de la legalidad, (iv) robustecer los procesos de corresponsabilidad entre actores para la generación de valor público, (v) impulsar iniciativas de innovación pública como una herramienta transversal para consolidar procesos orientados a un Estado Abierto.

2 En las fronteras de la Inteligencia Artificial

De lo hasta aquí expuesto se desprende que el Estado colombiano inició, hace más de veinte años, un lento proceso de adaptación para incorporar en sus organizaciones, procesos y procedimientos, la tecnología de la información y las comunicaciones, y, más recientemente, para utilizar medios tecnológicos avanzados. La epidemia del Covid-19, sin embargo, aceleró repentinamente lo que había sido

[23] El CONPES es la máxima autoridad de planeación y lo integran el presidente de la República, quien lo dirige, el vicepresidente de la República, todos los ministros, el director del Departamento Administrativo de la Presidencia de la República, el director del Departamento Nacional de Planeación y el director del Departamento Administrativo de Ciencia, Tecnología e Innovación – Colciencias. El Departamento Nacional de Planeación (DNP) desempeña la Secretaría Ejecutiva.

hasta entonces una perezosa evolución, y, como ocurrió en el mundo entero, la crisis obligó a hacer de una vez los cambios que se habían programado para el mediano y largo plazo.

De esta manera la transformación informática de los sectores público y privado, así como de la sociedad misma, se ha convertido en una sorprendente realidad, en la que la administración pública se aproxima ya a la frontera tecnológica de la Inteligencia Artificial, IA, concepto que ha entrado a formar parte de las más recientes medidas, normas y políticas.

De esta última fase forman parte varias leyes, documentos de política pública y procesos de reestructuración administrativa. En tiempos muy recientes la Ley nº 2,195, de 2022, sobre transparencia, prevención y lucha contra la corrupción, y la Ley nº 2.213, de 2022, que implanta de manera definitiva la justicia digital, a la cual se llegó repentinamente pero con buen suceso, como consecuencia de la pandemia del Covid-19, son una buena aproximación normativa al ideal del Estado abierto.[24]

Son numerosas las herramientas tecnológicas desarrolladas por la administración para hacer efectiva la *ciudadanía digital,* mediante el contacto virtual ciudadano-autoridad, el sostenimiento de páginas web por parte de todas las entidades públicas, nacionales y territoriales, y la popularización de los teléfonos celulares. Gracias a la densa dotación ciudadana e institucional de medios electrónicos, ha sido posible desarrollar importantes herramientas tecnológicas para la interlocución sociedad-estado, con gran beneficio para las personas y también para las instituciones. En este aspecto cabe mencionar, además de las páginas web singulares de más de mil quinientas instituciones públicas, idóneas para interactuar con los ciudadanos, el Portal del Estado Colombiano,[25] punto web que unifica el acceso a la información, los trámites y los servicios a cargo de las entidades del Estado. El Decreto nº 2.106, de 2019, ordenó simplificar, suprimir y reformar trámites,[26] al igual que modernizar el funcionamiento de la administración para implantar trámites, procesos y procedimientos administrativos sencillos, ágiles, coordinados, modernos y digitales. El capítulo II de esta ley, que se intitula “Transformación Digital para una Gestión Pública Efectiva”, estableció para la administración el deber y para los ciudadanos el derecho, de utilizar medios electrónicos mediante el modelo de Servicios Ciudadanos

[24] JORDÁN MOSQUERA, 2022.
[25] GOBIERNO EN LÍNEA, [2023].
[26] “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.”

Digitales,[27] que provee procedimientos y soluciones tecnológicas para la interacción digital de la administración con los ciudadanos.[28]

Ahora bien, la frontera de la digitalización administrativa se corrió nítidamente a partir del Documento CONPES nº 3.975, de 2019, mediante el cual el Consejo Nacional de Política Económica y Social adoptó e implantó una política nacional para la transformación digital e Inteligencia Artificial.[29]

Esta política tiene por objeto generar valor social y económico por medio del uso de las tecnologías digitales y la innovación digital pública y privada, e impulsar la competitividad y la productividad, de manera que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la Cuarta Revolución Industrial (4RI), que es la revolución de los datos y el *big data*, del almacenamiento masivo de información y la Inteligencia Artificial.

El CONPES nº 3.975 traza una ruta detallada para la transformación digital del Estado y del sector productivo, y plantea un enfoque en Inteligencia Artificial que comprende, entre otras, las siguientes acciones, dirigidas a los sectores público y privado: (i) fortalecer las competencias del capital humano para afrontar la 4RI, favoreciendo el desarrollo de competencias digitales durante la trayectoria educativa y la configuración de ecosistemas de innovación a través de alianzas internacionales para la formación de talento con prioridad en IA; (ii) impulsar otras tecnologías de la 4RI por medio del fomento al desarrollo de tecnologías digitales, la creación de ambientes de prueba regulatorio, financiamiento para la investigación y desarrollo tecnológico de IA.

De esta manera el gobierno hace una apuesta por la transformación digital, que está revolucionando la economía y la cultura, y es uno de los principales motores de la cuarta revolución industrial (4RI). La transformación digital incluye otras tecnologías digitales de la 4RI, como el Internet de las cosas, la robótica y la computación cuántica, que están trayendo el futuro a tiempo presente, y comienzan a impactar en la forma como vivimos, trabajamos e interactuamos.

Esta dirección de la política pública es consonante con la Carta Iberoamericana de Innovación en la Gestión Pública, aprobada por los 23 países miembros del CLAD en la "XIX Conferencia Iberoamericana de Ministras y Ministros de la Administración Pública y Reforma del Estado celebrada", en Andorra, el 8 de octubre de 2020. Entre sus numerosas disposiciones, la Carta destaca el teletrabajo como un ejemplo

[27] Decreto nº 620, de 2020: "Por el cual se establecen los lineamientos generales en el uso y operación de los servicios ciudadanos digitales."

[28] La Ley nº 2.052, de 2020 –"por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones" – reitera el deber que tiene el Estado de automatizar y digitalizar la gestión interna de trámites.

[29] COLOMBIA, 2019.

elocuente de una nueva forma de gestión pública eficiente que, además, fomenta el trabajo colaborativo, facilita las lógicas de inteligencia colectiva, y forma parte de lo que denomina la *Administración pública inteligente*.[30]

En lo concerniente a las relaciones entre Inteligencia artificial y administración pública, la Carta señala que la Administración pública no debe ser reactiva a la innovación de la gestión por la vía de la Inteligencia Artificial y, por el contrario, debe coliderar con el sector privado la agenda de innovación canalizada por la Inteligencia Artificial y la robótica. Se confía, por otra parte, en que la digitalización, la robotización y la gestión por la vía de la Inteligencia Artificial de la burocracia pueden contribuir decisivamente a erradicar la corrupción administrativa.

En sus fases más avanzadas la Inteligencia Artificial se manifiesta en el *internet de las cosas*, que permite la comunicación y el intercambio de datos entre objetos cotidianos sin intervención humana directa, y que en la administración pública tiene aplicaciones tan útiles como la digitalización de los flujos de tráfico urbano a través de cámaras y el reconocimiento de objetos y personas para efectos de seguridad.

Finalmente, se avanza hacia la creación de máquinas capaces de trabajar de una manera totalmente autónoma, aprehender el mundo y darle forma con sus acciones independientes. Esta última etapa es la que en algunos contextos se denomina singularidad (*singularity*), el momento en el que las máquinas serían capaces de pensar y actuar de forma independiente y, por consiguiente, al margen de los seres humanos.[31]

3 Conclusiones

La transformación digital de las organizaciones alude a los efectos económicos y sociales derivados de la digitalización, el procesamiento de los datos y el uso de las tecnologías digitales para desarrollar nuevos productos y servicios. Forma parte de la cuarta revolución industrial, que va dejando huella profunda en las reformas de la administración pública del presente.

Es evidente que la incorporación de la tecnología digital a los procesos y procedimientos de la administración pública le han permitido al Estado adoptar decisiones más eficientes, rápidas y masivas, facilita la publicidad y la transparencia de la gestión pública, contribuye a erradicar la corrupción, favorece el desarrollo de un Estado abierto. Este nuevo tipo de modernidad propicia el cumplimiento de los fines estatales, fortalece la legitimidad de las instituciones democráticas y produce mayor bienestar.

[30] CLAD, 2021.
[31] CLAD, 2021.

Con todo, la digitalización administrativa conlleva riesgos de naturaleza ética y política. Los procedimientos administrativos, según los hemos conocido tradicionalmente, se componen de reglas formuladas a partir de palabras que representan conceptos, objetos y acciones, y se combinan gramaticalmente para formar oraciones y expresar significados más complejos. Así han sido redactados los procedimientos administrativos por juristas y administradores públicos, mediante textos que son debatidos y aprobados por el poder legislativo. Dichas reglas, vertidas en un lenguaje que todo el mundo puede consultar y entender, permiten al ciudadano, al funcionario y al juez verificar que el contenido y la aplicación de dichas reglas a casos concretos sea acorde con la justicia y el ordenamiento jurídico.

Sin embargo, el conocimiento, la comprensión y el control público de las reglas administrativas se oscurece en la era digital. Las normas de la administración digital son elaboradas por ingenieros, por desarrolladores de la tecnología digital. La digitalización de los datos, su codificación y la secuencia de procedimientos mediante algoritmos que pretenden imitar procesos racionales, encierran la lógica de la actividad administrativa, antes pública y descifrable, en una caja negra accesible y comprensible únicamente para los técnicos que diseñan y administran los procedimientos administrativos digitales.

Los ciudadanos, al relacionarse con el Estado, ya no se comunican con personas sino con máquinas, cuya "inteligencia" ha sido programada para que realicen automáticamente muchas de las tareas que antes realizaban los funcionarios. Las decisiones de los funcionarios pueden ser reconsideradas porque se trata de una relación entre inteligencias afines. Pero, cuando son máquinas las que reciben, rechazan o tramitan peticiones, las sustancian y las deciden con base en informaciones estadísticas, procedimientos automáticos y soluciones tipo, la respuesta final es prácticamente incuestionable para el ciudadano. No es fácil la mutua comprensión entre una persona y una máquina, porque la causa de los eventuales errores de programación de la máquina suele ser indetectable para el ciudadano común, y porque la motivación automática del sistema no admite argumentos alternativos. Al no ser posible el diálogo entre un ser racional y un objeto que trata de imitar la racionalidad humana, en situaciones extremas serán infructuosos los esfuerzos del ser humano para procurar que la máquina razone en su favor frente a una decisión cuestionable.

La digitalización administrativa simplifica numerosas tareas rutinarias y masivas del Estado, pero suscita enorme preocupación cuando se extiende a decisiones relacionadas con los derechos de las personas. En tales casos la "clausura algorítmica a la deliberación" emerge como una negación a los derechos de defensa y contradicción, y por tanto al debido proceso.

Finalmente, los riesgos de las nuevas tecnologías aplicadas a la administración pública se convertirán en amenaza cuando los sistemas digitales, a partir de la reiteración y del ingreso de nuevos datos, no solo ejecuten las secuencias algorítmicas cada vez mejor, sino terminen aprendiendo y generando nuevo conocimiento de manera autónoma y por fuera del control humano. Habrá llegado entonces la Inteligencia Artificial en todo su esplendor.

Ante la inminencia de este inquietante futuro, por doquier se elevan voces de advertencia, para que las legislaciones adopten medidas preventivas y establezcan controles que permitan acotar prudentemente los alcances de la Inteligencia Artificial en el gobierno de las sociedades. Así, por ejemplo, la Carta Iberoamericana de Innovación en la Gestión Pública recomienda someter los algoritmos públicos, los procesos y el tipo de información con los que se alimentan los dispositivos de Inteligencia Artificial a la aprobación y monitoria de una agencia pública independiente que, además, verifique el cumplimiento de principios éticos y valores públicos.

La digitalización de los procedimientos administrativos tiene dos caras. Una nos llena de optimismo y de confianza en la realización del derecho a una buena administración, y en ese sentido avanzamos a pasos agigantados. La otra genera fundada incertidumbre alrededor de la vigencia de los derechos humanos y la preservación de la democracia, por lo cual se hace necesaria una cuidadosa regulación.

4 Referencias

BERNAL, Carlos. Derechos fundamentales e Inteligencia Artificial. *International Journal of Constitucional Law*, v. 20, n. 4, oct. 2022. Disponible en: https://academic.oup.com/icon/article/20/4/1431/7109154#401716135. Acceso en: 12 jan. 2023.

CAF. Banco de Desarrollo de América Latina. *DIG integridad*: La transformación digital de la lucha contra la corrupción, 2022.

CLAD. *Inteligencia Artificial y ética en la gestión pública*, 2021. Disponible en: https://clad.org/wp-content/uploads/2021/03/Libro-7-Inteligencia-artificial-y-%C3%A9tica-en-la-gesti%C3%B3n-p%C3%BAblica.pdf. Acceso en: 15 ago. 2022.

CLAD. *Carta Iberoamericana de Gobierno Abierto*, 2016. Disponible en: https://clad.org/wp-content/uploads/2020/07/Carta-Iberoamericana-de-Gobierno-Abierto-07-2016.pdf. Acceso en:15 ago. 2022.

CLAD. *Declaracíon de Lisboa.* Lisboa, 27 nov. 2020. Disponible en: https://clad.org/wp-content/uploads/2020/11/Declaracion-Lisboa-ES-2020-1.pdf. Acceso en: 30 jan. 2021

CEPAL. *Desde el gobierno abierto al Estado abierto en América Latina y el Caribe*, 2017. Disponible en: https://www.cepal.org/es/publicaciones/44769-gobierno-abierto-al-estado-abierto-america-latina-caribe. Acceso en: 11 jul. 2021.

COLOMBIA. Consejo Nacional de Política Económica y Social (CONPES). *Política nacional para la transformación digital e Inteligencia Artificial.* Documento CONPES 3975, 8 nov. 2019. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf. Acceso en: 11 ago. 2022.

COLOMBIA. Corte Constitucional. *Sentencia C-491/07.* Demanda de inconstitucionalidad contra la Ley nº 1097 de 2006. Referencia: expediente D-6583. Actor: Franky Urrego Ortiz. Relator: Dr. Jaime Córdoba Triviño. Bogotá, 27 jun. 2022.

COLOMBIA. Corte Constitucional. *Sentencia T-511/10.* Acción de tutela instaurada por Zonia Betancourt Rojas y Gabriela Fuquene Betancourt contra la Policía Nacional. 2010. Expediente T-2.395.898. Relator: Humberto Antonio Sierra Porto. Bogotá, 18 jun. 2010.

COLOMBIA. Agencia nacional de contratación publica. *SECOP II.* Disponible en: https://www.colombiacompra.gov.co/secop-ii. Acceso en: 4 feb. 2023.

BECERRA, Augusto Hernández. Del derecho de petición a la transparencia digital en Colombia. *Revista de Direito Administrativo, Infraestrutura, Regulação e Compliance*, São Paulo, n. 20, ano 6, p. 281-308, jan./mar. 2022.

GOBIERNO EN LÍNEA. *Encuentra los trámites, servicios e información del Estado colombiano*, [2023]. Disponible en: https://www.gov.co. Acceso en: 19 feb. 2023.

JORDÁN MOSQUERA, Daniela. El Decreto 806 de 2020 y su adopción como legislación permanente mediante la Ley nº 2213 de 2022. *Boletín Virtual, Universidad Externado de Colombia*, Departamento de Derecho Procesal, 4 oct. 2022. Disponible en: https://procesal.uexternado.edu.co/el-decreto-806-de-2020-y-su-adopcion-como-legislacion-permanente-mediante-la-ley-2213-de-2022/. Acceso en: 20 dez. 2022.

LALOUX, Frederic. *Reinventar las organizaciones*. Madrid: Arpa Editores, 2016.

NIELSEN ENEMARK, Carlos A. *El uso de Inteligencia Artificial en el acto administrativo. Revista de Derecho Administrativo – RDA*, Buenos Aires, jul. 2021. Disponible en: https://www.researchgate.net/publication/352970274_El_uso_de_inteligencia_artificial_en_el_acto_administrativo/citation/download. Acceso en:13 jan. 2023.

OCDE. *Gobierno Abierto*: Contexto mundial y el camino a seguir. Aspectos claves, 2016. Disponible en: https://www.oecd.org/gov/Open-Government-Highlights-ESP.pdf. Acceso en: 11 set. 2019.

OCDE. *Recommendation of the council on Artificial Intelligence*, 2019. Disponible en: https://ia-latam.com/portfolio/principios-de-la-ocde-sobre-ia/. Acceso en: 1 mar. 2020.

RAMIÓ, Carles. *Inteligencia Artificial y administración pública*: Robots y humanos compartiendo el servicio público. Madrid: Libros de la Catarata, 2019.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

BECERRRA, Augusto Hernández. Avances de la administración colombiana en la era digital. *International Journal of Digital Law*, Belo Horizonte, ano 4, n. 1, p. 87-106, jan./abr. 2023. DOI: 10.47975/digital.law.vol.4.n.1.becerra.

Sobre a Revista

IJDL – INTERNATIONAL JOURNAL OF DIGITAL LAW

Objetivo

O International Journal of Digital Law é um periódico científico eletrônico de acesso aberto e periodicidade quadrimestral promovido pelo **Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano (NUPED), do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná**.

O Conselho Editorial é composto por renomados professores vinculados a instituições de ensino superior do Brasil, Argentina, Austrália, Colômbia, Espanha, Egito, França, Holanda e Índia. A linha editorial segue o eixo das atividades de pesquisa do NUPED, um grupo inscrito no diretório do CNPq e filiado à **Rede de Pesquisa em Direito Administrativo Social (REDAS)**. Seu enfoque é o estudo crítico das instituições jurídico-políticas típicas do Estado de Direito, notadamente as voltadas à inovação e ao desenvolvimento humano por intermédio da revolução digital.

Linha Editorial

A linha editorial segue o eixo de concentração do **NUPED – PPGD/PUCPR** intitulada "**Direito Econômico e Desenvolvimento**". Por sua vez, a área congrega duas importantes linhas de pesquisa: 1. **Estado, Economia e Desenvolvimento** e 2. **Direitos Sociais, Globalização e Desenvolvimento**. A revista dará destaque a este marco teórico. Entretanto, transversalmente ao tema da economia, do desenvolvimento, da globalização e dos direitos sociais, as palavras-chave que melhor definem o escopo da revista implicam a tratativa de temas como: acesso à informação, *big data*, *blockchain*, cidades inteligentes, contratos inteligentes, *crowdsourcing*, cibercrimes, democracia digital, direito à privacidade, direitos fundamentais, *e-business*, economia digital, educação digital, eficiência administrativa, e-*government*, *fake news*, *gig economy*, globalização, inclusão digital, infraestrutura, inovação, inteligência artificial, interesse público, internet, internet das coisas, jurimetria, *lawfare*, novas tecnologias, perfilamento digital, pesquisa em multimeios, processo administrativo eletrônico, proteção de dados, regulação administrativa, regulação econômica, risco, serviços públicos, sistemas de informação, sociedade da informação, transparência governamental e telecomunicações.

Double blind peer review

A publicação dos artigos submete-se ao procedimento *double blind peer review*. Os trabalhos são remetidos sem identificação de autoria a dois pareceristas *ad hoc* portadores de título de doutor, todos eles exógenos à instituição promotora da revista (PUCPR). Os pareceristas são, portanto, sempre pesquisadores vinculados a renomadas instituições de ensino superior nacionais e estrangeiras.

Cobertura temática (classificação do CNPq)

GRANDE: Ciências Sociais Aplicadas (6.00.00.00-7)/Área: Direito (6.01.00.00-1)/ Subárea: Direitos Especiais (6.01.04.00-7)

GRANDE: Ciências Sociais Aplicadas (6.00.00.00-7)/Área: Ciência da Informação (6.07.00.00-9)/Subárea: Teoria da Informação (6.07.01.00-5)

GRANDE: Ciências Exatas e da Terra (1.00.00.00-3)/Área: Ciência da Computação 1.03.00.00-7/Subárea: Sistemas de Computação (1.03.04.00-2)

Diretrizes para Autores

1. Submissão de artigos
As propostas de artigos para publicação na *International Journal of Digital Law* deverão ser enviadas através do sistema eletrônico de submissões (gratuitamente), por meio de cadastro no Sistema Eletrônico e acesso mediante login e senha a ser realizado no site. Não serão aceitas propostas enviadas por e-mail. A revista reserva-se o direito de aceitar ou rejeitar qualquer original recebido, de acordo com as recomendações do seu corpo editorial, inclusive por inadequação da temática do artigo ao perfil editorial da revista, como também o direito de propor eventuais alterações.

2. Qualificação dos autores
Ao menos um dos autores do artigo deverá possuir o título de Doutor (Dr.), Doctor of Juridical Science (J.S.D. ou S.J.D.), Doctor juris (Dr. iur. ou Dr. jur.), Doctor of Philosophy (Ph.D.) ou Legum Doctor (LL.D.). A exigência poderá ser relativizada, nunca extrapolando o percentual de 30% por edição, em casos excepcionais de: (i) artigos de autores afiliados a instituições estrangeiras; (ii) artigos escritos em inglês.

3. Ineditismo e exclusividade
Os textos para publicação na *International Journal of Digital Law* deverão ser inéditos e para publicação exclusiva, salvo no caso de artigos em língua estrangeira que tenham sido publicados fora do país. Uma vez publicados nesta revista, também poderão sê-lo em livros e coletâneas, desde que citada a publicação original. Roga-se aos autores o compromisso de não publicação em outras revistas e periódicos, bem como de que as propostas de artigo não se encontrem postulados de forma simultânea em outras revistas ou órgãos editoriais.

4. Idiomas
Podem ser submetidos artigos redigidos em Português, Espanhol ou Inglês.

5. Cadastro dos metadados no sistema eletrônico de submissões
5.1. No momento da submissão do artigo no sistema eletrônico, os campos dos metadados deverão ser preenchidos obrigatoriamente de acordo com estas diretrizes, sob pena de rejeição liminar da submissão.
5.2. Autores
5.2.1. *Nome/Nome do Meio/Sobrenome:* indicação do nome completo do(s) autor(es) apenas com as iniciais de cada nome em caixa alta. Em caso de artigos em coautoria, os nomes de todos os coautores devem ser inseridos no sistema na ordem que deverá constar no momento da publicação.
5.2.2. *E-mail:* indicação do e-mail do(s) autor(es) para contato, que será obrigatoriamente divulgado na versão publicada do artigo.
5.2.3. *ORCID iD:* indicação do número de identificação ORCID (para maiores informações clique aqui). O identificador ORCID pode ser obtido no registro ORCID. Você deve aceitar os padrões para apresentação de iD ORCID e incluir a URL completa; por exemplo: https://orcid.org/0000-0003-1781-1726.

5.2.4. *URL:* link para o currículo completo do autor. No caso de autores brasileiros, deve ser indicado o link para o Currículo Lattes.
5.2.5. *Instituição/Afiliação:* indicação da sua principal afiliação institucional ou das duas principais, caso o vínculo com ambas possua a mesma importância (instituição à qual encontra-se vinculado como docente ou discente, ou, caso não seja docente ou discente, a instituição onde foi obtido o seu maior título acadêmico, como doutorado, mestrado, especialização etc.). O nome da instituição deverá constar por extenso e na língua original da instituição (ou em inglês quando a escrita não for latina), seguida da indicação do país de origem da instituição entre parênteses. Caso o autor seja docente e esteja cursando mestrado ou doutorado em outra instituição, a afiliação principal será a da instituição na qual o autor figura como mestrando ou doutorando.
5.2.6. *País:* indicação do país da principal afiliação institucional do autor.
5.2.7. *Resumo da biografia:* indicação do mini currículo, iniciando com a indicação da instituição onde figura como docente, seguida de cidade, sigla do Estado e país entre parênteses, indicação das titulações acadêmicas (começando pela mais elevada), outros vínculos com associações científicas, profissão etc.
5.3. Título e Resumo
5.3.1. *Título:* título no idioma do artigo, com apenas a primeira letra da sentença em maiúscula.
5.3.2. *Resumo:* resumo no idioma do artigo, sem parágrafo ou citações e referências, com até 200 palavras.
5.4. Indexação
5.4.1. *Palavras-chave*: indicação de 5 palavras-chave no idioma do artigo (em letras minúsculas e separadas por ponto vírgula).
5.4.2. *Idioma*: indicar a sigla correspondente ao idioma do artigo (Português=pt; English=en; Español=es).
5.5. Contribuidores e Agências de fomento: os artigos resultantes de projetos de pesquisa financiados deverão indicar neste campo a fonte de financiamento.
5.6. Referências: inserir a lista completa de referências citadas no artigo, dando um espaço entre cada uma delas.

6. Apresentação do texto e elementos pré-textuais
6.1. Recomenda-se que o trabalho tenha entre 15 e 30 páginas (tamanho A4 – 21 cm x 29,7 cm), compreendendo a introdução, desenvolvimento, conclusão (não necessariamente com esses títulos) e uma lista de referências bibliográficas.
6.2. As margens utilizadas deverão ser: esquerda e superior de 3 cm e direita e inferior de 2 cm.
6.3. No corpo do texto deverá ser utilizada Fonte Times New Roman, tamanho 12, espaçamento entre linhas de 1,5 cm e espaçamento de 0 pt (pontos) antes e depois dos parágrafos.
6.4. Nas notas de rodapé deverá ser utilizada Fonte Times New Roman, tamanho 10, espaçamento simples entre linhas.
6.5. No desenvolvimento do texto, os parágrafos deverão conter recuo de 1,5 cm em relação à margem esquerda. Títulos e subtítulos deverão estar alinhados à margem esquerda, sem recuo.
6.6. A estruturação deverá observar a exposta neste item 6.6.

6.6.1. Título no idioma do artigo, com apenas a primeira letra da sentença em maiúscula e em itálico, centralizado.
6.6.2. Nos casos de necessidade de indicar informações a respeito do artigo (financiamento por agências de fomento, agradecimentos, tradutores do texto etc.), deverá ser inserida uma nota de rodapé com um asterisco (e não com número) situada à direita do título no idioma do artigo.
6.6.3. Título em inglês, com apenas a primeira letra da sentença em maiúscula, em itálico e centralizado. No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelo título em português.
6.6.4. O artigo não deve incluir os nomes do(s) autor(es). As informações, para fins de publicação, serão retiradas dos metadados inseridos pelo(s) autor(es) no sistema eletrônico da revista no momento da submissão.
6.6.5. Resumo no idioma do artigo (fonte Times New Roman 12, espaçamento entre linhas simples, sem parágrafo ou citações e referências, com até 200 palavras), antecedido da palavra "Resumo" escrita no idioma do artigo.
6.6.6. Indicação de 6 palavras-chave no idioma do artigo (em letras minúsculas e separadas por ponto vírgula), antecedidas da expressão "Palavras-chave" redigida no idioma do artigo.
6.6.7. Resumo em inglês (Fonte Times New Roman 12, espaçamento entre linhas simples, sem parágrafo ou citações e referências, com até 200 palavras), antecedido da palavra "Abstract". No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelo resumo em português.
6.6.8. Indicação de seis palavras-chave em inglês (em letras minúsculas e separadas por ponto e vírgula), antecedidas da expressão "Keywords". No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelas palavras-chave em português.
6.6.9. Sumário com a identificação dos títulos das seções e das subseções, com numeração progressiva, separados por ponto vírgula, sequencialmente e em parágrafo único.
6.6.10. Desenvolvimento do trabalho científico: a numeração progressiva, em números arábicos, deve ser utilizada para evidenciar a sistematização do conteúdo do trabalho.
6.6.11. Lista das referências bibliográficas efetivamente utilizadas no artigo, ao final do trabalho, separadas por um espaço simples, alinhadas à margem esquerda (sem recuo).
6.6.12. Aplicam-se, para os demais aspectos de formatação, as normas técnicas brasileiras (ABNT NBR 10520:2002 e 14724:2011).
6.6.13. No caso de artigos com 4 ou mais autores, é necessário incluir uma nota de rodapé indicando qual foi a contribuição de cada um.
6.7. Todo destaque que se queira dar ao texto deve ser feito com o uso de itálico, ficando vedada a utilização de negrito, sublinhado ou caixa alta para fins de dar destaque ao texto.
6.8. Figuras e tabelas devem estar inseridas no texto, e não no final do documento na forma de anexos.

7. Metodologia científica
7.1. As referências dos livros, capítulos de obras coletivas, artigos, teses, dissertações e monografias de conclusão de curso de autores citados ou utilizados como base

para a redação do texto devem constar em nota de rodapé, com todas as informações do texto, em observância às normas técnicas brasileiras (ABNT NBR 6023:2018), e, especialmente, com a indicação da página da qual se tirou a informação apresentada no texto logo após a referência.

7.1.1. O destaque dado ao título dos livros (ou revistas) citados deverá constar em itálico, ficando vedada a utilização de negrito.

7.1.2. Os artigos redigidos com citação no formato AUTOR-DATA não serão aceitos para publicação, somente o sistema de chamadas numérico exposto nas notas de rodapé.

7.1.3. As referências deverão constar da seguinte forma:

7.1.3.1. Livros:

SOBRENOME, Nome. *Título da obra em itálico*: subtítulo sem itálico. número da edição. Cidade: Editora, ano.

Exemplo:

KEEN, Andrew. *Vertigem digital*: por que as redes sociais estão nos dividindo, diminuindo e desorientando. Trad. Alexandre Martins, Rio de Janeiro: Zahar, 2012. 254p.

7.1.3.2. Capítulos de livros coletivos:

SOBRENOME, Nome. Título do capítulo sem itálico. In: SOBRENOME DO 1º ORGANIZADOR, Nome do organizador; SOBRENOME DO 2º ORGANIZADOR, Nome do 2º organizador e assim sucessivamente, separados por ponto vírgula (Org. ou Coord.). *Título da obra ou coletânea em itálico*: subtítulo sem itálico. número da edição. Cidade: Editora, ano. página inicial-página final [antecedidas de "p."].

Exemplo**:**

DOTTA, Alexandre Godoy. Derechos de la Población LGBT+ en Brasil: Vulnerabilidad Social entre Avances y Retrocesos. In: BRAVO, Álvaro Sánches; CASIMIRO, Ligia Melo de; GABARDO, Emerson. (Org.). *Estado Social Y Derechos Fundamentales en Tiempos de Retroceso*. Sevilha: Ponto Rojo, 2019. p. 203-228.

7.1.3.3. Artigos em revistas:

SOBRENOME, Nome. Título do artigo sem itálico. *Título da Revista em itálico*, cidade, volume, número, página inicial-página final [antecedidas de "p."], meses da publicação [abreviados com as três primeiras letras do mês seguidas de ponto e separados por barra]. ano.

Exemplo:

GABARDO, Emerson; SAIKALI, Lucas Bossoni. A prescritibilidade da ação de ressarcimento ao erário em razão de atos de improbidade administrativa. *Revista Jurídica – Unicuritiba*, Curitiba, v. 1, p. 514-543, 2018.

7.1.3.4. Teses de Titularidade, Livre-Docência, Doutorado, Dissertações de Mestrado, Monografias de Conclusão de Curso de Graduação e Pós-Graduação:

SOBRENOME, Nome. *Título do trabalho em itálico*: subtítulo sem itálico. Cidade, ano. número de folhas seguido de "f". Modalidade do trabalho (Grau obtido com a defesa) – Órgão perante o qual o trabalho foi defendido, Nome da instituição.

Exemplo:

SANTOS, Fábio de Sousa. *Análise Comparada da Competição na Contratação Pública Brasileira e Estadunidense*. Curitiba, 2018. 134f. Dissertação (Mestrado em Mestrado em Direito) – Pontifícia Universidade Católica do Paraná. Curitiba: 2018.

7.1.3.5 DOI – Digital object identifier: Caso o documento consultado na pesquisa tenha o número de DOI recomenda-se a inclusão, de modo complementar, do número após o término de cada referência.
Exemplo:
DOTTA, Alexandre Godoy. Public policies for the assessment of quality of the Brazilian higher education system. *Revista de Investigações Constitucionais*, Curitiba, v. 3, p. 53-69, 2016. DOI. 10.5380/rinc.v3i3.49033.
7.1.3.6. Documentos em meio eletrônico: Documentos extraídos do meio eletrônico deverão apresentar após o término de cada referência o local da rede onde foi encontrado e apresentado da seguinte maneira.
Exemplo:
IJDL. International Journal of Digital Law. *Regras para a submissão de artigos*. Disponível em: https://journal.nuped.com.br/index.php/revista/about/submissions. Acesso em: 12 fev. 2020.
7.1.4. Os elementos das referências devem observar o seguinte padrão:
7.1.4.1. Autor: SOBRENOME em maiúsculas, vírgula, Nome com as iniciais em maiúsculas, seguido de ponto final.
7.1.4.2. Edição: deve ser incluída a informação somente a partir da segunda edição, sem ordinal, seguido de ponto e "ed.". Exemplo: 2. ed.
7.1.4.3. Ano: grafado com algarismos arábicos, sem ponto no milhar, antecedido de vírgula e seguido de ponto.
7.1.5. Nos casos em que for absolutamente impossível obter alguma das informações acima, a ausência deverá ser suprida da seguinte forma:
7.1.5.1. Ausência de cidade: substituir por [S.l.].
7.1.5.2. Ausência de editora: substituir por [s.n.].
7.1.5.3. Ausência de ano: indicar entre colchetes o ano aproximado, seguido de ponto de interrogação. Exemplo: [1998?].
7.2. As citações (palavras, expressões, períodos) deverão ser cuidadosamente conferidas aos textos originais.
7.2.1. Citações diretas devem seguir o seguinte padrão de registro: transcrição com até quatro linhas devem constar do corpo do texto, com letra e espaçamento normais, e estar entre aspas.
7.2.2. Recomenda-se fortemente que citações textuais longas (mais de quatro linhas) não sejam utilizadas. Entretanto, se imprescindíveis, deverão constituir um parágrafo independente, com recuo de 1,5 cm em relação à margem esquerda (alinhamento justificado), utilizando-se espaçamento entre linhas simples e tamanho da fonte 10. Neste caso, aspas não devem ser utilizadas.
7.2.3. Fica vedado o uso do op. cit., loc. cit., ibidem e idem nas notas bibliográficas, que deverão ser substituídas pela referência completa, por extenso.
7.2.4. Para menção de autores no corpo do texto, fica vedada sua utilização em caixa alta (ex.: para Nome SOBRENOME...). Nestes casos todas as menções devem ser feitas apenas com a primeira letra maiúscula (ex.: para Nome Sobrenome...).

8. Redação
8.1. Os textos devem ser revisados, além de terem sua linguagem adequada a uma publicação editorial científica.

8.2. No caso de artigos redigidos na língua portuguesa, a escrita deve obedecer às regras ortográficas em vigor desde a promulgação do ACORDO ORTOGRÁFICO DA LÍNGUA PORTUGUESA, a partir de 1º de janeiro de 2009.
8.3. As citações de textos anteriores ao ACORDO devem respeitar a ortografia original.

9. Artigos resultantes de pesquisas financiadas
Os artigos resultantes de projetos de pesquisa financiados deverão indicar em nota de rodapé, situada ao final do título do artigo no idioma do texto, a informação relativa ao financiamento da pesquisa.

10. Declaração de direitos autorais
Autores que publicam nesta revista concordam com os seguintes termos:
10.1. Não serão devidos direitos autorais ou qualquer outra remuneração pela publicação dos trabalhos.
10.2. Autores mantêm os direitos autorais e concedem à *IJDL* o direito de primeira publicação, com o trabalho simultaneamente licenciado sob a Licença Creative Commons Attribution que permite o compartilhamento do trabalho com reconhecimento da autoria e publicação inicial nesta revista. Ainda, em virtude de aparecerem nesta revista de acesso público, os artigos são de uso gratuito, com atribuições próprias, com aplicações educacionais e não comerciais.
10.3. Autores têm permissão e são estimulados a publicar e distribuir seu trabalho online (ex.: em repositórios institucionais ou na sua página pessoal) a qualquer ponto antes ou durante o processo editorial, já que isso pode gerar alterações produtivas, bem como aumentar o impacto e a citação do trabalho publicado (ver O Efeito do Acesso Livre).

11. Responsabilidade dos autores
11.1. Autores são responsáveis pelo conteúdo publicado, comprometendo-se, assim, a participar ativamente da discussão dos resultados de sua pesquisa científica, bem como do processo de revisão e aprovação da versão final do trabalho.
11.2. Autores são responsáveis pela condução, resultados e validade de toda investigação científica.
11.3. Autores devem noticiar a revista sobre qualquer conflito de interesse.
11.4. As opiniões emitidas pelos autores dos artigos são de sua exclusiva responsabilidade.
11.5. Ao submeter o artigo, o autor atesta que todas as afirmações contidas no manuscrito são verdadeiras ou baseadas em pesquisa com razoável exatidão.

12. Conflito de interesses
A confiabilidade pública no processo de revisão por pares e a credibilidade de artigos publicados dependem em parte de como os conflitos de interesses são administrados durante a redação, revisão por pares e tomada de decisões pelos editores.
12.1. É obrigatório que o autor do manuscrito declare a existência ou não de conflitos de interesse. Mesmo julgando não haver conflitos de interesse, o autor deve declarar essa informação no ato de submissão do artigo, marcando esse campo específico.
12.2. Conflitos de interesses podem surgir quando autores, pareceristas ou editores possuem interesses que, aparentes ou não, podem influenciar a elaboração ou avaliação

de manuscritos. O conflito de interesses pode ser de natureza pessoal, comercial, política, acadêmica ou financeira.

12.3. Quando os autores submetem um manuscrito, eles são responsáveis por reconhecer e revelar conflitos financeiros ou de outra natureza que possam ter influenciado seu trabalho.

12.4. Os autores devem reconhecer no manuscrito todo o apoio financeiro para o trabalho e outras conexões financeiras ou pessoais com relação à pesquisa. As contribuições de pessoas que são mencionadas nos agradecimentos por sua assistência na pesquisa devem ser descritas, e seu consentimento para publicação deve ser documentado.

12.5. Manuscritos não serão rejeitados simplesmente por haver um conflito de interesses, mas deverá ser feita uma declaração de que há ou não conflito de interesses.

12.6. Os pareceristas devem, igualmente, revelar aos editores quaisquer conflitos de interesse que poderiam influir em suas opiniões sobre o manuscrito, e devem declarar-se não qualificados para revisar originais específicos se acreditarem que esse procedimento é apropriado. Assim como no caso dos autores, se houver silêncio por parte dos pareceristas sobre conflitos potenciais, isso significará que os conflitos não existem.

12.7. No caso da identificação de conflito de interesse da parte dos pareceristas, o Conselho Editorial encaminhará o manuscrito a outro parecerista *ad hoc*.

12.8. Se os autores não tiverem certeza do que pode constituir um potencial conflito de interesses, devem contatar o Coordenador Editorial da Revista.

12.9. Para os casos em que editores ou algum outro membro publiquem com frequência na Revista, não serão atribuídos tratamentos especiais ou diferenciados. Todos os artigos submetidos serão avaliados através do procedimento *double blind peer review*.

13. Outras informações

13.1. Os trabalhos serão selecionados pelo Coordenador Editorial e pelo Conselho Editorial da Revista, que entrarão em contato com os respectivos autores para confirmar o recebimento dos textos, e em seguida os remeterão para análise de dois pareceristas do Conselho de Pareceristas.

13.2. Os originais recebidos e não publicados não serão devolvidos.

13.3. Asseguram-se aos autores o direito de recurso das decisões editorais.

13.3.1. Serão concedidos 5 (cinco) dias, contados da data da decisão final do Conselho Editorial.

13.3.2. O arrazoado escrito deverá ser enviado para o e-mail: journal@nuped.com.br.

13.3.3. O recurso será analisado pelo Conselho Editorial no prazo de 30 (trinta) dias.

CONDIÇÕES PARA SUBMISSÕES

Como parte do processo de submissão, os autores são obrigados a verificar a conformidade da submissão em relação a todos os itens listados a seguir. As submissões que não estiverem de acordo com as normas serão devolvidas aos autores.

1. A contribuição é original e inédita (salvo em caso de artigos em língua estrangeira publicados no exterior), e não está sendo avaliada para publicação por outra revista; caso contrário, deve-se justificar em “Comentários ao editor”.
2. O arquivo da submissão está em formato Microsoft Word.
3. URLs para as referências foram informadas quando possível.

4. O texto possui entre 15 e 30 páginas (tamanho A4 – 21 cm x 29,7 cm), compreendendo a introdução, desenvolvimento, conclusão (não necessariamente com esses títulos) e uma lista de referências bibliográficas; as margens utilizadas são: esquerda e superior de 3 cm e direita e inferior de 2 cm; no corpo do texto utilizou-se Fonte Times New Roman, tamanho 12, espaçamento entre linhas de 1,5, e espaçamento de 0 pt antes e depois dos parágrafos; nas notas de rodapé utilizou-se Fonte Times New Roman, tamanho 10, espaçamento simples entre linhas; no desenvolvimento do texto, os parágrafos contêm recuo de 1,5 cm em relação à margem esquerda; títulos e subtítulos estão alinhados à margem esquerda, sem recuo; as figuras e tabelas estão inseridas no texto, não no final do documento na forma de anexos.
5. O texto segue os padrões de estilo e requisitos bibliográficos descritos em Diretrizes para Autores, na página para submissão.
6. Em caso de submissão a uma seção com avaliação pelos pares (ex.: artigos), as instruções disponíveis em Assegurando a avaliação pelos pares cega foram seguidas.
7. O autor declara que, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, este artigo é de sua autoria e, portanto, não contém plágio. Declara, ainda, que está ciente das implicações legais que a utilização de material de terceiros acarreta.
8. O autor declara que participou suficientemente do trabalho para tornar pública sua responsabilidade pelo conteúdo e que todas as afirmações contidas no manuscrito são verdadeiras ou baseadas em pesquisa com razoável exatidão.
9. O autor concorda com a política de responsabilidade estabelecida no item 10. Responsabilidade dos autores das Diretrizes para Autores.

POLÍTICA DE PRIVACIDADE

Os nomes e endereços informados nesta revista serão usados exclusivamente para os serviços prestados por esta publicação, não sendo disponibilizados para outras finalidades ou a terceiros.

Este periódico tem um compromisso com a ética e a qualidade das publicações, seguindo padrões internacionais de publicação científica. Defendemos um comportamento ético de todas as partes envolvidas na publicação em nosso periódico: autores, editor, pareceristas, Equipe Editorial e a Editora. Não aceitamos plágio ou qualquer outro comportamento antiético. Para isso, são seguidas as diretrizes do 2nd World Conference on Research Integrity, Singapore, July 22-24, 2010.

Deveres do Editor

- **Decisão de publicação:** o editor é responsável por decidir quais artigos submetidos à revista devem ser publicados. O editor é guiado pelas políticas decididas pelo Conselho Editorial. Essas políticas devem obedecer às exigências legais em vigor sobre difamação, violação de direitos autorais e plágio. Para tomada de decisões o editor pode consultar o Conselho Editorial e os pareceristas.
- **Transparência e respeito:** o editor deve avaliar os manuscritos submetidos sem levar em conta a raça, sexo, a orientação sexual, a crença religiosa, a origem étnica, a nacionalidade ou a filosofia política dos autores.

- **Confidencialidade:** o editor e demais membros da equipe editorial não devem divulgar qualquer informação sobre um manuscrito submetido, a não ser aos pareceristas e os conselheiros editoriais.
- **Divulgação e conflitos de interesse:** O editor não deve utilizar materiais inéditos divulgados em um manuscrito submetido em pesquisas próprias sem o consentimento expresso e por escrito do autor. O editor deve recusar avaliar os manuscritos em que tenha conflitos de interesse por questões competitivas, colaborativas ou outros relacionamentos ou ligações com qualquer um dos autores, empresas ou (possivelmente) instituições ligadas aos manuscritos.
- **Envolvimento e cooperação em investigações:** o editor deve tomar medidas necessárias cabíveis quando foram apresentadas reclamações éticas a respeito de um manuscrito submetido ou artigo publicado.

Deveres dos Pareceristas

- **Contribuição para as decisões editoriais:** a revisão dos pareceristas auxilia o editor na tomada de decisões editoriais e por meio das comunicações com o autor também pode auxiliar o mesmo na melhora do artigo.
- **Pontualidade:** qualquer avaliador de artigo que não se sinta qualificado para analisar o artigo ou sabe que a sua imediata leitura será impossível deve notificar imediatamente o editor.
- **Confidencialidade:** os trabalhos recebidos para análise devem ser tratados como documentos confidenciais. Eles não devem ser mostrados ou discutidos com os outros.
- **Padrões de objetividade:** os pareceres devem ser conduzidos de forma objetiva. Os pareceristas devem expressar seus pontos de vista de maneira clara e apoiados em argumentos.
- **Sobre as fontes:** os pareceristas devem identificar trabalhos publicados relevantes que não foram citados pelos autores. O parecerista deve chamar a atenção do editor sobre qualquer semelhança substancial ou sobreposição entre o manuscrito em questão e qualquer outro *artigo* publicado de que tenha conhecimento pessoal.
- **Divulgação e conflito de interesses:** informações privilegiadas ou ideias obtidas pelo parecerista por meio da leitura dos manuscritos devem ser mantidas em sigilo e não devem utilizadas para proveito pessoal. O parecerista não deve avaliar manuscritos em que tenha conflitos de interesse por questões competitivas, colaborativas ou outros relacionamentos ou ligações com qualquer um dos autores, empresas ou instituições ligadas aos manuscritos.

Deveres dos Autores

- **Normas gerais:** os autores de trabalhos que se referem a pesquisas originais devem apresentar um relato preciso do trabalho realizado, bem como uma discussão objetiva sobre o seu significado. Dados complementares devem ser representados com precisão no artigo. O documento deve conter detalhes suficientes e referências que permitam que outros possam replicar o trabalho. Declarações fraudulentas ou intencionalmente imprecisas constituem um comportamento antiético e são inaceitáveis.

- **Originalidade e plágio:** os autores devem garantir que as obras são inteiramente originais e se eles utilizam o trabalho e/ou textos dos outros que isso seja devidamente citado. Plágio em todas as suas formas constitui um comportamento editorial antiético e é inaceitável.
- **Publicação múltipla ou redundante:** um autor não deve publicar manuscritos que descrevam essencialmente a mesma pesquisa em mais de um periódico. Publicar o mesmo artigo em mais de um periódico sem informar os editores e obter seu consentimento constitui um comportamento editorial antiético e é inaceitável.
- **Sobre as fontes:** o trabalho de outros autores deve sempre ser reconhecido. Os autores devem citar as publicações que foram importantes na determinação da natureza do trabalho relatado. As informações obtidas em particular, como em uma conversa, correspondência, ou discussão com terceiros, não devem ser utilizadas ou relatadas sem a permissão explícita por escrito da fonte. As informações obtidas por meio de serviços confidenciais, tais como arbitragem manuscritos ou pedidos de bolsas, não devem ser utilizadas sem a permissão explícita por escrito do autor do trabalho envolvido nestes serviços.
- **Autoria:** a autoria do trabalho deve ser restrita àqueles que fizeram uma contribuição significativa para a concepção, projeto, execução ou interpretação do estudo relatado. Todos aqueles que fizeram contribuições significativas devem ser listados como coautores. Pessoas que participaram em certos aspectos do projeto de pesquisa devem ser listadas como colaboradores. O autor principal deve garantir que todos os coautores apropriados estejam incluídos no artigo. O autor principal também deve certificar-se que todos os coautores viram e aprovaram a versão final do manuscrito e que concordaram com sua submissão para publicação.
- **Divulgação e conflitos de interesses:** todos os autores devem divulgar no manuscrito qualquer conflito financeiro ou de outra natureza que possa influenciar os resultados ou a interpretação de seu manuscrito. Todas as fontes de apoio financeiro para o projeto devem ser divulgadas.
- **Erros fundamentais em trabalhos publicados:** quando um autor descobre um erro significativo ou imprecisão em seu trabalho publicado é obrigação do autor informar imediatamente o editor da revista ou a Editoria de Periódicos e cooperar com o editor para corrigir o artigo.

Deveres da Editora

Estamos empenhados em garantir que publicidade, reimpressão ou qualquer outra fonte de receita comercial não tenha qualquer impacto ou influência sobre as decisões editoriais.

Nossos artigos são avaliados por pares para garantir a qualidade da publicação científica. Este periódico utiliza o CrossCheck (software antiplágio da CrossRef).

* Esta declaração se baseia nas recomendações da Elsevier e no *Best Practice Guidelines for Journal Editors* do Committee on *Publication Ethics – COPE*.

Author Guidelines

1. Article Submission

Article propositions for publishing on the International Journal of Digital Law must be sent through the electronic submission system (free of cost) and access through login and password. Propositions sent by e-mail will not be accepted. The Journal has the right to accept or reject any originals received, according to its Editorial Board's recommendations, including the inadequacy of the article's theme to the journal's editorial profile, as well as the right to propose modifications.

2. Author Qualification

At least one of the authors must own either a PhD degree or a Doctor of Juridical Science (J.S.D. or S.J.D), Doctor juris (Dr. iur. or Dr. jur.), Doctor of Philosophy (Ph.D.) ou Legum Doctor (LL.D.) degree. This requirement can be relativized, never exceeding 30% of the articles per edition, in exceptional cases of: (i) authors affiliated to foreign institutions; (ii) articles written in English.

3. Originality and exclusivity

Articles for publication in the International Journal of Digital Law must be original and exclusive, except in case of articles written in a foreign language and published outside Brazil. After the publication of the article in this journal, it can also be published in books and compilations, as long as the original publication is mentioned. We ask the authors to commit to not publish the article in other journals or reviews, as well as not to submit it to other journals at the same time.

4. Languages

Articles can be submitted in English, Portuguese, and Spanish.

5. Registration of the metadata in the electronic submission system

5.1. At the time of submission of the article to the electronic system, the metadata fields must be filled in according to these guidelines, under penalty of preliminary rejection of the submission.

5.2. Authors

5.2.1. *First name/Middle name/Last name:* indication of the full name of the author(s) with only the initials of each name in capital letter. In case of articles in co-authorship, the names of all coauthors must be inserted in the system in the order that should appear at the time of publication.

5.2.2. *E-mail:* indication of the e-mail address of the author(s) for contact, which will mandatorily appear in the published version of the article.

5.2.3. *ORCID iD:* indication of the number of the author's ORCID identifier (for further information click here). The ORCID identifier can be obtained in ORCID register. Authors must have to accept the patterns for presentation of ORCID iD and include the full URL (e.g.: https://orcid.org/0000-0003-1781-1726).

5.2.4. *URL:* link to the author's full curriculum. In the case of Brazilian authors, the link to the Lattes Curriculum should be indicated.

5.2.5. *Affiliation:* indication of the author's main institutional affiliation (or two main affiliations if both of the links with them have the same importance). The main institution is where the author is professor or student, or, in case of not being professor or student anymore, the institution where the authors obtained their major academic title (PhD, J.S.D., LL.M, B.A., etc.). The institution's name must be written in full (not abbreviated) and in the original language of the institution (or in English for non-Latin languages), followed by an indication of the country of origin of the institution between parentheses. If the author is a professor and also a PhD, J.S.D or LL.M candidate in another institution, the main affiliation will be the institution where the author is candidate.
5.2.6. *Country:* indication of the country of the author's main institutional affiliation.
5.2.7. *Bio Statement:* indication of the author's abbreviated CV, with the information organized in the following sequence: first, the indication of the institution to which the author is affiliated as a professor; second, between parentheses, the city, state/province (if applicable) and country of the institution; third, indication of academic titles (starting with the highest); fourth, other bonds with scientific associations; fifth, profession; etc.
5.3. Title and Abstract
5.3.1. *Title:* title in the language of the article, with only the first letter of the sentence in capital letter.
5.3.2. *Abstract:* abstract in the language of the article, without paragraph or citations and references, with up to 200 words.
5.4. Indexing
5.4.1. *Keywords:* indication of 5 keywords in the language of the article (in lower case and separated by semicolons).
5.4.2. *Language:* indicate the acronym corresponding to the language of the article (Português=pt; English=en; Español=es).
5.5. *Supporting Agencies:* articles resulting from funded research projects should indicate in this field the source of funding.
5.6. *References:* insert the complete list of references cited in the article, with a space of one line between them.

6. Text Presentation and pre-textual elements
6.1. The article must have between 15 and 30 pages (size A4 – 21 cm × 29,7 cm), including introduction, development and conclusion (not necessarily with these titles) and a bibliographic reference list. The maximum number of pages can be relativized in exceptional cases, decided by the Editorial team.
6.2. Edges (margins) must be: top and left with 3 cm, bottom and right with 2 cm.
6.3. The text must use Font Times New Roman, size 12, line spacing 1.5, and spacing 0 pt before and after paragraphs.
6.4. References must use Font Times New Roman, size 10, simple space between lines.
6.5. In the development of the text, the paragraphs must contain decrease of 1.5 cm from the left margin. Titles and subtitles must be aligned with the left margin without decrease.
6.6. The structure should observe the following order:

6.6.1. Title in the article's language, in bold, centralized, with the first letter of the sentence in capital letter.
6.6.2. In case of indicating information related to the article (financing from sponsoring agencies, acknowledgments, translators, etc.), it is necessary to insert a footnote with an asterisk (not number) on the right side of the title in the article's language.
6.6.3. Title in English, with only the first letter in capital letter, in bold and in italic, centralized. In the case of articles written in English, this element must be substituted by the title in Portuguese.
6.6.4. The article must not include the names of the author(s). The information for publication purposes will be taken from the metadata entered by the author(s) in the journal's electronic system at the time of submission.
6.6.5. Abstract in the article's language (font Times New Roman, 12, simples lines, without paragraph or quotations and references, until 200 words), preceded by the word "Abstract" written in the article's language.
6.6.6. Indication of five keywords in the article's language (in lower case and separated by semicolon), preceded by the expression "Keywords" written in the article's language.
6.6.7. Abstract in English (font Times New Roman, 12, simples lines, without paragraph or quotations and references, up to 200 words), preceded by the word "Abstract". In case of articles written in English, this element must be replaced by the abstract ("*resumo*") in Portuguese.
6.6.8. Indication of five keywords in English (in lower case and separated by semicolon), preceded by the expression "Keywords". In case of articles written in English, this element must be replaced by keywords ("*palavras-chave*") in Portuguese.
6.6.9. Table of contents, indicating the titles of the sections and subsections, with progressive numbering in Arabic numbers.
6.6.10. Development of the scientific article: progressive numbering, in Arabic numbers, must be used to make clear the content's systematization.
6.6.11. Bibliographic references list must bring only sources that were really used, located in the end of the article, separated by a simple space, lined to the left margin (no indent).
6.6.12. For other aspects, apply Brazilian technical norms (ABNT NBR 10520:2002 e 14724:2011).
6.6.13. In the case of articles with 4 or more authors, it is necessary to include a footnote indicating the contribution of each one to the article.
6.7. Highlights must be made only in italics, meaning that bold, underlined or caps lock, cannot be used to highlight.
6.8. Images and boards must be inserted in the text, not in the end in form of attachments.

7. Scientific Methodology

7.1. The references of books, chapters in collective books, articles, theses, dissertations/essays, monographs of quoted authors used as base to write the text must be mentioned as a reference on the footnotes, with all the information about the text, according to the Brazilian technical norms (ABNT NBR 6023:2018 – summarized in the item 7.1.3 below), and especially, indicating the page of which the information written on the text was taken, right after the reference.

7.1.1. Book's title (or journal's title) must be highlighted in italics (bold shall not be used for that purpose).
7.1.2. Articles written in the format AUTHOR-YEAR will not be accepted for publishing.
7.1.3. References shall appear as follows:
7.1.3.1. Books:
LAST NAME, Name Middle Name. *Title of the book in italics:* subtitle not in italics. Number of the edition. City: Publisher, Year.
Example:
KEEN, Andrew. *Vertigem digital*: por que as redes sociais estão nos dividindo, diminuindo e desorientando. Trad. Alexandre Martins, Rio de Janeiro: Zahar, 2012. 254p.
7.1.3.2. Chapter in a collective book:
LAST NAME, Name Middle Name. Title of the Chapter not in bold. In: ORGANIZER'S LAST NAME, Name Middle Name; 2ND ORGANIZER'S LAST NAME, Name Middle Name, and so on, separated by semicolon (Org. or Coord.). *Title of the book in italics***:** subtitle not in Italics. Number of the edition. City: Publisher, Year. first page-last page [preceded by "p."].
Example:
DOTTA, Alexandre Godoy. Derechos de la Población LGBT+ en Brasil: Vulnerabilidad Social entre Avances y Retrocesos. In: BRAVO, Álvaro Sánches; CASIMIRO, Ligia Melo de; GABARDO, Emerson. (Org.). *Estado Social Y Derechos Fundamentales en Tiempos de Retroceso*. Sevilha: Ponto Rojo, 2019. p. 203-228.
7.1.3.3. Articles in journals:
LAST NAME, Name Middle Name. Title of the article not in bold. *Title of the journal in italics*, city, volume, number, first page-last page [preceded by "p."], months of publishing [abbreviated with the first three letters of the month followed by dot and separated by a slash]. Year.
Example:
GABARDO, Emerson; SAIKALI, Lucas Bossoni. A prescritibilidade da ação de ressarcimento ao erário em razão de atos de improbidade administrativa. *Revista Jurídica – Unicuritiba*, Curitiba, v. 1, p. 514-543, 2018.
7.1.3.4. Theses of Full Professor contests, Doctoral theses, Master's dissertations/ essays, Undergraduate and Graduate courses monographs:
LAST NAME, Name Middle Name. *Title in italics:* subtitle. City, year. number of pages followed by "f". Kind of the work (Degree obtained with the defense) – Department or Sector, Name of the institution.
Example:
SANTOS, Fábio de Sousa. *Análise Comparada da Competição na Contratação Pública Brasileira e Estadunidense*. Curitiba, 2018. 134f. Dissertação (Mestrado em Mestrado em Direito) – Pontifícia Universidade Católica do Paraná. Curitiba: 2018.
7.1.3.5. DOI – Digital object identifier: If the document consulted in the research has the DOI number, it is recommended to include, in a complementary way, the number after the end of each reference. Example:
DOTTA, Alexandre Godoy. Public policies for the assessment of quality of the Brazilian higher education system. *Revista de Investigações Constitucionais*, Curitiba, v. 3, p. 53-69, 2016. DOI. 10.5380/rinc.v3i3.49033.

7.1.3.6. Documents in electronic media: Documents extracted from electronic media must present after the end of each reference the location of the network where it was found and presented as follows. Example:
DIJDL. International Journal of Digital Law*. Regras para a submissão de artigos*. Disponível em: https://journal.nuped.com.br/index.php/revista/about/submissions. Acesso em: 12 fev. 2020.
7.1.4. The elements of references must observe the following model:
7.1.4.1. **Author:** LAST NAME in capital letters, comma, Name with the initials in capital letters, Middle Name with the initials in capital letters, followed by a dot.
7.1.4.2. Edition: the information must only be included after the second edition of the book, without ordinal, followed by a dot and "ed.". Example: 2. ed.
7.1.4.3. Year: it must be written with Arabic numerals, without dot in thousand, preceded by comma, and followed by a dot**.** Example: 1997.
7.1.5. In case of being impossible to find one of those elements, the absence must be resolved in the following manner:
7.1.5.1. Absence of city: replace for [S.l.].
7.1.5.2. Absence of publisher: replace for [s.n.].
7.1.5.3. Absence of year: the approximated year must be indicated between brackets, followed by a question mark. Example: [1998?].
7.2. The quotations (words, expressions, sentences) must be carefully reviewed by the authors and/or translators.
7.2.1. The direct quotations must follow this pattern: transcription until four lines should fit in the text body, with normal letter, normal spacing and quotation marks.
7.2.2. It is strongly recommended that long textual quotations (more than four lines) are not used. However, if indispensable, they shall constitute an independent paragraph, with 1,5 cm of decrease related to the left margin (justified alignment), with simple lines and font 10. In that situation, quotation marks must not be used.
7.2.3. It is forbidden the use of "op. cit.", "loc. cit.", "ibidem" and "idem" in the footnotes. The references in footnote must be complete and written out.
7.2.4. For the mention of authors in the text body, it is forbidden the use of capital letters (e.g. for Name LAST NAME...). In this case all mentions shall be written only with the first letter in capital letter (ex.: for Name Last Name...).

8. Composition
8.1. Apart from having an adequate scientific language for an editorial publication, the text must be reviewed.
8.2. In the case of articles written in Portuguese, the writing must obey the new orthographic rules in force since the promulgation of the Portuguese Language Orthographic Agreement, from January 1st, 2009.
8.3. Citations of texts that precede the Agreement must respect the original spelling.

9. Articles resulted from funded researches
Articles resulted from funded research projects shall indicate in a footnote, located at the end of the article title in the original language, the information related to the research financing.

10. Copyright statement

Authors who publish in this Journal have to agree to the following terms:

10.1. No copyright or any other remuneration for the publication of papers will be due.

10.2. Authors retain copyright and grant the International Journal of Digital Law the right of first publication with the article simultaneously licensed under the Creative Commons Attribution License, which allows sharing the work with recognition of its initial publication in this Journal. Moreover, because of their appearance in this open access Journal, articles are free to use, with proper attribution, in educational and non-commercial applications.

10.3. Authors are allowed and encouraged to post their work online (e.g. in institutional repositories or on their personal webpage) at any point before or during the submission process, as it can lead to productive exchanges, as well as increase the impact and citation of published work (see The Effect of Open Access).

11. Authors responsibilities

11.1. Authors are responsible for the published content, committing therefore to participate actively in the discussion of the results of their scientific research, as well as the review process and approval of the final version of the work.

11.2. Authors are responsible for the conducting all the scientific research, as well as its results and validity.

11.3. Authors should report the Journal about any conflict of interest.

11.4. Authors are fully and exclusively responsible for the opinions expressed in their articles.

11.5. When submitting the articles, authors recognize that all statements contained in the manuscript are true or based on research with reasonable accuracy.

12. Conflict of interest

The public confidence in the double-blind peer review process and the credibility of published articles depend in part on how conflicts of interest are managed during manuscript writing, peer review and decision making by the editors.

12.1. It is mandatory that the author of the manuscript declares the existence or not of conflicts of interest. Even thinking that there are no conflicts of interest, the author must declare this information in the article submission act, marking that field.

12.2. Conflicts of interest may appear when authors, reviewers or editors have interests that, apparently or not, may influence the development or evaluation of manuscripts.

12.3. When authors submit a manuscript, they are responsible for recognizing and revealing financial or other nature conflicts that may have influenced their work.

12.4. Authors must recognize all the financial support for the work and other financial or personal connections related to the research. The contributions of people who are mentioned in the acknowledgments for their assistance in the research must be described, and its consent to publication should be documented.

12.5. Manuscripts will not be simply dismissed because of a conflict of interest. A statement that there is or not a conflict of interest must be made.

12.6. The ad hoc reviewers must also reveal to editors any conflicts of interest that could influence their opinions about the manuscript and must declare themselves unqualified to review specific documents if they believe that this procedure is appropriate. In the

case of the authors, if there is silence from the peer reviewers about potential conflicts, it will mean that conflicts do not exist.

12.7. If a conflict of interest on the part of the peer reviewers is identified, the Editorial Board will send the manuscript to another ad hoc reviewer.

12.8. If the authors are not sure about what might constitute a potential conflict of interest, they should contact the Journal's Editor-in-Chief.

12.9. In cases in which members of the Editorial Team or some other member publish frequently in the Journal, it will not be given any special or different treatment. All submitted papers will be evaluated by double blind peer review procedure.

13. Other information

13.1. The articles will be selected by the Editor-in-Chief and the Editorial Board of the Journal, which will contact the respective authors to confirm the text reception, and then forward them to the two ad hoc reviewers' analysis.

13.2. The received and not published originals will not be given back.

13.3. Authors have the right to appeal of the editorial decisions.

13.3.1. They will be granted five (5) days from the date of the final decision of the Editorial Board to appeal.

13.3.2. The written appeal must be sent to the e-mail: <journal@nuped.com.br>.

13.3.3. The appeal will be examined by the Editorial Board within thirty (30) days

CONDITIONS FOR SUBMISSIONS

As part of the submission process, authors are required to check off their submission's compliance with all the following items, and submissions may be returned to authors that do not adhere to these guidelines.

1. The contribution is original and unpublished (except in the case of articles in a foreign language published abroad) and it is not being evaluated for publication by another Journal; otherwise, it must be justified in "Comments to the Editor."
2. The submission file is in Microsoft Word, OpenOffice or RTF.
3. URLs for the references have been informed when possible.
4. The text has between 15 and 30 pages (A4 size – 21 cm by 29.7 cm), including the introduction, development, conclusion (not necessarily with these titles) and a list of references; margins used are: left and top of 3 cm and right and bottom of 2 cm; the text is written in Times New Roman format, size 12, line spacing 1.5, and spacing 0 pt. before and after paragraphs; in the footnotes it was used Times New Roman, size 10, 1 pt. spacing; in the text development, paragraphs have an indent of 1.5 cm from the left margin; headings and subheadings are aligned on the left margin; figures and tables are inserted in the text, not in the end of the document as attachments.
5. The text respects the stylistic and bibliographic requirements outlined in the Author Guidelines, on the page About.
6. In case of submission to a section with peer review (e.g.: articles), the instructions available in Ensuring blind evaluation by peer reviewers have been followed.
7. The author states that, except for the direct and indirect quotations clearly indicated and referenced, the article is of his/her authorship and therefore does not contain plagiarism. And states that he/she is aware of the legal implications of the use of other authors material.

8. The author states that participated in the work enough to make public their responsibility for the content and that all statements contained in the manuscript are true or based on research with reasonable accuracy.
9. The author agrees with the liability policy defined in item 10. Authors responsibilities of the Author Guidelines.

PRIVACY STATEMENT

This journal is committed to ethics and quality in publication, following international patterns of scientific publication. We support standards of expected ethical behavior for all parties involved in publishing in our journal: the author, the journal editor, the peer reviewer and the publisher. We do not accept plagiarism or other unethical behavior. Thus, it follows the guidelines of the 2nd World Conference on Research Integrity, Singapore, July 22-24, 2010.

Duties of Editors

- **Publication decision:** The journal's editor is responsible for deciding which of the articles submitted to the journal should be published. The editor is guided by the policies of the journal's editorial board and constrained by such legal requirements as shall then be in force regarding libel, copyright infringement and plagiarism. The editor may consult with editorial board or reviewers in decision making.
- **Fair play:** The editor should evaluate manuscripts for their intellectual content without regard to race, gender, sexual orientation, religious belief, ethnic origin, citizenship, or political philosophy of the authors.
- **Confidentiality:** The editor and any editorial staff must not disclose any information about a submitted manuscript to anyone other than the corresponding author, reviewers, potential reviewers, other editorial advisers, and the publisher, as appropriate.
- **Disclosure and Conflicts of interest:** The editor must not use unpublished information in his/her own research without the express written consent of the author. The editor should recuse him/herself from considering manuscripts in which he/she has conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or (possibly) institutions connected to the papers.
- **Involvement and cooperation in investigations:** The editor should take reasonable responsive measures when ethical complaints have been presented concerning a submitted manuscript or published paper.

Duties of Reviewers

- **Contribution to Editorial Decision:** Peer review assists the editor in making editorial decisions and through the editorial communications with the author may also assist the author in improving the paper.
- **Promptness:** Any selected referee who feels unqualified to review the research reported in a manuscript or knows that its prompt review will be impossible should notify the editor and excuse himself from the review process.
- **Confidentiality:** Any manuscripts received for review must be treated as confidential documents. They must not be shown to or discussed with others.

- **Standards of Objectivity:** Reviews should be conducted objectively and referees should express their views clearly with supporting arguments.
- **Acknowledgement of Source:** Peer reviewers should identify relevant published work that has not been cited by the authors. The peer reviewer should also call to the editor's attention any substantial similarity or overlap between the manuscript under consideration and any other published paper of which they have personal knowledge.
- **Disclosure and Conflicts of Interest:** Privileged information or ideas obtained through peer review must be kept confidential and not used for personal advantage. Reviewers should not consider manuscripts in which they have conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or institutions connected to the papers.

Duties of Authors

- **Reporting standards:** Authors of reports of original research should present an accurate account of the work performed as well as an objective discussion of its significance. Underlying data should be represented accurately in the paper. A paper should contain sufficient detail and references to permit others to replicate the work. Fraudulent or knowingly inaccurate statements constitute unethical behavior and are unacceptable.
- **Originality and Plagiarism:** The authors should ensure that they have written entirely original works, and if the authors have used the work and/or words of others that this has been appropriately cited or quoted. Plagiarism in all its forms constitutes unethical publishing behavior and is unacceptable.
- **Multiple or Redundant Publication:** An author should not in general publish manuscripts describing essentially the same research in more than one journal or primary publication. To publish the same article in different journals without informing the editors and having their agreement constitute unethical publishing behavior and is unacceptable.
- **Acknowledgement of Sources:** Proper acknowledgment of the work of others must always be given. Authors should cite publications that have been influential in determining the nature of the reported work. Information obtained privately, as in conversation, correspondence, or discussion with third parties, must not be used or reported without explicit, written permission from the source. Information obtained in the course of confidential services, such as refereeing manuscripts or grant applications, must not be used without the explicit written permission of the author of the work involved in these services.
- **Authorship of the Paper:** Authorship should be limited to those who have made a significant contribution to the conception, design, execution, or interpretation of the reported study. All those who have made significant contributions should be listed as co-authors. Where there are others who have participated in certain substantive aspects of the research project, they should be acknowledged or listed as contributors. The corresponding author should ensure that all appropriate co-authors and no inappropriate co-authors are included on the paper, and that all co-authors have seen and approved the final version of the paper and have agreed to its submission for publication.

- **Disclosure and Conflicts of Interest:** All authors should disclose in their manuscript any financial or other substantive conflict of interest that might be construed to influence the results or interpretation of their manuscript. All sources of financial support for the project should be disclosed.
- **Fundamental errors in published works:** When an author discovers a significant error or inaccuracy in his/her own published work, it is the author's obligation to promptly notify the journal editor or publisher and cooperate with the editor to retract or correct the paper.

Duties of the Publisher

We are committed to ensuring that advertising, reprint or other commercial revenue has no impact or influence on editorial decisions.

Our articles are peer reviewed to ensure the quality of scientific publishing and we are also users of CrossCheck (CrossRef's plagiarism software).

* This statement is based on Elsevier recommendations and COPE's Best Practice Guidelines for Journal Editors.