

FÁBIO DA SILVA VEIGA
JOSÉ CAMPOS AMORIM
PATRÍCIA AZEVEDO
(COORDS.)

ÉTICA JURÍDICA NA ERA DIGITAL



IBEROJUR
INSTITUTO IBEROAMERICANO
DE ESTUDOS JURÍDICOS

P.PORTO
ISCAP

CEOS PP
CENTRO DE ESTUDOS ORGANIZACIONAIS
E SOCIAIS DO POLITÉCNICO DO PORTO

ÉTICA JURÍDICA NA ERA DIGITAL

Fábio da Silva Veiga
José Campos Amorim
Patrícia Anjos Azevedo
(Coordenadores)

Porto, 2022



IBEROJUR

P. PORTO
ISCAP

CEOS.PP
CENTRE FOR ORGANISATIONAL AND
SOCIAL STUDIES OF POLYTECHNIC OF PORTO

FCT Fundação
para a Ciência
e a Tecnologia

O editor não é responsável pelas opiniões, comentários e manifestações contidas nos textos dos respectivos autores. A presente obra expõe exclusivamente a opinião de cada autor como manifestação do seu direito à liberdade de expressão e ao padrão académico-científico definido pelo parâmetro de revisão do Comité Científico. O editor se opõe expressamente a qualquer das páginas desta obra ou partes da mesma nas quais sejam utilizados resumos ou textos jornalísticos. Qualquer forma de reprodução, distribuição, comunicação pública ou transformação desta obra só pode ser realizada mediante autorização de seus titulares, salvo exceção prevista na lei. Portanto, este livro não poderá ser reproduzido de forma integral sem a autorização prévia dos editores. Os autores dos capítulos ficam autorizados à reprodução e indexação na forma eletrónica sem fins comerciais, fazendo-se menção de que os respectivos textos pertencem à integralidade do livro, desde que citados o editor e demais informações da obra. Quaisquer outras formas de cessão do uso da obra, sem a autorização prévia, por escrito, dos titulares do copyright, são consideradas proibidas.

O procedimento de seleção de originais ajusta-se aos critérios específicos de investigação, no que se indica que as admissões dos trabalhos publicados respondem a critérios de qualidade equiparáveis aos exigidos pelas revistas científicas, nomeadamente avaliação double-blind review do Comité Científico composto por doutores em conformidade com a especialização da matéria.

Citação:

VEIGA, Fábio da Silva; AMORIM, José Campos; AZEVEDO, Patrícia Anjos. *Ética Jurídica na Era Digital*, Porto: Instituto Iberoamericano de Estudos Jurídicos e Instituto Superior de Contabilidade e Administração do Porto, 2022, 297 págs. ISBN: 978-989-53281-7-8

Ficha Técnica

© 2022 Instituto Iberoamericano de Estudos Jurídicos – IBEROJUR

Título: Ética Jurídica na Era Digital

Coordenadores: Fábio da Silva Veiga, José Campos Amorim e Patrícia Anjos Azevedo

Edição e Diagramação: Talita Corrêa Gomes Cardim

© [Autores vários]

Suporte: Eletrónico; Formato: PDF

ISBN: 978-989-53281-7-8

1ª edição: Instituto Iberoamericano de Estudos Jurídicos e Instituto Superior de Contabilidade e Administração do Porto

Rua de Aviló, 214, Matosinhos (Porto) - Portugal.

4460-282.

Abril, 2022

Depósito Legal - Biblioteca Nacional de Portugal

498148/22

Comité Científico

Antonio Tirso Sánchez (ULPGC, Espanha)

Beata Stępień-Załucka (University of Rzeszów, Poland)

Deolinda Meira (ISCAP/IPP)

Doglas Lucas (UNIJUÍ, Brasil)

Fábio da Silva Veiga (Universidade Lusófona do Porto)

José Campos Amorim (ISCAP/IPP)

Manuel Silva (ISCAP/IPP)

Manuela Patrício (ISCAP/IPP)

Mariusz Załucki (AFM Kraków University, Poland)

Patrícia Azevedo (ESTG/IPP)

Paulo Vasconcelos (ISCAP/IPP)

Sandrina Teixeira (ISCAP/IPP)

Wilson Engelmann (UNISINOS, Brasil)

Instituições Organizadoras

Instituto Iberoamericano de Estudos Jurídicos – IBEROJUR –
PORTUGAL

Instituto Superior de Contabilidade e Administração do Porto
(ISCAP) – através do seu Centro de investigação CEOS.PP

Apresentação

O livro debate analiticamente os principais assuntos que envolvem os problemas de ordem ética e jurídica relacionados com os mecanismos de Inteligência Artificial (IA), quer seja nas relações com a atividade humana ou com os sistemas automáticos ou autónomos de IA. Os diversos temas apresentados discorrem sobre os impactos que a IA causa direta ou indiretamente na vida das pessoas ou os riscos de abuso e violação dos direitos subjetivos.

Como objetivo final, discute-se os limites éticos do progresso económico em consequência da massiva digitalização das operações empresariais e das atividades públicas.

Porto, 4 de abril de 2022

Fábio da Silva Veiga
Professor ULP

José Campos Amorim
Professor ISCAP/IPP

Patrícia Anjos Azevedo
Professora ESTG/IPP

Coordenadores

Índice

O acesso a dados digitais como meio de obtenção de prova no processo penal brasileiro 12

Gabriela Soldano Garcez

Guilherme da Silva Freitas

Harmonização do direito de acesso à informação e de proteção de dados pessoais 27

Flávia Monaco Vieira

Judite Sanson de Bem

A evolução digital do direito notarial em Portugal – do presencial ao virtual 41

Patrícia Anjos Azevedo

Andreia Madalena Magalhães Jesus

As novas regras do IVA para o comércio eletrónico 55

José de Campos Amorim

GDPR tailored-made explanations in credit scoring must end 70

Diogo Morgado Rebelo

Biased algorithms: a risky violation of article 14 of the European Convention on Human Rights 87

Jacqueline Hellman

Democracia e liberdade de expressão na era digital: aplicação de restrições a canais de notícias virtuais como mecanismo de combate à polarização e à desinformação 100

Mariana Caroline Pereira Félix

Lucas Nogueira Holanda

Os riscos da inteligência artificial 115

Ana Isabel Guerra

Patrícia Anjos Azevedo

Direito de Manifestação e Cedência de Dados Pessoais 129

Mário Simões Barata

Jorge Barros Mendes

Entre a transparência e o controle nas Assembleias gerais virtuais em cooperativas 142

Leonardo Rafael de Souza

Cinthia Obladen de Almendra Freitas

Desafíos a la imputación de responsabilidad por ilícitos anticompetitivos cometidos en sistemas blockchain 157

Jesús A. Soto Pineda

Antonio J. Villanueva Tobalina

A utilização do blockchain como prova eletrônica do processo civil na Justiça Brasileira 170

Miguel Carlos Cristiano

O digital como prioridade da Comissão Europeia: breve análise sobre a transformação digital no âmbito da União Europeia 182

Dora Resende Alves

Ana Carolina Assumpção Stoffel

O uso da inteligência artificial e a possibilidade de eliminação dos vieses cognitivos na decisão jurídica 196

Thiago Henrique Reis de Araújo Costa

Marcelo Leandro Pereira Lopes

Inteligência artificial, economia comportamental e publicidade: uma união perigosa para o consumidor virtual 211

João Pedro Leite Barros

Débora Fernandes Maranhão

O uso de tecnologia de reconhecimento facial pelo poder público: necessidade de regulação específica em defesa da privacidade 225

Christiane Bedini Santorsula

Marcos Vinícius Sales dos Santos

Inteligência artificial como ferramenta auxiliar no processamento de execuções fiscais no Brasil: panorama e perspectivas 240

Marcos Vinicius Sales dos Santos

Vivian Leinz

Blockchain como mecanismo propulsor de conformidade tributária: panorama e perspectivas **254**

Carlos Alexandre Dias Torres

Christiane Bedini Santorsula

Os efeitos da pandemia de Covid-19 sobre a regulação do comércio internacional como estabelecida pela OMC **270**

Hérica Cristina Paes Nascimento

Maique Barbosa de Souza

A defesa do consumidor frente ao A.ISPLAINING **287**

Karlo Messa Vettorazzi

Julia de Mello Bottini

O acesso a dados digitais como meio de obtenção de prova no processo penal brasileiro

Access to digital data as a means of obtaining evidence in the brazilian criminal procedure

Gabriela Soldano Garcez¹

Guilherme da Silva Freitas²

Sumário: Introdução. 1. Ciberespaço e criminalidade; 2. Meio de prova e meio de obtenção de prova: uma distinção necessária; 2.1. Meio de obtenção de prova de dados digitais dinâmicos; 2.2. Meio de obtenção de prova de dados digitais estáticos; Conclusão. Referências Bibliográficas.

Resumo: O presente artigo busca apresentar, a partir da análise da transformação social implementada pelas novas tecnologias digitais, sobretudo àquelas oriundas da internet, que permitem que eventos locais produzam efeitos globais (em claro consonância com o conceito de globalização), de que modo a legislação brasileira reconhece e admite os modernos meios de obtenção de prova criminal. Para tanto, buscará analisar, primeiramente (através da adoção de método crítico-dedutivo realizado por meio de referencial bibliográfico sobre o tema, com base nacional e internacional), o ciberespaço como local de ocorrência de crimes (principalmente, no que se refere a uma nova sociedade complexa, plural e tecnológica, vivida atualmente, numa clara correlação com a Sociedade de Risco, conforme pregada por Ulrich Beck), mas também como local de realização de direitos fundamentais (tais como: vida privada e intimidade, uma vez que tais direitos passam a ter uma dimensão virtual ou digital, inclusive conforme nova dimensão de Direitos Humanos, qual seja, quinta dimensão). Após, buscará diferenciar os conceitos de “meio de prova” e “meio de obtenção de prova”, para que se possa concluir pela análise de tais referenciais em relação aos dados digitais, principalmente no que diz respeito aos dados digitais dinâmicos

1 Advogada; professora permanente do Programa de Pós-Graduação Stricto Sensu (mestrado e doutorado) da Universidade Católica de Santos. Pós-Doutora pela Universidade Santiago de Compostela/Espanha. Doutora em Direito Ambiental Internacional e Mestre em Direito Ambiental, ambas com bolsa CAPES, pela Universidade Católica de Santos. Email: gabrielasoldano@unisantos.br

2 Advogado. Mestrando em Direito Internacional, pela Universidade Católica de Santos. E-mail: guilherme.freitas@unisantos.br

e estáticos, tendo em vista a legislação brasileira atual sobre o tema.

Palavras-chave: Ciberespaço; Dados digitais; Provas digitais; Direito Fundamental.

Abstract: This article seeks to present, from the analysis of the social transformation implemented by new digital technologies, especially those coming from the internet, which allow local events to produce global effects (in clear consonance with the concept of globalization), how Brazilian legislation recognizes and acknowledges the modern means of obtaining criminal evidence. Therefore, it will seek to analyze, firstly (through the adoption of a critical-deductive method carried out through a bibliographical reference on the subject, with national and international basis), cyberspace as a place of occurrence of crimes (mainly, with regard to a new complex, plural and technological society, currently experienced, in a clear correlation with the Society of Risk, as preached by Ulrich Beck), but also as a place for the realization of fundamental rights (such as: private life and intimacy, since such rights they now have a virtual or digital dimension, even according to the new dimension of Human Rights, that is, the fifth dimension). Afterwards, it will seek to differentiate the concepts of “means of evidence” and “means of obtaining evidence”, so that it can be concluded by the analysis of such references in relation to digital data, especially with regard to dynamic and static digital data, having in view of the current Brazilian legislation on the subject.

Keywords: Cyberspace; Digital data; Digital proofs; Fundamental right.

Introdução

O alcance expressivo de novas tecnologias experimentadas por cada vez mais pessoas em todo o mundo tem ocasionado profundas transformações sociais, sobretudo nos modos de agir e interagir. Celulares, smartphones, smartwatches, notebooks, GPS, entre outros aparelhos eletrônicos, especialmente os que dispõem de tecnologia embarcada de conexão à internet, são hoje ferramentas indispensáveis para a comunicação e informação de parcela significativa da humanidade. Estas mesmas tecnologias também propiciam, mediante a profusão das redes sociais e a ampliação do acesso à rede, o exercício da liberdade de expressão e da própria democracia.

Dessa forma, é inegável que, ao “suprimir” distâncias, a internet promove igualdade e impulsiona o ensino, a cultura, o trabalho, entre outros direitos essenciais e considerados fundamentais. Portanto, em razão desse aspecto pluripotencial de promoção de direitos que hoje defende-se o acesso à internet como também um direito humano³. Não por acaso que, no Brasil, desde 2014, a legislação reconhece o acesso à internet como direito de todos⁴.

Conquanto se identifique esses aspectos benéficos, é preciso admitir que, por meio dessa mesma rede ações criminosas são planejadas, executadas, informadas ou, até mesmo, ocultadas em detrimento a outros direitos igualmente fundamentais.

A partir de tais considerações, o presente artigo analisa (através de referencial bibliográfico, com método crítico-dedutivo), primeiramente, a criação do ciberespaço como local de criminalidade, sendo imprescindível a atuação do Estado neste novo ambiente digital a fim de proteger os cidadãos, bem como de que forma tal atuação pode se dar, em virtude da existência pretérita de direitos fundamentais (como inviolabilidade de domicílio, vida privada e intimidade), que, até o momento, são tradicionalmente considerados tendo em vista ambientes físicos (e não digitais). Em seguida, analisa os significados de “meio de prova” e “meio de obtenção de prova”, tendo em mente a análise necessária de tais conceitos frente ao ambiente digital. Por fim, analisa os meios de obtenção de prova digitais dinâmicos e estáticos, frente a legislação brasileira atual.

1. Ciberespaço e criminalidade

O contato recíproco, instantâneo, próximo e frequente entre indivíduos, ou mesmo entre máquinas a serviço de indivíduos

3 Cf.: BACCIOTTI, J.K. Direitos humanos e novas tecnologias da informação e comunicação: o acesso à internet como direito humano. Dissertação (Mestrado). São Paulo: Pontifícia Universidade Católica de São Paulo, 2014.

4 Cf.: Art. 4º, inciso I, da Lei n. 12.965, de 23 de abril de 2014.

(conhecido como “internet das coisas”⁵), todos interligados numa mesma rede, possibilitou uma interação sem precedentes, desenvolvida em um novo ambiente artificial fruto da engenhosidade humana. É o chamado ciberespaço.

Aparentemente cunhado por William Gibson, em 1984, no livro de ficção científica “Neuromancer”⁶, o termo hoje tem sido assim compreendido:

O ciberespaço, assim como o entorno digital, retrata a interligação universal entre as redes de computadores para finalidades informacionais e comunicativas. Refere-se, porém, a algo mais, pois neste espaço viabiliza-se o contato entre pessoas permanentemente conectadas. Enquanto no entorno digital, os usuários interagem mediante o uso de aparelhos eletrônicos com finalidades comunicacionais e auto-informativas, no ciberespaço, pessoas ininterruptamente conectadas desenvolvem todas as atividades cotidianas.”⁷

Nesse sentido, Sombra enfatiza que:

Com a expansão de novos padrões de comportamento social em torno de valores e condutas a que se convencionou denominar cibercultura, uma vez que identificada pelas características da disrupção (rompimento de padrões), da convergência (direcionamento de funcionalidades) e da digitalização (transformação de informações em bits), um fórum dinâmico de interação entre indivíduos se emancipou, o ciberespaço. A riqueza desse processo de desenvolvimento de um nicho tecnológico de interação entre os indivíduos envolveu fatores de todas as grandezas e foi capaz de impactar quase todos os meandros da vida em sociedade, tal como até então não se conhecia.⁸

É evidente que, neste novo espaço humano, marcado pela interação massiva de indivíduos para o exercício de todas as atividades cotidianas e pelo fenômeno da digitalização (que nada

5 STEIBEL, Fabro; VICENTE, Victor F.; DE JESUS, Diego S. V. Possibilidades e potenciais da utilização da Inteligência Artificial. In: FRAZÃO Ana; MULHOLLAND, Caitlin. Inteligência artificial e Direito [livro eletrônico]: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019, RB-4.1.

6 Disponível em: <<https://super.abril.com.br/blog/turma-do-fundao/7-coisas-que-o-classico-cyberpunk-neuromancer-previu/>>. Acesso em: 02 ago. 2021.

7 GUARDIA, Gregório Edoardo Raphael Selinguardi. Meios de busca de provas e inovações tecnológicas: obtenção e tratamento de dados digitais no processo penal. São Paulo: Max Limonad, 2016. p. 46.

8 SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados pessoais. São Paulo: Thomson Reuters Brasil, 2019, p.2.

mais é do que a transformação de informações em bits), o ilícito penal, enquanto fato social, também se revela.

Ciente e antevendo esse aspecto, há mais de vinte anos, o Conselho da Europa, com a Convenção n.º 185, de 2001⁹, buscou traçar diretrizes aos signatários em matéria de direito penal material e processual penal, ao padronizar terminologias (tais como: “dados informáticos” e “dados de tráfego”) e dispor sobre a adoção comum de novos tipos penais, meios de obtenção de prova, competência e cooperação jurídica internacional.

No Brasil, também já se percebeu a essa nova realidade. Não por acaso o constituinte, no longínquo ano de 1988, utilizou a expressão genérica “dados”, no inciso XII do art. 5º, antevendo inovações tecnológicas futuras, ao dispor acerca da inviolabilidade das comunicações, mas excepcionando o sigilo para fins de obtenção de provas penais.

Isso ocorre porque, liberdade e segurança são valores normatizados como direitos fundamentais, decorrentes do art. 5º, caput, da Constituição brasileira Federal de 1988, e, por consequência, não se apresentam como direitos antagônicos. Ao contrário, são complementares, eis que necessitam coexistir para o fim de se contruir uma sociedade justa e fraterna (conforme fundamento do art. 3º, I, objetivo fundamental da República brasileira).

Assim, da liberdade individual, pilar democrático, escoram-se os direitos fundamentais à liberdade de pensamento e expressão (IV), intimidade, vida privada e imagem (X), inviolabilidade de domicílio e das comunicações (XI e XII) e não autoincriminação¹⁰ (LXIII). Entretanto, para a concretização de tais direitos, é necessário que o Estado atue de forma positiva no sentido de criar procedimentos adequados e estruturar órgãos de persecução penal eficientes que, ao mesmo tempo, promovam segurança pública e garantam a

9 Disponível em: <<https://rm.coe.int/16802fa428>>. Acesso em: 02 ago. 2021.

10 Trata-se do direito a não-autoincriminação. O princípio é expresso na Convenção Interamericana de Direitos Humanos, art. 8.2, “g”, norma considerada de estatura “supralegal” pelo Supremo Tribunal Federal.

liberdade e seus consectários¹¹.

Para tanto a construção do processo penal justo, por obediência a Constituição, deve levar em consideração tanto na definição do procedimento quanto da relação jurídica processual estabelecida no caso concreto, o respeito à liberdade individual do imputado, sem descuidar da defesa social. Daí, a importância de se estabelecer procedimentos e pressupostos normativos mínimos legitimadores da intervenção do Estado na esfera íntima e privada dos dados informatizados.

2. Meio de prova e meio de obtenção de prova: uma distinção necessária

A partir da constatação da interação massiva entre indivíduos proporcionada pela internet e do fenômeno da digitalização, é preciso reconhecer que o acesso a dados informáticos, também intitulados “dados digitais” pela doutrina brasileira¹² e pelos órgãos de persecução penal, representam valioso instrumento no combate à criminalidade.

Não só para a atividade probatória voltada à repressão dos “cibercrimes” (crimes cometidos no ciberespaço, como, por exemplo, o armazenamento e disponibilização em rede de pornografia infantil), mas, em todos os demais, na medida em que o simples uso de smartphones já é capaz de produzir dados digitais de interesse para a investigação criminal, tais como: dados de localização, troca de mensagens, áudios, sons e imagens, a denotar participação, coautoria, preparação, execução, consumação ou mesmo exaurimento, ocultação e proveito de crimes.

Diante dessa constatação urge distinguir “meio de obtenção

11 FERNANDES. Antonio Scarance. Reflexões sobre as noções de eficiência e de garantismo no processo penal. In: FERNANDES. Antonio S.; ALMEIDA, José R. G.; MORAES, Maurício Z. Sigilo no Processo Penal: eficiência e garantismo. São Paulo: Revista dos Tribunais, 2008.

12 GOMES FILHO, Antonio; TORON, Alberto Z.; BADARÓ, Gustavo H. Código de processo penal comentado [livro eletrônico]. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, RL-1.31.

de prova” ou “de investigação” ou “de pesquisa de prova” de “meio de prova”. “Meios de obtenção de prova” são procedimentos em geral extraprocessuais, regulados por lei e utilizados pelos órgãos de persecução penal, com o objetivo de obter fontes de prova e ou elementos de prova. Enquanto os “meios de prova” são instrumentos pelos quais se leva ao processo aqueles elementos de prova aptos a revelar ao juiz, diretamente, a verdade de um fato¹³.

Vale ressaltar que, apesar dessa distinção estar expressa em legislações processuais como a portuguesa e a italiana, bem como no atual Projeto de alteração do Código de Processo Penal (CPP) brasileiro (conforme PLS nº 156/2009), é ausente na Codificação brasileira processual vigente.

A diferenciação é indispensável pois o meio de prova será produzido sob o contraditório, no processo penal, perante e para a autoridade judicial. Já o meio de obtenção de prova, enquanto técnica especial de investigação, será desenvolvido de forma inquisitorial, pelo Estado-Investigação ou Estado-Acusação, em procedimento administrativo. Nesse último caso, limitar-se-á não só o contraditório, eis que a surpresa é a principal arma dos meios de investigação, mas outros direitos fundamentais como à inviolabilidade das comunicações, o domicílio, a vida privada e a intimidade.

Por isso, a produção de meio de prova atípica, ou seja, sem procedimento probatório previsto em lei, no processo penal, seria admitida pela aplicação do art. 3º do CPP (analogia), combinado com o art. 369¹⁴ do Código de Processo Civil (CPC). Mas, o mesmo não ocorre com o meio de pesquisa de prova atípico, que reclama lei em sentido estrito.

13 BADARÓ, Gustavo Henrique. *Processo Penal*. 6. ed. São Paulo: Thomson Reuters Brasil, 2020, RB-10.4.

14 “Art. 369. As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz”. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm>. Acesso em: 02 ago. 2021.

2.1. Meio de obtenção de prova de dados digitais dinâmicos

Não por acaso que a Constituição no art. 5º, inciso XII, anuncia que “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”, a tutelar a comunicação durante o processo de fluxo de dados, ao proibir o acesso não autorizado a ela enquanto perdurar o processo comunicativo. Todavia, o texto constitucional deixa claro que é possível, de modo excepcional, o acesso a comunicação pelos órgãos de persecução penal, a abranger a telefônica e a informatizada, desde que observada a cláusula de reserva jurisdicional, o procedimento legal estabelecido e a finalidade específica de “investigação criminal ou instrução processual penal”. Portanto, atendida tais premissas, é possível a interceptação, ou seja, a captação e o registro dos dados digitais em tempo real (dados dinâmicos, ou seja, em movimento, em tráfego via rede) realizada pelo Estado sem conhecimento e autorização dos interlocutores.

Com o objetivo de estabelecer o procedimento legal imposto pela Constituição, surge a Lei n. 9.296, de 24 de julho de 1996¹⁵, que deixa claro, logo no artigo 1º, que estabelecerá o procedimento penal aplicável para interceptação de comunicações telefônicas e de “fluxo de comunicações em sistemas de informática e telemática”. Assim, toda e qualquer investigação que necessita do acesso a dados digitais dinâmicos em sistema informático ou telemático para a elucidação da autoria e materialidade delitiva, encontra supedâneo nessa norma.

Também no art. 1º, a norma mencionada reafirma que a medida se sujeita a reserva jurisdicional, observada as regras de competência, bem como que é voltada apenas para fins penais (ou seja, para tutela dos bens jurídicos mais relevantes), sendo

15 Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 02 ago. 2021.

assegurado o segredo da medida, como mecanismo de assegurar a própria eficácia da diligência pretendida, enquanto o investigado não terá dados pessoais vazados.

Já no artigo 2º, dado o alto grau de mitigação aos direitos fundamentais, são estabelecidos requisitos, sendo eles a presença de indícios razoáveis de autoria ou participação em infração penal punível com pena de reclusão e a inexistência de outro meio menos gravoso para a obtenção do elemento ou fonte de prova.

Vale salientar que, recentemente alterada pela Lei nº 13.964, de 24 de dezembro de 2019¹⁶, a lei de interceptação de comunicações avançou, de modo a permitir a interceptação da comunicação entre presentes, ou seja, a que se desenvolve num mesmo ambiente, através de captação de sinais eletromagnéticos, ópticos ou acústicos (art. 8-A), a exigir autorização judicial apenas nos casos em que a captação seja realizada em ambientes privados.

Antes da norma disciplinar a interceptação de sinais entre presentes, a medida era largamente admitida pela prática forense, tendo por base o cumprimento dos mesmos requisitos da interceptação de dados. Com o advento da previsão expressa desse novo meio de obtenção de prova, reforça-se o entendimento pela necessidade de lei específica para estabelecer e disciplinar o procedimento restritivo de privacidade.

2.2. Meio de obtenção de prova de dados digitais estáticos

Encerrado o processo comunicativo, deixa-se de tutelar as comunicações em si e passa-se a perquirir acerca da proteção do próprio conteúdo do dado digital comunicado, já acabado, estático, podendo ser ele uma imagem, um vídeo, um som, um texto, entre outros. Essa proteção específica advém da inviolabilidade à intimidade e à vida privada (consagrados como direitos fundamentais, nos incisos X e XI, respectivamente, do

16 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm>. Acesso em: 02 ago. 2021.

artigo 5º, da Constituição Federal brasileira de 1988).

Curioso perceber que diferentemente da tutela da inviolabilidade das comunicações (inciso XII), o constituinte não previu no inciso X, de forma expressa, a restrição pela lei do direito fundamental. Isso não quer dizer, contudo, que há impossibilidade de fazê-lo, mas corrobora o entendimento pela necessidade de lei formal estabelecer o procedimento.

Em verdade, o inciso XI ao trazer proteção ao domicílio e suas exceções, complementa de significado o inciso X (inviolabilidade da vida privada e intimidade), devendo ser lidos conjuntamente. Isso porque o exercício da vida privada e da intimidade, na sociedade pré-informatizada, momento da promulgação da Constituição, se davam quase que exclusivamente no ambiente “casa”, expressão de significado mais amplo do que o conferido pelo Código Civil ao termo “residência” e “domicílio”, conforme já se manifestou o Supremo Tribunal Federal (STF), no Recurso Extraordinário nº 251.445/GO.

Naquele momento histórico, o ciberespaço não passava de ficção. Atualmente, como uma realidade, é preciso considerá-lo. Se não for possível emprestar o mesmo significado de “casa” ao ciberespaço, ao menos é imperioso reconhecê-lo como espaço em que são realizados o tráfego e armazenados dados digitais, reveladores de diversas relações privadas (decorrentes de atividades bancárias, fiscais, afetivas, amorosas etc.), que carecem de igual proteção, mas que também estarão sujeitas as restrições constitucionais em caso de flagrante delito ou por determinação judicial (conforme inciso XI).

No Brasil, a Lei n. 12.965, de 23 de abril de 2014¹⁷, que estabelece direitos e deveres para o uso da internet, no art. 22, prevê a possibilidade genérica de a autoridade judicial, devidamente provocada pela “parte interessada”, requisitar ao responsável pela guarda o fornecimento de “registro de conexão” ou “registro de

17 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 02 ago. 2021.

acesso a aplicações de internet”, “com o propósito de formar conjunto probatório em processo judicial cível ou penal”. Trata-se da cessão de dados digitais, outro meio de obtenção de prova.

Referida norma exige que o interessado, no caso a polícia ou o Ministério Público, demonstre fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória, e a delimitação do período ao qual se referem os registros pretendidos.

Sobre a cessão de dados digitais:

(...) prestadores de serviços na internet têm a incumbência de disponibilizar informações conservadas nos respectivos bancos de dados. Encaminhada a requisição judicial, será dirigida ao responsável pelo tratamento dos dados para a respectiva apresentação do conteúdo pretendido. A cessão também ocorrerá quando o próprio titular dos dados, mediante consentimento livre, inequívoco, específico e prévio, franquear o respectivo acesso. Os dados requisitados para a investigação criminal podem concernir à identidade do sujeito passivo da medida; identidade de terceiros envolvidos no processo comunicativo; serviços básicos utilizados; serviços suplementares; direção da comunicação; indicação da resposta; causas de finalização da comunicação; aspectos temporais da comunicação, informações de localização e informação intercambiada por meio do canal de controle.¹⁸

Por outro lado, como outro meio de investigação de dados digitais estáticos, há as chamadas “quebras” dos sigilos legalmente protegidos, como o financeiro ou bancário (regidos pela Lei Complementar n. 105/2001¹⁹), e o fiscal (conforme art. 198, do Código Tributário Nacional - CTN²⁰), passíveis de serem solicitados pelos órgãos de persecução penal ao juízo competente, sobretudo no combate aos crimes contra a Administração, lavagem de capitais, evasão de divisas, entre outros.

Por sua vez, o único meio de obtenção de prova disciplinado

18 GUARDIA, Gregório Edoardo Raphael Seligardi. A intervenção nas comunicações eletrônicas e o acesso a dados digitais armazenados em suporte eletrônico como meios de investigação no processo penal. In: Revista Fórum de ciências criminais. v. 3, n. 5, jan./jun., 2016, p. 79.

19 Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>. Acesso em: 02 ago. 2021.

20 Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm>. Acesso em: 02 ago. 2021.

pelo Código de Processo Penal (CPP) é o antigo procedimento de busca e a apreensão (arts. 240 a 250). Imaginado para objetos fisicamente palpáveis, torna-se útil para o acesso a dados digitais estáticos armazenados em meio físico (pen-drives, cartão de memória, CDs, DVDs, disco rígido, disco rígido externo, smartphones, notebooks etc.) fora da rede. Não obstante, tal medida restritiva deva ser subsidiária e bem fundamentada, eis que tolher, indefinidamente, o indivíduo de um smartphone ou notebook, nos tempos atuais, poderá importar séria mitigação de direitos, especialmente em face da possibilidade da cessão de dados digitais, técnica menos invasiva e igualmente eficaz²¹.

Por último, cite-se a possibilidade de infiltração de agente de polícia na internet, novo meio de obtenção de provas digitais criado pela Lei nº 13.964, de 24 de dezembro de 2019, como instrumento de combate à pedofilia e crimes perpetrados por organizações criminosas, que necessariamente pressupõem a colheita de dados digitais eis que, conforme a lei, “todos os atos eletrônicos praticados durante a operação deverão ser registrados, gravados, armazenados e encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado”²².

Dessa forma, pode-se concluir que:

(...) parece ser possível conceituar a prova digital como: o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo.²³

Sendo certo que, conforme a Resolução 59, de 2008, do Conselho Nacional de Justiça (CNJ), a informatização das

21 GUARDIA, Gregório Edoardo Raphael Seligardi. Op. cit.

22 Cf. Art. 10-D, da Lei nº. 12.850, de 2 de agosto de 2013 e mesma redação do art. 190-E, da Lei nº. 8.069, de 13 de julho de 1990.

23 THAMAY Renna; TAMER, Mauricio. Provas no Direito Digital: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020, RB-1.3.

rotinas procedimentais penais demanda “tempo, investimento e aparelhamento das instituições envolvidas”²⁴.

Conclusão

A partir da transformação social ocasionada pelas novas tecnologias, sobretudo a internet (onde o ciberespaço toma forma e permite o fenômeno da digitalização), a legislação brasileira, de forma esparsa e não sistematizada, reconhece e admite os modernos meios de obtenção de prova criminal, embora ausente a padronização terminológica necessária para conferir unidade normativa e balizas seguras para os intérpretes. Sendo certo que, o Estado não pode prescindir desse novo ambiente para auxiliar à repressão de infrações penais, eis que grande parte da convivência humana tem sido realizada neste ambiente (principalmente, em tempos de pandemia da covid-19). Entretanto, por acarretar necessariamente na mitigação de direitos fundamentais, a atuação legislativa torna-se função essencial, frente a necessidade de previsão procedimental do meio de obtenção de prova (digital) em lei formal.

Acrescente-se que a autointitulada Lei Geral de Proteção de Dados Pessoais (nº 13.709/2018²⁵), deixou de fora sua aplicabilidade para o tratamento de dados pessoais utilizados para fins de segurança pública, investigação e repressão de infrações penais.

Assim, aceitar que disposições normativas possuam certo grau de abertura para conceber novos meios tecnológicos de obtenção de prova é possível, mas a ausência de uma sistematização geral no CPP, principalmente no que se refere ao acesso à dados digitais, é ponto crítico que merece a reflexão dos operadores do Direito.

24 Disponível em: <<https://atos.cnj.jus.br/atos/detalhar/101>>. Acesso em: 02 ago. 2021.

25 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 02 ago. 2021.

Referências Bibliográficas

BACCIOTTI, Karina Joelma. Direitos humanos e novas tecnologias da informação e comunicação: o acesso à internet como direito humano. Dissertação (Mestrado). São Paulo: Pontifícia Universidade Católica de São Paulo, 2014.

BADARÓ, Gustavo Henrique. Processo Penal. São Paulo: Thomson Reuters Brasil, 2020.

FERNANDES. Antonio Scarance. Reflexões sobre as noções de eficiência e de garantismo no processo penal. In: FERNANDES. Antonio S.; ALMEIDA, José R. G.; MORAES, Maurício Z. Sigilo no Processo Penal: eficiência e garantismo. São Paulo: Revista dos Tribunais, 2008.

GOMES FILHO, Antonio; TORON, Alberto Z.; BADARÓ, Gustavo H. Código de processo penal comentado [livro eletrônico]. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, RL-1.31.

GUARDIA, Gregório Edoardo Raphael Selinguardi. Meios de busca de provas e inovações tecnológicas: obtenção e tratamento de dados digitais no processo penal. São Paulo: Max Limonad, 2016.

_____. A intervenção nas comunicações eletrônicas e o acesso a dados digitais armazenados em suporte eletrônico como meios de investigação no processo penal. In: Revista Fórum de ciências criminais. v. 3, n. 5, jan./jun., 2016.

SAAD, Marta et al. In GOMES FILHO, Antonio; TORON, Alberto Z.; BADARÓ, Gustavo H. Código de processo penal comentado [livro eletrônico]. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados pessoais. São Paulo: Thomson Reuters Brasil, 2019.

STEIBEL, Fabro; VICENTE, Víctor F.; DE JESUS, Diego S. V. Possibilidades e potenciais da utilização da Inteligência Artificial. In FRAZÃO Ana; MULHOLLAND, Caitlin. Inteligência artificial e Direito [livro eletrônico]: ética, regulação e responsabilidade. São

Paulo: Thomson Reuters Brasil, 2019.

THAMAY Renna; TAMER, Mauricio. Provas no Direito Digital: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020.

Harmonização do direito de acesso à informação e de proteção de dados pessoais

Harmonization of the right of access to information and personal data protection

Flávia Monaco Vieira¹

Judite Sanson de Bem²

Sumário: 1. A tecnologia e a sociedade; 2. A Lei de Acesso à Informação (LAI); 3. A Lei Geral de Proteção de Dados Pessoais (LGPD); 4. Harmonização do direito de acesso à informação e de proteção de dados; Considerações Finais.

Resumo: A sociedade, em geral, foi afetada pelas novas tecnologias da informação. Uma delas foi à relação entre o cidadão e a Administração Pública, que permitiu a aproximação, sobretudo devido ao surgimento de um governo aberto e à transparência dos dados públicos. Não obstante, os avanços tecnológicos favoreceram o surgimento de programas de processamento automático de dados, o que gerou problemas éticos quanto à coleta, o uso e disposição desses dados. O objetivo do trabalho é discutir a necessidade de harmonizar o direito de proteção de dados pessoais e o acesso à informação pública, a fim de promover um Estado democrático. Para tanto, foi realizada uma pesquisa teórica por meio da análise de referências bibliográficas referente ao assunto, especialmente sobre as características da Lei de Acesso à Informação e da Lei de Proteção de Dados Pessoais. As duas leis se complementam, incluindo conceitos relacionados, e favorecem a construção de uma sociedade democrática, fundamentada na transparência e no sigilo de dados pessoais. No entanto, às vezes são verificados pontos conflitantes, como a ausência de dispositivo legal sobre a confidencialidade dos dados estatísticos e políticas de preservação da privacidade individual. Para a harmonização destes direitos é necessário definir mecanismos na defesa de cada um sem que haja a preferência de uma lei em detrimento a outra.

1 Contadora e Perita Contábil Judicial. Mestre em Avaliação de Impactos Ambientais pela Universidade La Salle. E-mail: flavia.201910304@unilasalle.edu.br

2 Professora Dr^a do Programa de Pós Graduação em Memória Social e Bens Culturais da Universidade La Salle. Pós-doutorado em Geografia da Universidade Federal do Rio Grande do Sul, Doutora em História Ibero Americana pela Pontifícia Universidade Católica do Rio Grande do Sul, Mestre em Economia pela Universidade Federal do Rio Grande do Sul. E-mail: Judite.bem@unilasalle.edu.br

Palavras-chave: Proteção de dados pessoais; Sigilo; Acesso à Informação; Transparência; Democracia.

Abstract: Society in general has been affected by new information technologies. One of them was the relationship between the citizen and the Public Administration, which allowed the approximation, mainly due to the emergence of an open government and the transparency of public data. However, technological advances favored the emergence of automatic data processing programs, which generated ethical problems regarding the collection, use and disposal of these data. The objective of the work is to discuss the need to harmonize the right to protection of personal data and access to public information, in order to promote a democratic State. For this purpose, a theoretical research was carried out through the analysis of bibliographical references on the subject, especially on the characteristics of the Law on Access to Information and the Law for the Protection of Personal Data. The two laws complement each other, including related concepts, and favor the construction of a democratic society, based on transparency and confidentiality of personal data. However, conflicting points are sometimes verified, such as the absence of a legal provision on the confidentiality of statistical data and policies to preserve individual privacy. For the harmonization of these rights it is necessary to define mechanisms in defense of each one without the preference of one law over another.

Keywords: Protection of personal data; Secrecy; Access to information; Transparency; Democracy.

1. A tecnologia e a sociedade

O avanço das novas tecnologias trouxe mudanças significativas para a sociedade e impactou as relações humanas e organizações, seja devido à quebra de barreiras do tempo ou de limitações geográficas. Além disso, facilitou que um grande fluxo de dados e informações fosse disponibilizado no ambiente virtual, sendo necessária “regulamentação tanto no campo ético, como no que se refere ao uso e ao tratamento dos dados pessoais e particulares, em ambientes privados e públicos” (GARNIER, PADILHA, 2019).

Na busca desta regulamentação, houve a promulgação da Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de

Proteção de Dados Pessoais (LGPD), considerada um marco legal brasileiro de tanto para as instituições privadas como as públicas (PINHEIRO, 2020). A LGPD estabelece regras para o uso de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Não obstante, em 2011 foi estabelecida no Brasil a Lei nº 12.527, denominada Lei de Acesso à Informação (LAI), que especifica a transparência como regra, e o sigilo como exceção, nos casos expressamente previstos nela. Carvalho et al. (2019) a consideram como a lei brasileira mais abrangente em significância sobre transparência.

Neste contexto, observa-se que a legislação brasileira visa garantir dois princípios básicos para a democracia: a transparência na Administração Pública e o sigilo dos dados. Para Carvalho e Cabral (2019, p. 53) estes dois valores têm a mesma magnitude e “devem ser vistos em suas especificidades e garantidos na medida das funções que cada um deles cumpre para preservação da democracia e do Estado de Direito”.

Partindo destas premissas, o presente trabalho tem como objetivo discutir a necessidade de harmonizar o direito de proteção de dados pessoais e o acesso à informação pública, a fim de promover um Estado democrático. Para atingir o objetivo, este trabalho foi dividido em cinco partes, sendo esta introdução à primeira. A segunda parte discorre sobre aspectos da Lei de Acesso a Informação, seguido da Lei Geral de Proteção de Dados Pessoais (terceira parte), a quarta parte apresenta alguns pontos conflitantes de ambas as leis e a necessidade de harmoniza-las para a garantia da transparência da Administração Pública e o sigilo de dados pessoais dos cidadãos. A conclusão do estudo está contemplada na quinta parte.

A importância do tema reside na tensão existente entre os dois direitos, não havendo uma solução pré-definida, mas sim a

necessidade de julgamento e ponderação nos casos concretos em que ocorre (BENTO, 2020).

2. A Lei de Acesso à Informação (LAI)

A transparência dos atos do governo é um importante instrumento da democracia moderna, fundada na participação social (CARVALHO; CABRAL, 2019). Nesse sentido, a Lei nº 12.527, de 18 de novembro de 2011, conhecida como a Lei de Acesso à Informação (LAI) representa um importante avanço na consolidação de um Estado participativo, no qual o sigilo da relação do Estado com a sociedade é substituído pela transparência, por meio de estabelecimentos de regras e procedimentos específicos para o sigilo.

O acesso à informação pode ser compreendido como um direito humano fundamental, por ser condição necessária ao exercício competente da liberdade de expressão e da cidadania em um sistema político democrático (BENTO, 2020). Além disso, o acesso à informação pública tem como premissa a obrigação das autoridades públicas de prestar contas de suas ações a seus representados (accountability), permitindo a responsabilização dos gestores públicos pelos resultados entregues à sociedade.

De acordo com Carvalho e Cabral (2019, p. 50) “[...] o Brasil é um país cuja tradição democrática é muito recente e frágil [...]”, onde se percebe uma cultura de centralização e de sigilo de informações públicas, inclusive aquelas de interesse coletivo e consideradas fundamentais para a construção de formas ativas de cidadania. A vista disso, o acesso à informação se torna um instrumento de combate à corrupção, já que permite o monitoramento das decisões políticas e administrativas, inibindo o desvio de poder para benefício de grupos privados (BENTO, 2020).

Queiroz e Motta (2017) ressaltam que o avanço da tecnologia, com o acesso a internet e serviços on-line, possibilita que países

utilizem novas ferramentas que contribuam para a participação dos cidadãos e a consequente transparência.

De acordo com Oliveira (2021, p.39),

Tendo como norte hermenêutico e axiológico o direito fundamental, assegurado a todos, de acesso à informação pública de interesse particular, coletivo ou geral, a Lei de Acesso à Informação visa à participação do administrado na Administração Pública, em respeito ao axioma democrático de que esta pertence e se subordina ao povo.

Os procedimentos previstos na LAI devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes: observância da publicidade como preceito geral e do sigilo como exceção; divulgação de informações de interesse público, independentemente de solicitações; utilização de meios de comunicação viabilizados pela tecnologia da informação; fomento ao desenvolvimento da cultura de transparência na administração pública; e desenvolvimento do controle social da administração pública (BRASIL, 2011).

A Lei nº 12.527 prevê em seu art. 6º que cabe aos órgãos públicos, observadas as normas e procedimentos específicos aplicáveis, assegurar a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. A informação sigilosa é definida como informações submetidas temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, enquanto que a informação pessoal é compreendida como qualquer informação relacionada à pessoa natural identificada ou identificável (BRASIL, 2011).

Quanto às informações pessoais, a LAI dispõe que o tratamento destas informações deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. Além disso, essas informações pessoais terão seu acesso restrito pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem;

e poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem (BRASIL, 2011).

Assim como ocorre com informações sigilosas, as informações pessoais tratadas pela Administração Pública são restritas, configurando exceção à regra de transparência da informação. Contudo, diferentemente daquelas que, ainda que estejam restritas por tempo determinado, são públicas, estas, relacionadas com a pessoa natural identificada ou identificável, não têm natureza pública, pertencendo tão somente à pessoa a que se vinculam. Por dizerem respeito à intimidade, à vida privada, à honra e à imagem da pessoa, além de respeito aos direitos de liberdade e às garantias do indivíduo, as informações pessoais não são um bem público nem concerne a interesse público, e, portanto, não são abarcadas pelos mecanismos de transparência ativa e passiva³ da Administração Pública, tampouco necessitam de ser classificadas como sigilosas para serem restritas (OLIVEIRA, 2021).

Ramos (2016) descreve que a preocupação exposta pela LAI, referente aos dados pessoais, visa atender ao preceito estabelecido na Constituição Federal de 1988, que, no Artigo 5º, inciso X, afirma “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Apesar da consagração constitucional do direito à informação como um direito fundamental, Ramos (2016) aponta que, por vezes, os dados públicos podem estar em conflito com bens constitucionalmente protegidos (segurança interna e externa, investigação criminal e intimidade das pessoas). Nesse sentido, “[...] não se pode negar que a proteção de dados e informações

3 A transparência ativa refere-se à divulgação de dados sem solicitação prévia dos mesmos, por meio da internet, tendo como responsáveis pela divulgação as instituições públicas. A transparência passiva, por sua vez, é realizada por meio do Serviço de Informação ao Cidadão (SIC), mantido por cada entidade, e a resposta ao cidadão pode ser realizada pessoalmente ou por correspondência (QUEIOZ; MOTTA, 2019).

personais é também um importante valor para as democracias modernas e se torna uma questão ainda mais sensível quando se fala de uma ‘Sociedade da Informação’” (CARVALHO e CABRAL, 2019, p. 52-53).

Ainda nesse contexto, Ramos (2016, p. 82), descreve que “[...] no Estado Democrático de Direito, o Poder Público não é o detentor do interesse público, e sim seu guardião: o interesse continua sendo de titularidade do cidadão e do povo”. Ante o exposto, a transparência deve ser tratada como um direito fundamental do cidadão-administrado, e não como um dever da administração pública para a consecução de um interesse público abstrato e satisfatório apenas dos interesses desta.

3. A Lei Geral de Proteção de Dados Pessoais (PGDP)

Reconhecendo que a Administração Pública depende de dados para exercer suas atividades na manutenção da coisa pública, é natural a evolução para uma estatal mais tecnológica, que culmina na expansão de um direito administrativo eletrônico, pautado em bancos de dados eletrônicos, Big Data e computação em nuvem (OLIVEIRA, 2021).

Inicialmente a legislação brasileira promulgou a Lei nº 12.965, de 23 de abril de 2014, denominada Marco Civil da Internet, que estabelecia princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Apesar da referida lei dispor sobre a proteção de dados pessoais em seu conteúdo, a forma que essa proteção era apresentada ainda era tímida, configurando a necessidade de uma legislação que estabelecesse condições específicas para a proteção de dados pessoais (BARROS et al., 2019). Assim, a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD) foi instituída, especificando o aspecto de privacidade e dados pessoais, nos meios físicos e digitais (CARVALHO et al., 2019).

De acordo com Pinheiro (2020, p. 15), a LGPD é “[...] uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas”. A normativa evoca problemas éticos associados com questões de humanidades digitais de impacto social, como Direito à Explicação, Direito à Autodeterminação Informativa, Direito ao Esquecimento, surveillance e Direito à Intimidade (CARVALHO et al., 2019).

A LGPD é fundamental para superar inseguranças jurídicas e garantir as devidas proteções à população. O capítulo IV da Lei de Proteção de Dados Pessoais é destinado exclusivamente ao tratamento de dados pessoais pelo setor público, que ressalta a importância desse tema “visto que a administração pública é custodiante de muitos dados pessoais dos cidadãos e sua proteção ou tratamento de dados de maneira equivocada pode trazer sérios prejuízos à intimidade e à vida privada das pessoas” (CHAVES, 2021, p. 2).

A Administração Pública, devido à sua natureza e finalidade, detém inúmeros dados de seus cidadãos, tais como à situação fiscal, nível de escolaridade, utilização de serviços de saúde e viagens ao exterior. O direito à proteção de dados pessoais engloba inclusive os dados triviais do indivíduo, ou seja, aqueles não enquadrados na categoria de dados sensíveis (origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dado genético, entre outros).

Diferente da LAI que abrange apenas organizações públicas, a LGPD inclui as privadas. No artigo 2º, II da LGPD é exposto o fundamento da autodeterminação informativa, ou seja, o titular pode permitir a agentes de tratamento o uso de seus dados pessoais livremente, destes que estes usos estejam transparentes ao mesmo (CARVALHO et al., 2019).

A LGPD confere autonomia ao cidadão no consentimento de seus dados, assim sendo, na ausência do consentimento expresso,

as instituições não estarão autorizadas a coletar, usar ou tratar os dados dos usuários, salvo nas hipóteses de exceção previstas na própria lei. Além disso, o cidadão tem o direito de saber clara e especificamente quais os objetivos da coleta e do uso de seus dados, e possui o direito de pedir a eliminação dos dados, ou seja, revogar o consentimento anteriormente outorgado, devendo a empresa coletora deletar os dados do usuário de seus cadastros (GARNIER; PADILHA, 2019).

4. Harmonização do direito de acesso à informação e de proteção de dados

A democracia é um regime de governo no qual o cidadão participa ativamente das decisões políticas, por meio do sufrágio universal. O uso das tecnologias de informação (por exemplo: governo aberto) pode fortalecer esse regime político, uma vez que proporciona a aproximação do cidadão comum com as diversas esferas de governo (QUEIROZ; MOTTA, 2017).

No entanto, o crescente avanço tecnológico na Administração Pública e o surgimento de programas de tratamento automatizado de dados em grande escala trouxeram à tona dúvidas quanto ao limite ético e normativo de coleta, uso, disposição, venda etc. de dados da pessoa natural (OLIVEIRA, 2021).

Se por um lado, a transparência tem sua importância para o desenvolvimento de uma sociedade democrática, não podendo utilizar como desculpa a proteção de dados pessoais para frustrar este desenvolvimento, por outro lado, deve-se considerar a magnitude da coleta, circulação e processamento de dados pessoais, que permitem que instituições públicas e privadas usem os dados dos cidadãos em uma escala sem precedentes no desempenho de suas atividades (BENTO, 2020). Deste modo, compreender e estabelecer a relação entre transparência e proteção de dados é essencial, segundo Bento (2020, p. 193), por

tratar-se, “[...] então, de não dar caráter absoluto a nenhum desses dois direitos, mas de harmonizá-los, para que o Estado possa ser transparente sem que os indivíduos o sejam”.

Corroborado por Carvalho (2021, p. 80), apesar das leis se complementarem, existem pontos de contradição entre a LGPD e a LAI (tal como: ausência de dispositivo legal sobre o sigilo de dados estatísticos)⁴, “[...] os quais somente serão superados pelo aplicador das normas, ao partir do plano abstrato do deve-ser para o plano concreto do ser, se realizada interpretação sistemática e teológica conjunta desses diplomas”.

Na busca da harmonização dos direitos de acesso à informação e da proteção de dados pessoais, Bento (2020) descreve que se deve considerar a cultura da sociedade e das instituições sobre os problemas vividos em cada país.

Nos países em desenvolvimento, com um histórico de corrupção e secretismo, é provável que se atribua um peso maior à transparência e ao acesso a informações, ao passo que os cidadãos de países desenvolvidos, particularmente afetados pelos avanços tecnológicos de coleta e processamento massivo de dados, tendem a ser mais sensíveis a considerações de privacidade e reivindicam um maior controle sobre seus próprios dados (Bento, 2020, p. 193).

Queiroz e Motta (2019) aos analisarem documentos oficiais e extraoficiais, constataram o uso de métodos ineficazes para a preservação da privacidade individual. Deste modo, os autores recomendam que seja estabelecida uma política para preservação de privacidade individual, a ser executada por órgãos públicos em colaboração com setores da sociedade interessados no tema, além da realização das ações já previstas na LAI.

Barros et al. (2019) verificam que os dados pessoais registrados

4 Carvalho (2021) disserta sobre as pesquisas estatísticas, onde qualquer pessoa tem o dever de prestar as informações solicitadas, o que conduz à quebra obrigatória da privacidade, para o fim de atender aos interesses da coletividade. Nesse caso, “[...] o Estado pode constranger os indivíduos para despersuadi-los de se negarem a revelar-se” (CARVALHO, 2021, p. 55). Devido a ausência de normativa sobre o sigilo de dados estatísticos, os órgãos oficiais de produção de estatísticas se deparam com pedidos e requisições de acesso a esses dados.

em documentos de arquivo de caráter público se encontram em um dito “limbo” legislativo para o operador de tratamento destes dados, isso porque as leis que versam sobre este tema possuem pontos de encontro e desencontro, abrindo espaço para um dúvida entendimento entre o direito de acesso aos documentos públicos e o direito à privacidade da pessoa sobre a qual os dados registrados em documentos públicos se referem.

Cabe salientar que ambas as Leis desempenham papéis complementares em uma sociedade democrática e buscam assegurar o *accountability*. No entanto, a necessidade de salvaguardar ambos os direitos pode gerar conflitos, especificamente quando se solicitam informações que contêm dados pessoais de terceiros. Entre os solicitantes, destacam-se jornalistas investigativos, grupos da sociedade civil que atuam no combate à corrupção, acadêmicos e todo cidadão que exige saber por que determinada decisão foi tomada (BENTO, 2020).

Nesse sentido, Venturini (2016) aponta a necessidade de esforços coordenados para a construção de políticas amplas de gestão da informação, que permitam o acesso à informação e transparência, assim como a proteção de dados pessoais. Bento (2020) descreve algumas boas práticas na harmonização destes direitos, tais como definir previamente critérios interpretativos e de ponderação, de acordo com a categoria de dados pessoais tratados, bem como o estabelecimento de um mecanismo de coordenação institucional obrigatório para as autoridades encarregada da promoção e defesa de cada um dos direitos.

5. Considerações Finais

O avanço da tecnologia pode contribuir para que novas ferramentas sejam utilizadas pelo Estado, que por sua vez pode favorecer a transparência, além da participação e o controle social. Não obstante, essas tecnologias também possibilitam que

grandes fluxos de dados sejam coletados e processados, surgindo à necessidade de mecanismos que protejam os dados pessoais.

Nesse sentido, duas Leis brasileiras se tornam fundamentais e complementarem: a Lei de Acesso a Informação e a Lei Geral de Proteção de Dados Pessoais. Enquanto que o acesso à informação é essencial para garantir o princípio da transparência na Administração Pública, considerado um instrumento de combate à corrupção, uma parte significativa dos documentos e informações solicitadas no exercício desse direito é permeada por dados pessoais, cuja proteção também é considerada um direito fundamental.

Deste modo, é necessário haver a harmonização das leis, seja por meio de políticas de gestão de informação ou por definição de critérios prévios interpretativos de dados pessoais tratados. Por fim, pode-se considerar que com a aplicação e o amadurecimento das normas, novas questões tendem a emergir, o que poderá, por sua vez, influenciar novos dispositivos legais.

Referências Bibliográficas

BARROS, Gabriel da Silva; SILVA, Lorena dos Santos; SCHMIDT, Clarissa. Documentos públicos e dados pessoais: o acesso sob a ótica da Lei Geral de Proteção de Dados Pessoais e da Lei de Acesso à Informação. Arquivo Público do Estado de São Paulo, Ano V, n. 9, p. 22-39, 2019.

BENTO, Leonardo Valles. Critérios de ponderação entre o direito de acesso a informações públicas e o direito à proteção de dados pessoais: lições a partir do modelo espanhol. Revista da CGU, v. 12, n. 22, p.184-195, 2020.

BRASIL. Constituição da República Federativa do Brasil: texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nos 1 a 6/94, pelas Emendas Constitucionais nos 1/92 a 91/2016 e pelo Decreto Legislativo no 186/2008. Brasília: Senado

Federal, Coordenação de Edições Técnicas, 2016. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 20 ago. 2021.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 20 ago. 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 ago. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil, Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20 ago. 2021.

CARVALHO, Luiz Paulo; Oliveira, Jonice; CAPPELLI, Claudia; MAJER, Violeta. Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais. Anais do VII Workshop de Transparência em Sistemas. Sociedade Brasileira de Computação, VII, 2019. Porto Alegre, 2019.

CARVALHO, Mariana Martins de; CABRAL, Rodolfo de Carvalho. Dilemas entre transparência e proteção de dados: as requisições dos órgãos de controle e o sigilo estatístico. Revista Esferas, n.14, p. 49-60, 2019.

CHAVES, Joe Luis de Souza. O impacto da Lei Geral de Proteção de Dados (LGPD) nas investigações administrativas. Revista Caderno

Virtual, v. 1, n. 50, 2021.

GARNIER, Cíntia Miele; PADILHA, Tamyris Michele. Ética, privacidade e novas tecnologias: o impacto da lei de proteção de dados na sociedade. In: Migalhas, 2019. Disponível em: <https://www.migalhas.com.br/depeso/311142/etica--privacidade-e-novas-tecnologias--o-impacto-da-lei-de-protecao-de-dados-na-sociedade>. Acesso em: 20 ago. 2021.

OLIVEIRA, Vinícius da Silva. Lei Geral de proteção de dados pessoais e administração pública: aplicação da norma. Monografia (Bacharel em Direito) – Universidade do Sul de Santa Catarina – Unisul, 2021.

PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). 2. ed., São Paulo: Saraiva Educação, 2020.

QUEIRO.Z, Maria Jane de; MOTTA, Gustavo Henrique Matos Bezerra. Transparência e preservação de privacidade em dados governamentais no Brasil: pesquisa documental e estudo de caso. Planejamento e políticas públicas, n. 49, p.431-468, 2019.

RAMOS, Alexandra Lemos. O princípio da administração aberta versus o princípio da proteção dos dados pessoais. Dissertação (Mestrado em Direito Administrativo) – Universidade de Lisboa, 2016.

VENTURINI, Jamila. Da privacidade à transparência: desafios da interação entre agentes públicos e privados na gestão de informações pessoais. Revista Eletrônica de Comunicação, Informação & Inovação em Saúde, v. 10, n. 4, p. 1-6, 2016.

A evolução digital do direito notarial em Portugal – do presencial ao virtual

The digital evolution of Notarial Law in Portugal - From presential to virtual

Patrícia Anjos Azevedo¹

Andreia Madalena Magalhães Jesus²

Sumário: 1. O Direito na Sociedade Digital. A proteção dos dados pessoais. A Carta Portuguesa de Direitos Humanos na Era Digital; 2. Breves considerações sobre os atos notariais em Portugal. Do presencial ao virtual; 3. Parecer 91/2021 da Comissão Nacional de Proteção de Dados - O Regime Jurídico aplicável à realização de atos notariais à distância; Considerações Finais; Referências bibliográficas.

Resumo: Nas últimas décadas ocorreram várias mudanças na sociedade devido ao grande avanço da tecnologia da informação, mudanças essas onde o Direito está incluído. Assim, considerando o mundo digital em que vivemos, é essencial que o Direito esteja preparado para dar respostas a uma nova sociedade onde passaram a existir novos desafios jurídicos, nomeadamente a proteção dos dados pessoais e a criação de novas plataformas eletrónicas. Sendo uma das características do Direito Notarial a existência da vontade das partes para a outorga dos atos, o presente contributo visa apresentar reflexões iniciais sobre o regime jurídico aplicável à realização de atos notariais à distância que irá entrar em vigor em Portugal a 15 de novembro de 2021, e onde se discutem alguns pontos negativos do referido regime, como é o caso da (possível) falta de vontade das partes aquando a execução dos atos notariais, a proteção dos seus dados pessoais e o cumprimento dos deveres do Código Deontológico por parte do profissional que irá exercer as funções notariais, como os deveres de diligência,

1 Licenciada, Mestre e Doutora em Direito – Faculdade de Direito da U. Porto. Pós-Graduada em Direito da Contratação Pública – CEDIPRE/Faculdade de Direito da Universidade de Coimbra. Prof.^a Adjunta Convidada - ESTG/P. Porto. E-mail: patricia_anjos_azevedo86@hotmail.com.

2 Mestranda em Solicitoria na Escola Superior de Tecnologia e Gestão – Instituto Politécnico do Porto; Pós-Graduada em Gestão de Recursos Humanos pelo Instituto de Estudos Superiores de Fafe; Licenciada em Solicitoria pela Escola Superior de Tecnologias e Gestão – Instituto Politécnico do Porto – Prémio de Mérito Académico; Formadora certificada pelo IEFP. E-mail: andreia_madalena1@hotmail.com

verdade, lealdade e informação. Neste âmbito, será feita uma abordagem à execução dos atos notariais ainda em vigor, onde é exigida a presença física dos intervenientes, não existindo até agora a possibilidade da execução de tais atos à distância, através de videoconferência. Do mesmo modo, achamos oportuno analisar o parecer 91/2021 da Comissão Nacional de Proteção de Dados, uma vez que será necessário acautelar a proteção dos dados pessoais e a tutela dos direitos, liberdades e garantias dos intervenientes que irão fazer uso da (futura) plataforma digital.

Palavras-chave: Ética Jurídica; Sociedade Digital; Direito Notarial à distância; Proteção de dados pessoais.

Abstract: In recent decades there have been several changes in society due to the great advances in information technology, changes where the Law is included. Thus, considering the digital world we live in, it is essential that the Law is prepared to respond to a new society where new legal challenges have arisen, namely the protection of personal data and the creation of new electronic platforms. As one of the characteristics of Notary Law is the existence of the will of the parties to grant the acts, this contribution aims to present initial reflections on the legal regime applicable to the performance of notarial acts at a distance, which will come into force in Portugal on November 15, 2021, and where some negative points of the referred regime are discussed, such as the (possible) lack of will of the parties when performing notarial acts, the protection of their personal data and compliance with the duties of the Code of Ethics by the professional who will perform notarial functions, such as the duties of diligence, truth, loyalty and information. In this context, an approach will be made to the execution of notarial acts still in force, where the physical presence of the interveners is required, and until now the possibility of performing such acts at a distance, through videoconference, will not exist. Likewise, we think it is opportune to analyze the opinion 91/2021 of the National Data Protection Commission, since it will be necessary to safeguard the protection of personal data and the protection of the rights, freedoms and guarantees of the interveners who will make use of the digital platform.

Keywords: Legal Ethics; Digital Society; Notary Law at a distance; Protection of personal data.

1. O Direito na Sociedade Digital. A proteção dos dados pessoais.

O avanço tecnológico tem tido um grande impacto na nossa sociedade, sendo importante que nos saibamos e tenhamos oportunidade de nos adaptar a esta nova era digital. Assim, a própria lei vem garantir o livre acesso às redes informáticas de uso público³ de modo a salvaguardar os interesses dos cidadãos no que a este assunto diz respeito.

A internet veio modificar, por completo, os nossos comportamentos tradicionais e a forma em como obtemos a informação, criando um ambiente mais ágil, mais completo e com mais oportunidades. Também «A República Portuguesa participa no processo mundial de transformação da Internet num instrumento de conquista de liberdade, igualdade e justiça social e num espaço de promoção, proteção e livre exercício dos direitos humanos, com vista a uma inclusão social em ambiente digital.»⁴, sendo que a «todos, independentemente da ascendência, género, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual, têm o direito de livre acesso à Internet.»⁵

Obviamente que o Direito não se encontra imune a estas alterações tecnológicas. E, por esse motivo, é necessário que esteja preparado para dar respostas à sociedade da era digital, nomeadamente aos cibercrimes, a necessidade de combate ao branqueamento de capitais e a proteção dos dados pessoais. É o designado Direito Digital ou Ciberdireito⁶.

Existe, portanto, «(...) a necessidade de que o Direito venha a cada vez mais preocupar-se em desempenar satisfatoriamente seu

3 Artigo 36º, n.º 6 da Constituição da República Portuguesa: «A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional».

4 Artigo 2º, n.º 1 da Lei n.º 27/2021 de 17 de maio - Carta Portuguesa de Direitos Humanos na Era Digital.

5 Artigo 3º, n.º 1 da Lei n.º 27/2021 de 17 de maio - Carta Portuguesa de Direitos Humanos na Era Digital.

6 Conjunto de normas que regulam os novíssimos direitos da que surgiram com os Computadores Pessoais e a Internet. SCHWALBACH, José Gaspar. Direito Digital. Edições Almedina. Coimbra. 2021. p. 7.

papel no contexto das novas tecnologias de informação no que pertence à prevenção/normatização de situações que lhe compete regular.»⁷

Em consequência, havendo uma acréscimo das novas tecnologias digitais, é igualmente importante que o Direito venha a prever novos enquadramentos legais de disciplina e proteção dos cidadãos face às vulnerabilidades inerentes e um ambiente digital e também que se crie, cada vez mais, um Direito informatizado, acessível a todos os cidadãos.

Tudo isto são aspetos positivos, contudo, uma das considerações que devemos ter sempre presente, é que a internet evolui a uma velocidade muito maior que a criação de medidas de segurança capazes de proteger as informações, existindo, entre outros aspetos negativos, a possibilidade da violação dos dados pessoais dos cidadãos.

Como refere Henrique Sousa Antunes: «Se o acesso aos dados (pessoais) é proclamado como uma condição de implementação das novas tecnologias, a afirmação da capacidade, e necessidade, de os sistemas comunicarem entre si corresponde à arquitetura da nova realidade.»⁸

O número 1 do artigo 26º da Constituição da República Portuguesa (doravante designada por CRP), estabelece expressamente que «A todos são reconhecidos os direitos à identidade pessoal, (...) à reserva da intimidade da vida privada (...)), referindo o número 1 do seu artigo 35º que «Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.», não podendo a informática ser utilizada para tratamento de

7 PICON, Leila Cássia, ANTUNES, Solange e DUARTE, Isabel Cristina Brettas. O papel do Direito na sociedade da era informacional. 2º Congresso Internacional de Direito e Contemporaneidade. Universidade Federal de Santa Maria, Brasil. Edição 2013, p. 989, Disponível em <http://coral.ufsm.br/congressodireito/anais/2013/6-17.pdf>, consultado em 18/08/2021.

8 ANTUNES, Henrique Sousa. Direito e Inteligência Artificial. Universidade Católica Editora. Lisboa. Maio de 2020, p. 13

dados referentes à vida privada, a não ser que haja consentimento expresso do respetivo titular (artigo 35º, nº 3 da CRP), sendo também proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei (artigo 35º, nº 4 da CRP).

2. A Carta Portuguesa de Direitos Humanos na Era Digital

A Lei nº 27/2021, de 17 de maio, veio criar a Carta Portuguesa de Direitos Humanos na Era Digital.

Esta Carta, tão recente, demonstra que de facto a Era digital veio mesmo para ficar, e que foi necessário criar um conjunto de medidas que acautelem o acesso ao ambiente digital.

Assim, logo no seu artigo 2º é referido que a República Portuguesa “participa no processo mundial de transformação da Internet num instrumento de conquista de liberdade, igualdade e justiça social e num espaço de promoção, proteção e livre exercício dos direitos humanos, com vista a uma inclusão social em ambiente digital.”

Desta forma, fica expressamente previsto que as normas que na ordem jurídica portuguesa consagram e tutelam direitos, liberdades e garantias são plenamente aplicáveis no ciberespaço, sendo também acautelado o direito à cibersegurança⁹.

O artigo 8º da Carta Portuguesa de Direitos Humanos na Era Digital estabelece o Direito à privacidade em ambiente digital. Assim, é referido que «Todos têm direito a comunicar eletronicamente usando a criptografia e outras formas de proteção da identidade ou que evitem a recolha de dados pessoais, designadamente para

9 Artigo 15.º - Direito à cibersegurança:

1 - Todos têm direito à segurança no ciberespaço, incumbindo ao Estado definir políticas públicas que garantam a proteção dos cidadãos e das redes e sistemas de informação, e que criem mecanismos que aumentem a segurança no uso da Internet, em especial por parte de crianças e jovens.

2 - O Centro Nacional de Cibersegurança promove, em articulação com as demais entidades públicas competentes e parceiros privados, a formação dos cidadãos e empresas para adquirirem capacitação prática e beneficiarem de serviços online de prevenção e neutralização de ameaças à segurança no ciberespaço, sendo para esse efeito dotado de autonomia administrativa e financeira.

exercer liberdades civis e políticas sem censura ou discriminação.»

Com o acréscimo e atualização da legislação referente à proteção dos dados pessoais das pessoas singulares¹⁰, verificamos o aumento na preocupação, por parte do legislador, em salvaguardar os dados pessoais dos cidadãos, numa época em que todas as áreas fazem uso das tecnologias para disseminarem informação.

Como referem Simão de Sant’Ana e Vitorino Gouveia: «(...) a proteção de dados deixou de ser apenas um princípio constitucional de cariz distante. Agora, interage diretamente com todos (...), em poucas palavras, porque a tecnologia mudou tudo à nossa volta – mudou a forma como vivemos.»¹¹

3. Breves considerações sobre os atos notariais em Portugal. Do presencial ao virtual.

Em Portugal, o Decreto-Lei n.º 207/95, de 14 de agosto veio aprovar o atual Código do Notariado, revogando o Código do Notariado aprovado pelo Decreto-Lei n.º 47619, de 31 de março de 1967, uma vez que este último “embora inspirada pelos princípios jurídico-civilistas mais modernos à data, revela-se desadequada face aos desafios do desenvolvimento sócio-económico do País e à internacionalização da economia.”¹²

Ora, de forma resumida, neste momento os atos notariais têm duas características fundamentais:

- São sempre efetuados na presença das partes (seja pelas próprias, seja em representação das mesmas), devendo as mesmas estar presentes para a outorga, a título exemplificativo, de escrituras públicas, de documentos particulares autenticados de factos

10 Podemos ainda referir o Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679 do Parlamento e do Conselho Europeus, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados) e a Lei n.º 58/2019 de 8 de agosto (que assegura a execução na ordem jurídica nacional do RGPD).

11 SANT’ANA, Simão de, e GOUVEIA, Vitorino. O RGPD e os Recursos Humanos – Guia prático para a conformidade. Edições Almedina. Coimbra. março de 2021, p.21.

12 Preâmbulo do Decreto-Lei n.º 207/95, de 14 de agosto.

sujeitos a registo, de reconhecimentos de assinaturas simples ou com menções especiais (salvo no caso em que é possível efetuar reconhecimentos com menções especiais por semelhança¹³), de termos de autenticação.

Esta característica é essencial para que os profissionais possam verificar a vontade das partes e possam aferir da existência de algum vício na formação da vontade das mesmas. E;

- Não se prescinde a apresentação dos documentos originais (documentos de identificação das partes, documentos comprovativos dos poderes de representação, certidões, e dos próprios documentos notariais), salvo nos casos em que os documentos são acessíveis de forma online¹⁴.

Décadas depois, podemos dizer que está na altura de mudar o Direito Notarial (entre outros ramos do Direito) para fazer face a todas as alterações vigentes, nomeadamente em face da Pandemia do Covid-19 em que toda a nossa sociedade teve a necessidade

13 “Artigo 153º do Código do Notariado:
(...)

4 - Os reconhecimentos simples são sempre presenciais; os reconhecimentos com menções especiais podem ser presenciais ou por semelhança.

5 - Designa-se presencial o reconhecimento da letra e assinatura, ou só da assinatura, em documentos escritos e assinados ou apenas assinados, na presença dos notários, ou o reconhecimento que é realizado estando o signatário presente ao acto.

6 - Designa-se por semelhança o reconhecimento com a menção especial relativa à qualidade de representante do signatário feito por simples confronto da assinatura deste com a assinatura aposta no bilhete de identidade ou documento equivalente emitidos pela autoridade competente de um dos países da União Europeia ou no passaporte.”

14 A título exemplificativo: as procurações (devidamente depositadas) podem ser consultadas através do site www.procuracoesonline.pt; as certidões prediais permanentes podem ser consultadas em www.predialonline.pt; as certidões comerciais permanentes podem ser consultadas em www.eportugal.gov.pt; as certidões permanentes dos assentos de nascimento, casamento e óbito podem ser consultadas em www.civilonline.mj.pt; sendo todas elas (entre outras) válidas como se de o original se tratasse.

de uma rápida alteração¹⁵, em que tudo se tornou distanciável (os cidadãos, os métodos de ensino, a forma de fazer e formalizar os negócios).

E, na sequência dos novos paradigmas digitais, está em curso uma grande alteração ao Direito Notarial – a possibilidade de serem realizados atos notariais à distância.

A constante alteração do mundo físico para um mundo (cada vez mais) digital, faz com que seja necessário criar novas soluções, nomeadamente novas formas de alcance referente a negócios jurídicos, sendo exigida uma adaptação dos regimes tradicionais, definição de novos requisitos de validade negocial ou de forma, novos direitos e obrigações das partes envolvidas e consequente alteração legislativa.

De forma a salvaguardar os cidadãos que, neste caso em concreto, recorrem a plataformas informáticas com o intuito de celebrar atos notariais, o Direito deverá estar preparado para possíveis ciberataques, como por exemplo, manipulação dos conteúdos colocados na plataforma, possível exposição ilícita de dados ou de documentos pessoais, reprodução fraudulenta da imagem ou da voz das partes, falsificação de dados que instruem os atos notariais, entre outros.

Uma nota importante para referir que também é necessário adaptar todos aqueles que lidam com o Direito Notarial tradicional – notários, solicitadores, advogados, conservadores, e todos os respetivos funcionários. Assim, é importante que as referidas Ordens Profissionais coloquem ao dispor a formação necessária para que tudo funcione em conformidade antes da entrada em vigor

15 “Já se sentia a necessidade de uma maior integração das novas tecnologias, novas plataformas, novas formas de estar e aprender, com novas dinâmicas, mais práticas e eminentemente tecnológicas e digitais. A pandemia potenciou a construção de uma nova cultura, de onde poderemos retirar lições preciosas (...) – no que refere quanto ao às metodologias tradicionais no ensino superior - Joana Nair S. Carvalho, em https://www.publico.pt/2021/08/27/opiniao/opiniao/paradigma-digital-chegou-universidade-futuro-sera-combinacao-digital-presencial-1975393?fbclid=IwAR3tCGi_xB1DennjlozlkYKpnP-yukc7eVZQWW1PgvRRPq9vMZN6pbpub8, consultado em 20/08/2021

da Lei que irá possibilitar a realização de atos notariais à distância.

A título exemplificativo, o presidente do Sindicato Nacional dos Registos já se pronunciou, referindo que “Nós não temos formação nenhuma, há vários anos, ministrada pelo Ministério da Justiça, não há formação aos trabalhadores e, quando assim é, estas simplificações só nos podem trazer imensas reservas, [sobre] se efetivamente aqui estão acautelados todos os direitos e interesses dos cidadãos e das empresas, ao ser-lhes disponibilizado um canal “online”, em que os trabalhadores nem sequer têm conhecimento de como vai funcionar, nem sequer têm formação para o realizar”¹⁶

4. Parecer 91/2021 da Comissão Nacional de Proteção de Dados - O Regime Jurídico aplicável à realização de atos notariais à distância

A Comissão Nacional de Proteção de Dados (CNPd) é uma entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República. Controla e fiscaliza o cumprimento do Regulamento Geral da Proteção de Dados, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais¹⁷.

Ora, no exercício das suas funções, a mesma emitiu um parecer, a pedido do Gabinete da Secretaria de Estado da Justiça, onde se pronunciou¹⁸ sobre o projeto de lei nº 959/XXII/2021, que estabelece o regime jurídico aplicável à realização, através de

16 Consultado em <https://www.dinheirovivo.pt/economia/nacional/trabalhadores-dos-registos-nao-tem-formacao-para-escrituras-a-distancia-13999568.html> em 27/08/2021

17 Fonte: <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>. Consultado em 20/08/2021.

18 Apenas quanto à matéria de proteção de dados.

videoconferência, de atos autênticos, termos de autenticação de documentos particulares e reconhecimentos de assinaturas, que entrará em vigor a 15 de novembro de 2021.

Para a realização dos atos notariais à distância, prevê-se a criação de uma plataforma informática do Ministério da Justiça, acessível a partir da plataforma digital da justiça e gerida pelo Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., em articulação com o Instituto dos Registos e do Notariado, I.P., na qual serão criadas duas áreas reservadas: uma para os intervenientes e outra para os profissionais.

Para aceder à respetiva área reservada, o utilizador deverá autenticar-se através de cartão de cidadão ou chave móvel digital ou através do certificado profissional (quanto a notários, solicitadores ou advogados).

Será através da área reservada que as partes submetem os documentos instrutórios e acedem aos documentos a lavrar, assinando-os através de assinatura eletrónica qualificada.

É também através da área reservada que as partes acedem às sessões de videoconferência e onde manifestam a vontade com o documento a lavrar, devendo ser prestado o consentimento para a gravação audiovisual.

Quanto ao profissional, através da sua área reservada, o mesmo agenda a realização dos atos a realizar por videoconferência, enviando de seguida uma mensagem ao interveniente, através de endereço eletrónico, com uma hiperligação para a área reservada da plataforma informática que permitirá aceder à videoconferência no dia agendado.

As sessões de videoconferência só se iniciam depois dos intervenientes na sessão terem prestado o seu consentimento para a recolha, pela plataforma informática, dos elementos de identificação associados ao seu cartão de cidadão, assim como prestarem o consentimento para a gravação audiovisual da videoconferência.

Após a leitura e a explicação do documento a lavrar, os intervenientes apõe nele a sua assinatura eletrónica qualificada, submetendo na plataforma digital e após verificar a qualidade da gravação da sessão, o documento é assinado pelo profissional que submete na plataforma digital¹⁹.

Quanto à verificação da identidade dos intervenientes (que no método tradicional é feito através da presença dos mesmos em confronto com os documentos de identificação originais dos mesmos), é efetuada na videoconferência, através do confronto dos elementos de identificação associados ao cartão e constantes no sistema, com a imagem facial da pessoa (neste caso, afigura-se que a única comparação possível seja com a fotografia do documento de identificação), e com as respostas colocadas no início da sessão pelo profissional com o intuito de conformar a sua identidade.

É ainda referido no projeto de lei que, em alternativa, pode aquela identificação fazer-se por recurso a sistema biométrico da comparação das imagens do rosto recolhidas eletronicamente, em tempo real, com a imagem facial constante do sistema de informação responsável pelo cartão de cidadão (devendo-se ter aqui em consideração que os dados biométricos são dados sensíveis que merecem tutela reforçada nos termos do n.º 1 do artigo 9.º do RGPD).

Desta forma, após analisarem o referido projeto de lei, a CNPD verificou que existem lacunas a corrigir no que diz respeito à proteção dos dados pessoais dos interessados, nomeadamente:

- A necessidade de o Decreto-Lei referir expressamente quais os dados do cartão de cidadão que serão objeto de recolha e tratamento, de acordo com as finalidades do tratamento e necessidade da sua utilização;
- A necessidade de estabelecer um regime de salvaguardas

¹⁹ Artigo 9.º, n.º 1 e 4 do projeto de lei: “Encontra-se estabelecido o prazo de conservação dos documentos instrutórios apresentados através da plataforma, bem como das sessões de gravações de videoconferência, que é de 20 anos, as quais apenas podem ser disponibilizadas aos intervenientes através de decisão judicial.

para o sistema de identificação biométrico que venha a prever-se;

- Que se proceda à alteração do artigo 11º, relativa ao responsável do tratamento de dados;

- A necessidade de se consagrar os direitos dos titulares, nomeadamente o direito à informação sobre o tratamento de dados e nomeadamente do modo como pode exercer-los e ainda seja revista a exigência do consentimento para a autorização de gravação da videoconferência.

Considerações Finais

Devido ao grande avanço da tecnologia da informação, ocorreram várias mudanças na sociedade, mudanças essas onde o Direito está incluído, uma vez que a internet veio modificar, por completo, os nossos comportamentos tradicionais e a forma em como obtemos a informação, criando um ambiente mais ágil, mais completo e com mais oportunidades, mas também com mais perigos, nomeadamente quanto à proteção dos nossos dados pessoais.

Para tal, é necessário que o Direito esteja preparado para fazer face aos perigos que existem no mundo digital, de forma a salvaguardar os interesses dos cidadãos.

Um dos ramos do Direito que está prestes a entrar nesta nova Era digital é o Direito Notarial, uma vez que iremos passar de um ambiente onde impera o presencial das partes, para um ambiente virtual, que poderá ser caracterizado pela insegurança, pela falta de vontade das partes, pelo receio da manipulação dos documentos juntos e da própria voz dos interessados, uma vez que será feita a gravação audiovisual.

Assim, para a realização dos atos notariais à distância, prevê-se a criação de uma plataforma informática do Ministério da Justiça, acessível a partir da plataforma digital da justiça e gerida pelo Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., em

articulação com o Instituto dos Registos e do Notariado, I.P., na qual serão criadas duas áreas reservadas: uma para os intervenientes e outra para os profissionais e serão recolhidos dados das partes, com a devida autorização das mesmas.

Cabe ao Direito garantir que todos os interesses das partes envolvidas estejam assegurados e que na formação da vontade das mesmas não surja nenhum vício. Cabe também ao Direito estar preparado para possíveis ataques à dita plataforma, pois estamos perante uma evolução que poderá ser muito útil, mas ao mesmo tempo também muito frágil.

Por último, não poderemos esquecer a diferença de gerações. Poderá esta evolução colocar entraves aos cidadãos de gerações mais antigas e que não saibam lidar com as novas tecnologias?

Nada substitui o presencial, mas deve-se saber, com respeito pela ética digital e profissional, tirar o maior partido das possibilidades que as novas tecnologias nos proporcionam, com o fim único de satisfazermos as necessidades dos interessados, com respeito pela privacidade dos mesmos.

Referências Bibliográficas

AA.VV. Direito e Novas Tecnologias. Edições Almedina Brasil. 2020;

ANTUNES, Henrique Sousa. Direito e Inteligência Artificial. Universidade Católica Editora. Lisboa. Maio de 2020;

CORDEIRO, A. Barreto Menezes. Direito da Proteção de Dados- À luz do RGPD e da Lei n.º 58/2019. Edições Almedina. Coimbra. 2020;

FERREIRINHA, Fernando Neto. A função Notarial dos Advogados e dos Solicitadores. Edições Almedina. Coimbra. 2019;

FERREIRINHA, Fernando Neto. Manual de Direito Notarial. 2ª edição. Edições Almedina. Coimbra. 2019;

FIGUEIREDO, David Martins Lopes de. Titulação de Negócios

Jurídicos sobre Imóveis. 3ª edição. Edições Almedina. Coimbra. 2019;

PICON, Leila Cássia, ANTUNES, Solange e DUARTE, Isabel Cristina Brettas. O papel do Direito na sociedade da era informacional. 2º Congresso Internacional de Direito e Contemporaneidade. Universidade Federal de Santa Maria, Brasil. Edição 2013. Disponível em <http://coral.ufsm.br/congressodireito/anais/2013/6-17.pdf>, consultado em 18/08/2021;

SANT'ANA, Simão de, e GOUVEIA, Vitorino. O RGPD e os Recursos Humanos – Guia prático para a conformidade. Edições Almedina. Coimbra. Março de 2021;

SCHWALBACH, José Gaspar. Direito Digital. Edições Almedina. Coimbra. 2021;

SILVA, Artur Flamínio da. Direito Administrativo e Tecnologia. Edições Almedina. Coimbra. Março de 2021;

VALLES, Edgar. Atos Notariais dos Advogados e Solicitadores. 7ª edição, Edições Almedina. Coimbra. 2020.

As novas regras do IVA para o comércio eletrónico

The new vat rules for e-commerce

José de Campos Amorim¹

Sumário: 1. Introdução; 2. Conceito de comércio eletrónico; 3. Tipos de transações eletrónicas; 4. Regras de tributação; 5. Localização das vendas à distância; 6. Aplicação das novas regras de localização das prestações de serviços; 7. Considerações finais.

Resumo: O presente trabalho apresenta uma reflexão sobre o novo regime de tributação em sede de IVA das prestações de serviços de telecomunicações, de radiodifusão ou televisão e serviços por via eletrónica a não sujeitos passivos estabelecidos ou domiciliados na União Europeia. O regime do Balcão Único destina-se a responder a este tipo de prestações de serviços e evita que os sujeitos passivos tenham que se registar para efeitos do IVA em cada Estado-membro de consumo. Este sistema pode ainda ser utilizado pelas interfaces eletrónicas (mercados, plataformas, etc.) para facilitar todas as entregas intracomunitárias de bens ou serviços. São assim criadas novas regras de localização das vendas à distância que preveem a tributação no território nacional ou noutro Estado-membro, em função da situação em concreto.

Palavras-chave: IVA; Balcão Único; Sujeito Passivo, Comércio Eletrónico

Abstract: This work presents a reflection on the new regime for VAT on supplies of telecommunications, broadcasting and electronic services to non-taxable persons established or domiciled in the European Union. The One Stop Shop system is designed to deal with this type of supply of services and avoids the need for taxable persons to register in each Member State of consumption. This system can also be used by electronic interfaces (marketplaces, platforms, etc.) to facilitate all intra-Community supplies of goods or services. New rules have therefore been created for the location of distance sales which provide for taxation on national territory or in another Member State, depending on the specific situation.

Keywords: VAT; One-stop-shop; Taxable person, E-Commerce.

¹ Doutorado em Direito. Professor Coordenador de Direito Fiscal. Membro do Centro de Estudos Organizacionais e Sociais do Politécnico do Porto (CEOS.PP).

1. Introdução

Com a evolução das novas tecnologias e o seu impacto no dia-a-dia das pessoas tornou-se necessário adaptar as regras do IVA para fazer face ao desenvolvimento do comércio eletrónico.

Perante o novo regime resultante da entrada em vigor da Diretiva 2017/2455, do Conselho, de 5 de dezembro de 2017, que altera a Diretiva IVA - Diretiva 2006/112/CE - e a Diretiva (UE) 2019/1995 do Conselho, de 21 de novembro de 2019, que foram transpostas para a ordem jurídica portuguesa pela Lei n.º 47/2020, de 24 de agosto, importa analisar as suas especificidades e determinar as obrigações em matéria de IVA para as prestações de serviços e as vendas de bens à distância realizadas pelas empresas.

Objetivos do novo regime de tributação:

- a) Simplificar as obrigações declarativas e de pagamento, facilitar as transações transfronteiriças e combater a elevada taxa de evasão fiscal;
- b) Promover a concorrência entre empresas europeias e não europeias, entre pequenos e grandes contribuintes, sem esquecer o papel importante das grandes plataformas digitais.
- c) Criar regras comuns para todas as empresas da UE e fora da UE, que vendam bens ou serviços on-line a particulares na União Europeia (B2C), independentemente do meio utilizado (sites Web exclusivos; Marketplaces (Amazon, Ebay, AliExpress, Fnac, etc...); redes sociais (Facebook, Instagram, Snapchat, Twitter, etc...)).

Desta nova realidade resultou um conjunto de alterações fiscais destinadas a simplificar as obrigações declarativas, facilitar as transações, combater a evasão fiscal e manter uma certa concorrência entre empresas. O sistema fiscal apresenta diferentes soluções legislativas, baseadas em recentes diretivas comunitárias, destinadas a fazer face aos vários tipos de prestações de serviços e vendas à distância.

Este artigo tem por objetivo apresentar alguns aspetos teóricos e práticos destinados a compreender as alterações fiscais em matéria de comércio eletrónico.

2. Conceito de comércio eletrónico

O legislador nacional não dá uma definição de serviços prestados por via eletrónica, apenas limitou-se a acrescentar no art. 3º do Decreto-Lei nº 130/2003 um anexo D, que contém uma lista exemplificativa dos serviços prestados por via eletrónica a que se refere a art. 6º nºs 9 e 10 do CIVA que faz parte integrante.

O serviço prestado por via eletrónica implica a utilização da tecnologia da informação para a sua prestação, envolvendo uma intervenção humana mínima, sendo a prestação assegurada de forma automática ou quase automática, em que as transações são efetuadas não de forma tradicional, mas num ambiente virtual, por via eletrónica.

O comércio eletrónico envolve as transações comerciais realizadas por via eletrónica, praticadas por organizações ou indivíduos, baseadas num processo de transmissão de dados por via eletrónica, incluindo texto, som e imagem. Nele se integram todas as atividades comerciais relevantes realizadas por empresas, consumidores e governos, através de redes eletrónicas, como a Internet e a Word Wide Web (WWW), incluindo operações de marketing, serviços de telecomunicações, serviços jurídicos, financeiros, musicais e audiovisuais, etc..., bem como a venda de bens físicos através de meios eletrónicos (Comissão Europeia, 1998)².

Por exemplo, as empresas que se dedicam à comercialização de jogos virtuais e músicas possuem um site onde se pode, mediante

2 Comissão Europeia (1998). “Comércio Electrónico e Fiscalidade Indirecta”, COM(1998) 374 final. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:51998DC0374&from=FR>

3 IDC (2002), eBusiness: Análise do mercado e tendências de investimento, 2001-2005, Lisboa, IDC Portugal, maio de 2002.

pagamento, adquirir músicas, através do descarregamento das mesmas no próprio equipamento informático. Segundo Oliveira e Ruão (2016), o comércio eletrónico permite a comercialização de bens intangíveis em formato digital, dando a possibilidade ao cliente de adquirir um determinado tipo de produto e proceder ao seu descarregamento através da internet, realizando a encomenda e efetuando o pagamento por via de meios eletrónicos³.

O comércio eletrónico permite assim aos compradores e vendedores transacionarem virtualmente bens e serviços através da internet ou por via de outros meios eletrónicos.

3. Tipos de transações eletrónicas

O comércio eletrónico abrange vários tipos de transações eletrónicas:

- a) As transações eletrónicas entre as empresas (B2B),
- b) As transações eletrónicas entre empresas e consumidores finais (B2C),
- c) As transações eletrónicas entre empresas e o Estado (B2A)

As transações eletrónicas entre empresas - “ Business to business” (B2B) - estão divididas em três grandes áreas: o e-Marketplace (são plataformas eletrónicas que permitem às empresas estabelecerem relações comerciais entre compradores ou vendedores), o e-Procurement (são plataformas digitais que se destinam a apoiar o aprovisionamento das empresas, possibilitando a redução de custos no abastecimento dos bens), e o e-Distribution (são plataformas eletrónicas que permitem a integração das organizações com os seus distribuidores e filiais).

As transações eletrónicas entre empresas e consumidores finais - “Business to consumer” (B2C) - envolvem relações

3 Oliveira, M. O., & Ruão, J. B. A. B. (2015). “A tributação do consumo no comércio internacional: da falta de coesão à necessidade de concertação”, Revista da Faculdade de Direito da Universidade Lusófona do Porto, v. 7, n.º 7.

comerciais de bens e serviços entre empresas e consumidores finais e operam, fundamentalmente, no comércio de retalho, promovendo novas oportunidades de distribuição.

No caso das transações eletrónicas entre as empresas e a administração pública (“ Business to Administration” (B2A)), as empresas envolvem uma grande quantidade de produtos e serviços, todos digitais, no setor, principalmente, da administração fiscal, do notariado, dos registos, do emprego e da segurança social. Através destas transações, o Estado consegue uma redução significativa dos custos e ainda uma melhoria na arrecadação de tributos.

4. Regras de tributação

Desde 1 julho de 2021, o regime das vendas à distância, regulado nos artigos 10.º e 11.º do RITI, sofreu profundas alterações, em consequência da entrada em vigor da Diretiva (UE) 2017/2455 do Conselho, de 5 de dezembro de 2017, e da Diretiva (UE) 2019/1995 do Conselho, de 21 de novembro de 2019, que foram transpostas para a ordem jurídica portuguesa, pela Lei n.º 47/2020, de 24 de agosto, bem como do Regulamento de Execução (UE) 2019/2026, do Conselho de 21 de novembro de 2019.

A Lei n.º 47/2020, de 24 de agosto aditou a alínea q) do n.º 2 do artigo 1.º do Código do IVA que a seguir transcrevemos:

“q) ‘Vendas à distância intracomunitárias de bens’, as transmissões de bens expedidos ou transportados pelo fornecedor ou por conta deste, inclusive quando o fornecedor intervenha indiretamente no transporte ou na expedição dos bens, a partir de um Estado-Membro que não seja o Estado-Membro de chegada da expedição ou transporte com destino ao adquirente, quando se verificarem, simultaneamente, as seguintes condições:

i) O adquirente não se encontre abrangido por um regime de tributação das aquisições intracomunitárias no Estado-Membro de chegada da expedição ou transporte dos bens, ou seja um particular;

ii) Os bens não sejam meios de transporte novos nem bens a instalar ou montar.”

As novas regras preveem a tributação no país de destino e introduzem, para tal, mecanismos simplificados de cumprimento das obrigações fiscais, bem como uma nova definição do papel das plataformas eletrónicas na cobrança do IVA nas vendas online.

É criado um novo limiar de tributação (na origem) de 10.000€ para as vendas à distância na União Europeia aplicável aos serviços de telecomunicações, de radiodifusão ou televisão e serviços prestados por via eletrónica (TBE) e para as vendas à distância intracomunitárias de bens, determinando a aplicação do princípio da tributação no destino de vendas à distância intracomunitárias de bens. De acordo com as novas regras em vigor desde 1 de julho de 2021, abaixo de um limiar de 10.000€, o IVA pode ser pago ao Estado-membro onde a empresa vendedora está localizada. Acima deste limiar, as empresas poderão registar-se num Balcão Único (OSS - One Stop Shop) – onde podem facilmente declarar e pagar o IVA devido noutros Estados-membros.

Com a entrada em vigor deste novo regime é possível efetuar o registo no Portal das Finanças.

A obrigação de registo no Balcão Único/Regime OSS não se coloca se os clientes da empresa forem todos sujeitos passivos de IVA (B2B). No caso de vendas à distância ou serviços eletrónicos prestados a sujeitos passivos (B2B) ou consumidores finais (B2C), então já se impõe efetuar o registo no Portal das Finanças. Da mesma forma que se uma empresa estiver a trabalhar exclusivamente com consumidores finais (B2C), torna-se também necessário efetuar o registo.

O Balcão Único tem em vista simplificar as obrigações fiscais para os vendedores de bens e prestadores de serviços aos consumidores finais da UE, uma vez que lhes permite efetuar o registo eletrónico para efeitos de IVA num único Estado-membro para todas as vendas à distância de bens e prestações de serviços entre empresas e consumidores, evitando assim o registo em vários Estados-membros. Em termos de obrigações declarativas,

o Balcão Único admite a apresentação de uma única declaração eletrónica trimestral e o pagamento do IVA relativamente a todas as entregas de bens e prestações de serviços. Além disso, o Balcão Único permite trabalhar diretamente com a administração fiscal do seu próprio Estado, facilitando o acesso a um portal - Balcão Único - onde as empresas poderão efetuar o registo. O registo é válido para todas as vendas a consumidores de outros Estados-membros da UE.

O Balcão Único tem ainda a vantagem de permitir a aplicação da taxa de IVA do Estado-membro para o qual os bens são enviados ou onde são prestados os serviços; de cobrar o IVA ao comprador nas vendas à distância de bens ou prestações de serviços intracomunitárias; de enviar uma declaração trimestral de IVA através do portal do Balcão Único do Estado onde estiver registado e de fazer um pagamento trimestral do IVA ao Estado onde estiver registado no Balcão Único.

O Balcão Único pode ainda ser utilizado pelas interfaces eletrónicas (mercados, plataformas, etc.) para facilitar todas as entregas intracomunitárias de bens ou serviços. A interface eletrónica facilita as vendas à distância de bens através de um vendedor não estabelecido na UE a um comprador da UE. A interface eletrónica, como é o caso do Marketplace, coloca à disposição dos compradores diversos produtos e serviços. Para declarar e pagar o IVA, a interface eletrónica deverá estar registado no sistema OSS. Uma vez que a interface eletrónica tem o papel de facilitadora da entrega de bens, torna-se também responsável pelo pagamento do IVA.

O Marketplace é considerado um fornecedor presumido, de acordo com a Diretiva (UE) 2017/2455, do Conselho, de 5 de dezembro de 2017, na medida em que tem em vista facilitar as vendas à distância de bens importados de países terceiros de valor igual ou inferior a 150€ e a entrega de bens dentro da comunidade por um sujeito passivo de IVA, que não se encontra estabelecido na

UE, a um não sujeito passivo de IVA. Assim, nas vendas efetuadas através de um Marketplace, os bens podem ser transacionados diretamente do vendedor real (fornecedor subjacente) para o consumidor final. No caso de serem efetuadas através de um fornecedor presumido (Marketplace), o sujeito passivo que opera a Interface eletrónica adquire e vende os bens ao fornecedor subjacente e ao consumidor final, respetivamente.

Resulta que quando a cláusula do fornecedor presumido é aplicada, a transação real do fornecedor subjacente para o adquirente deixa de existir para efeitos de IVA, sendo convertida numa transmissão de bens do fornecedor subjacente para o Marketplace e numa transmissão de bens do Marketplace para o consumidor final. A transmissão de bens do fornecedor subjacente para o Marketplace é uma operação B2B e, de acordo com o n.º 11 do artigo 13 do CIVA ocorre sem afetação de transporte. Esta transmissão de bens localiza-se no território onde os bens se encontram no momento em que se inicia o transporte da operação real⁴.

Quanto à transmissão de bens do Marketplace para o consumidor final, trata-se de uma operação B2C e, de acordo com o art. 3.º do CIVA, o seu transporte é afetado a essa operação. Assim, nas importações e nas transmissões internas a operação é tributada no Estado-membro de destino.

No Portal da Autoridade Tributária e Aduaneira, estão previstas quatro opções de balcões únicos, sendo o regime da UE e o regime da Importação os mais comuns. Para assegurar a transição para o novo regime, os sujeitos passivos com anterior registo feito no MOSS não precisam de efetuar um novo registo, transitam diretamente para o novo regime (OSS) a partir de 01-07-2021. Ao contrário do registo no regime OSS, em que se mantém o NIF do sujeito passivo PT, no regime i-OSS é atribuído um novo NIF,

4 COMISSÃO EUROPEIA (2020). Explanatory Notes on VAT e-commerce rules, https://ec.europa.eu/taxation_customs/system/files/2020-12/vatecommerceexplanatory_28102020_en.pdf

a utilizar exclusivamente para este efeito. Vejamos, sucintamente, cada uma destes regimes:

a) Regime da União Europeia

Regime da União - OSS-UE – que já existia, aplicável às empresas da UE, é alargado, passando a incluir as vendas à distância intracomunitárias, incluindo as realizadas através de plataformas digitais.

Os operadores económicos registados na UE, que prestam serviços à distância, aplicam o regime da União. Para se registar no regime da EU, o operador deverá preencher uma das seguintes condições:

- Ser sujeito passivo estabelecido na UE e pretender declarar e pagar o IVA relativamente a prestações de serviços B2C ou a vendas à distância;

- Ser uma interface eletrónica (estabelecida na UE ou fora da UE) que facilita a venda à distância intracomunitária de bens.

b) Regime Extra-União

O regime extra-União – OSS-EUE – é alargado a todos os serviços prestados por sujeitos passivos não estabelecidos na UE a consumidores da UE (B2C), obrigados a registo e liquidação do IVA à taxa do país de consumo (ou através de intermediário – devedor do IVA).

Os operadores económicos não registados na UE podem aplicar o regime extra-União, bem como podem registar-se no regime da União para efetuar vendas à distância intracomunitárias. Por exemplo, se um operador dos Estados Unidos pretender realizar vendas de bens e prestações de serviços na UE, poderá registar-se no regime da União para as transmissões de bens localizadas na UE, no regime extra-União para a realização de serviços e no regime

IOSS da importação para a transmissão de bens importados.

O regime extra-União é a continuação do MOSS, que apenas se aplicava a serviços de telecomunicações, radiodifusão ou televisão e serviços por via eletrónica e que agora se aplica a todos os serviços prestados por sujeitos passivos não estabelecidos na UE a consumidores da UE (B2C).

Para se registar neste regime deverá ser um sujeito passivo não estabelecido na UE que efetua prestações de serviços a consumidores finais e cujo local de tributação das mesmas se situa na UE.

c) Regime Importação

O regime das vendas à distância de bens importados – iOSS – corresponde ao novo regime aplicável aos bens importados de valor inferior a 150 €, que não sejam sujeitos a IEC e se destinem a consumidores da UE.

Para se registar neste regime, deverá confirmar que é sujeito passivo que efetua vendas à distância de bens (de produtos não sujeitos a impostos especiais de consumo) importados de países ou territórios terceiros, de valor intrínseco não superior a 150 €.

Assim, se uma empresa americana pretender vender um determinado bem a partir dos Estados Unidos, através de uma plataforma eletrónica, a um preço abaixo de 150€, terá que liquidar o IVA ao cliente final, desde que obtenha um número IOSS. Caso não o faça, o IVA será liquidado na alfândega do Estado-membro de chegada dos bens, através do regime especial de liquidação do IVA, pelo intermediário. Se o valor ultrapassar os 150€, seguem-se as regras gerais de importação no Estado-membro do adquirente, não tendo o fornecedor de obter um número IOSS.

d) Regime Importação (por um intermediário)

Para se registar como intermediário, o sujeito passivo deve estar estabelecido no território nacional, ter a intenção de agir em nome e por conta de outro(s) sujeito(s) passivo(s) e cumprir todas as obrigações do regime em nome daqueles que irá representar.

5. Localização das vendas à distância

As regras de localização das vendas à distância preveem a tributação no território nacional, com IVA português, ou noutro Estado-membro, neste caso sem IVA português.

Consideram-se localizadas no território nacional, com IVA português, as vendas à distância intracomunitárias efetuadas por um sujeito passivo de um outro Estado-membro a particulares em território nacional, com local de entrega no território nacional; as vendas à distância de bens importados quando desalfandegados noutro Estado-membro mas entregues a particulares no território nacional e ainda as vendas à distância intracomunitárias de bens importados quando desalfandegados em Portugal e entregues a particulares em território nacional por um vendedor registado no Novo Regime Especial dos Bens Importados (iOSS).

Nestes três casos, sendo o local de entrega o território nacional, a tributação opera em Portugal, à taxa de IVA nacional.

As operações são consideradas localizadas noutros Estados-membros, não sendo então aplicado o IVA português, quando resulta de vendas à distância intracomunitárias efetuadas por um sujeito passivo português a particulares de outros Estados-membros, com local de entrega noutros Estados-membros; bem como quando se trata de vendas à distância de bens importados e desalfandegados em Portugal, mas entregues a particulares residentes noutros Estados-membros da UE.

Nestes dois casos, não sendo operações tributadas em Portugal pelo facto de o local de entrega não ser o território nacional, não se aplica o IVA português.

6. Aplicação das novas regras de localização das prestações de serviços

Uma empresa portuguesa deve liquidar IVA português, na sua declaração periódica de IVA, caso preste serviços eletrónicos ou faça vendas à distância para consumidores finais, “de forma esporádica”, não ultrapassando os 10.000,00 €/ano (no ano anterior ou no decorrer do atual). Este limiar é aplicável a todos os Estados-membros da UE.

Fora destas condições, a regra é a tributação à taxa do país de destino/consumo (particulares da UE) mediante um único registo no Balcão Único, através do qual o sujeito passivo português fará a entrega da declaração e o pagamento do imposto devido a cada Estado-membro no final do mês seguinte ao trimestre anterior.

Assim, se o total das vendas a particulares de outros Estados-membros ultrapassar esse limite, os sujeitos passivos portugueses terão que se registar nos Estados-membros de destino e aí liquidar e entregar imposto às taxas em vigor nesses países.

Como alternativa, os sujeitos passivos podem proceder ao seu registo no Balcão Único, por via eletrónica, acedendo, para o efeito, à respetiva aplicação que se encontra disponível no Portal das Finanças, em: <https://www.portaldasfinancas.gov.pt/oss/>

Este registo no Balcão Único é facultativo e não obrigatório, estando regulamentado no Anexo I da Lei 47/2020, de 24/08.

O sujeito passivo que opte pelo registo no Balcão Único tem que entregar a declaração e o respetivo pagamento do IVA, que deverá ocorrer trimestralmente, até ao fim do mês seguinte a cada trimestre civil, nos termos do artigo 13.º, conjugado com os artigos 6.º, 7.º e 8.º do anexo I da Lei n.º 47/2020, de 24/08, sendo que nos trimestres onde não efetua vendas terá que entregar a declaração a zeros.

Por exemplo, se uma empresa portuguesa, sujeito passivo

estabelecido no continente, vender jogos online a um particular espanhol, tendo tido no ano civil em curso um volume anual de negócios de 8.000€, a operação é considerada localizada no território nacional (art.6.ºA, n.º 1 do CIVA). Contudo, esta mesma empresa portuguesa pode optar por ser tributado em Espanha, pelo facto de a operação ser aí localizada (artigo 6.ºA, n.os 1 e 4 do CIVA).

Ao contrário, se um sujeito passivo estabelecido em Espanha vender livros online (Ebook) a particulares domiciliados em Portugal, tendo tido no ano civil em curso um volume anual de negócios de 6.000€, a operação é localizada em Espanha, podendo contudo optar pela tributação em Portugal (artigo 6.ºA, n.º 2 e 4 do CIVA).

Resulta que no caso de uma empresa portuguesa efetuar a venda de uma mercadoria, sem instalação ou montagem, com destino a um cliente particular residente noutra Estado-membro da UE, a venda deve ser tratada como uma venda à distância intracomunitária de bens, sendo tributada à taxa de IVA português se a venda à distância for efetuada a um particular de um outro Estado-membro e se não ultrapassar o valor anual de € 10.000,00. Este novo regime não prevê qualquer alteração se os clientes forem sujeitos passivos de IVA.

7. Considerações finais

O desenvolvimento das novas tecnológicas aumentou as transações de bens e serviços por via eletrónica, tornando-se pertinente que as administrações fiscais tenham em atenção que estes problemas existem e que importa fixar regras ao nível das vendas à distância intracomunitária de bens para poder aplicar o novo regime de IVA se uma determinada venda à distância for efetuada a um particular de um outro Estado-membro e ultrapassar ou não ultrapassar o limiar anual de € 10.000,00. Este novo regime não prevê qualquer alteração se os clientes forem sujeitos passivos

de IVA.

O novo regime apresenta várias soluções para os sujeitos passivos que efetuem prestações de serviços de telecomunicações, de radiodifusão ou televisão e serviços prestados por via eletrónica, efetuadas a uma pessoa que não seja sujeito passivo. Este novo regime, em vigor desde 1 de julho de 2021, fixa igualmente regras de simplificação das obrigações declarativas e de pagamento, facilita as transações transfronteiriças e tenta assim combater a evasão fiscal. Este regime promove também a concorrência entre empresas europeias e não europeias, entre pequenos e grandes contribuintes, e atribui um papel importante às plataformas digitais, como é o caso dos Marketplaces.

Falta saber se estas regras comuns aplicáveis a todas as empresas da UE e fora da UE vão efetivamente promover a concorrência e combater a evasão fiscal. Temos que aguardar para saber se as empresas vão aderir ao regime OSS e se, tecnicamente, o sistema está totalmente operacional para fazer face a todo este tipo de operações.

Referências bibliográficas

ALMEIDA, Maria Teresa de Jesus. (2010). A Tributação do Comércio Electrónico on-line, Universidade de Aveiro.

COMISSÃO EUROPEIA (1998). “Comércio Electrónico e Fiscalidade Indirecta”, COM(1998) 374 final.

<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:51998DC0374&from=FR>

COMISSÃO EUROPEIA (2020). Explanatory Notes on VAT e-commerce rules, https://ec.europa.eu/taxation_customs/system/files/2020-12/vatecommerceexplanatory_28102020_en.pdf

IDC (2002), eBusiness: Análise do mercado e tendências de investimento, 2001-2005, Lisboa, IDC Portugal, maio de 2002.

LIGHTHART, J. E. (2004). “Consumption Taxation in a Digital World: A Primer”. Center Discussion Paper; Vol. 2004-102, Macroeconomics.

OLIVEIRA, M. O., & RUÃO, J. B. A. B. (2015). “A tributação do consumo no comércio internacional: da falta de coesão à necessidade de concertação”, Revista da Faculdade de Direito da Universidade Lusófona do Porto, v. 7, n.º 7.

PARRILLI, Davide Maria (2008). «European VAT and electronically supplied services» in

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261822, consultado a 14 de setembro de 2021.

RORIZ, J. (2017). Atualização fiscal em IVA. Ordem dos Contabilistas Certificados.

TAVARES, Armando Jorge de Almeida (2007). A tributação do comércio electrónico: dificuldades na aplicação do normativo nacional, Dissertação de Mestrado do Departamento de Economia, Gestão e Engenharia Industrial da Universidade de Aveiro.

GDPR tailored-made explanations in credit scoring must end

Case study on the Right to Suggestive-commoditization of an IDSS MAS-based classifier

Diogo Morgado Rebelo¹

Summary: 1. Introduction; 2. Application scoring for Credit in the Age of Artificial Intelligence; 3. Intelligent-based CWA Profiling and ADM; 4. Conclusion.

Abstract: Nowadays, consumers should fear how some of their demographic, financial, employment or behavioural information might impact their ability to be granted loans. DM approaches, applying ML models, often hide black box correlations within multiple fuzzy inferences. Apart from lenders' trade secrets, the average level of digital literacy does not let data subjects to fully understand the logic involved - i.e., how the machine follows the rules -, regardless of how aware they might be of the importance and the consequences of such processing. Consequently, consents provided will in no way be deemed as valid, hence, affecting the lawfulness of evaluations. Those opacity traits make it possible to doubt the existence, scope and feasibility of a right to an ex-post detailed explanation enshrined in Article 22(3) of the GDPR, also indirectly underlying many other technophobic remits. In this study, particularly, the purposed credit suggestion agent settles the solution to the unenforceable entanglement of a right to informative self-determination in automated (cyber)-credit. To make it clear, when put into practice, the solvency profile automatically drawn up by the model-based decision agent operates by clustering clients in their creditworthiness condition, using NNs for such classification task. Alternatively, the suggestion agent operating next externalize a genetic automated counterfactual, revealing why a particular application ends up in denial or refusal of lending credit. By design, within ADM course, this methodology provides interpretations of which parameters were individually lacking and leads to inverse the non-acceptance outcome, being more feasible and useful for consumer applicants. Thus, national legislators must once and for all perceive data as a real asset. Banking institutions shall be obliged to ascertain the duty by which clients would achieve specific transactional and personal advantages for providing alternative missing data.

¹ Junior Researcher at JusGov Centre, E. Tec. Department and Postgraduate on Law and Informatics, both at the University of Minho. E-mail: djmr1995@gmail.com.

Keywords: Consumer's Creditworthiness Assessment; IDSS MAS-based Agent; Right to (Automated) Suggestions.

1. Introduction

Despite all the European attempts to uniformize sufficient legal grounds of privacy-preserving on exclusive credit-related ADM, data subjects still do not understand autonomous processing and have little control over how personal credit data is used to exhort predictions. With the establishment of a right to Automated Suggestion in application-related scoring, Fábio Silva's Multi-Agent System (MAS) provides, by default, SMEs or FinTech Giants a straightforward privacy-friendly compliance solution through 'Law in Action'.

2. Application scoring for credit in the age of Artificial Intelligence

Creditworthiness assessment (CWA) figure under statistical classification models that extract insights from relevant data into numeric measures, thus influencing lending decision-making at different levels². The process represents either mathematical theories, computational algorithms or statistical programmes that can ascertain how likely consumers are to pay back their debt obligations³. Today, scoring in credit outlines customers' creditworthiness review, a helpful tool for assessing and preventing default risk, an essential step in credit risk evaluation, or rather, last

2 See ANDERSON, Raymond - The credit scoring toolkit: theory and practice for retail credit risk management and decision automation. Oxford University Press, 2007, p. 3.

3 See FERRETI, Federico - The Never-Ending European Credit Data Mess, BEUC Position Paper, Brunel University London, 2017, pp. 15-16.

(but not least), an active research field in financial risk management⁴.

Albeit referred to as one of the most ancient financial intricacies (or consumer law hot topics) since its very beginning, CWA positioned itself as a useful Intelligent Decision Support Systems (IDSSs)⁵ to aid lenders' arrangements in banking institutions for about fifty years ago⁶. Nowadays, AI-powered CWA underpin some self-evident advantages over conventional methods in a contemporary FinTech scenario. Creditors who grant (or at least promise) loans in business courses can or may evaluate quicker and better investment risks from multiple approaches - using broader, dynamic or even refreshed datasets - also ensuring a maximum operational profit by readjusting management policies. At its best and worst, AI procedures in credit now provide the capability to automatically monitor assets in real-time, reduce maintenance expenses and improve the quality of the services provided. With AI, banks can now deal more carefully with unknown and unpredictable consumers' behaviour⁷.

3. Intelligent-based profiling for CWA and ADM

Nowadays, clients' history constitutes valuable assets to banking institutions, spotlighting Artificial Intelligence (AI) governance on credit scoring, and thus, the growth of the human-machine interface in Banking 4. 0.. In this regard, Article 18(1) of the Proposal for a Directive of the European Parliament and of the

4 See LOUZADA, Francisco; ARA, Anderson; FERNANDES, Guilherme, Classification methods applied to credit scoring: Systematic review and overall comparison. In: Surveys in Operations Research and Management Science, 2016, vol. 21, no. 2, p. 117.

5 IDSSs are computer-based programs that manage database systems, expert knowledge, and organisations' models to help decision-makers (DMs) solve semi-structured tasks, Intelligent applications within the Business Intelligence spectrum aid a set of recommendations imparting particular domain expertise. See KAKLAUSKAS, Arturas - Introduction to Intelligent Decision Support Systems. In: Biometric and Intelligent Decision-Making Support, Springer, Cham, 2015. p. 2.

6 See THOMAS, Lyn; CROOK, Jonathan; EDELMAN, David - Credit scoring and its applications, Society for industrial and Applied Mathematics, Philadelphia, 2017, p. 9.

7 See BPI; Covington & Burling LLP - Artificial Intelligence Discussion Draft: The future of credit underwriting – Artificial Intelligence and its role in Consumer Credit, 2019, pp. 4-5.

Council on consumer credits (COM(2021) 347 final), of 30 June 2021 (hereinafter, PDCC), enhance the general interest in preventing irresponsible lending and costumers' over-indebtedness. According to Article 18(2) of the PPCC, credit-related assessments shall consider relevant and accurate information on the consumers' income, their expenses, among other financial and economic circumstances. So, clients' profiles will have to be inferred solely whether necessary and proportionate, such as evidence of income or other sources of repayment, information on financial assets and liabilities, or other financial commitments⁸. To that its non-exhaustive extent, some supplementary demographic, financial, employment, or behavioural predictors⁹ portray yet and further soon excellent input sources for AI-based systems to perform predictive analysis at the scale of better Know-your-costumer (KYC) strategies¹⁰.

However, (potential) credit-related borrowers should fear how all some sorts of personal data (e.g., gender, age, social background, purchase history, web browsing, etc.) might impact their ability to be granted a loan over target advertising (see Article 4(1) of the GDPR)¹¹. This occurs since managing AI tools for scoring in retail banking (among other lending entities involved) often entails outlining privacy-invasive, non-intuitive and unverifiable inductions¹². Inferred data regarding credit solvency often premises profiling clients, especially in what concerns to their (c)haracter, (c)apacity, (c)apital or (c)ollateral traits (see Articles 4(4), 9(1), 22 and

8 See Proposal for a Directive of the European Parliament and of the Council on consumer credits, of 30 June 2021, p. 24.

9 See VOJTEK, Martin; KOÅENDA, Evien – Credit-Scoring Methods. In: Czech Journal of Economics and Finance (Finance a uver), Prague, vol. 56, no. 3-4, 2006, p. 164, table no. 1.

10 See CHEN, Ting-Hsuan - Do you know your customer? Bank risk assessment based on machine learning. In: Applied Soft Computing, vol. 86, no. 105779, 2020, p. 1.

11 See SARTOR, Giovanni – The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, EPRS Study, June 2020, p. 15, p. 15.

12 See WACHTER, Sandra; MITTELSTADT, Brent - A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. In: Columbia Business Law Review, vol. 2012, no. 2, 2019, p. 497, in general, and p. 516, concerning credit scoring in particular.

Recitals 71,72,73 of the GDPR)¹³.

As it is now clear, during negotiation stage, the usage of AI software to prospect CWA represent more than ever the dynamics of IDSSs' underlying exclusive Automated Decision-Making (ADM)¹⁴. Today, computer programs self-manage Data Warehouses, expert knowledge and learning models to assist semi-structured problem-solving in finance, thus, improving the quality, speed and effectiveness of the underwriting operations.

At its best and its worst, consumers acceptances or denials figure to be exclusively automated. And that may occur directly into the usage of online platforms or by the formal intermediation of a middleman who, in practice, is obliged to fulfil banking policies and do not control the outcomes processed.¹⁵ From a psychological viewpoint, although perhaps stamped by formal human-in-the-loop involvement, front-officers may tend to become too complacent, over-reliant or unduly diffident when faced with the highly accurate outputs of an AI-based system.¹⁶

On the one hand, the denial of a credit application, regarding AI systems, can significantly affect the user's legal sphere, as envisaged by the prohibition prescribed in Article 22(1)(4) of the GDPR. It can entail excluding end-users from granting loans, thus, impacting their consumption habits and life satisfaction indexes. On the other viewpoint, even a decision favouring granting credit

13 See SILVA, Fábio – Credit scoring as an asset for decision making in intelligent decision support systems, Master's Thesis on Computer Science, University of Minho, Braga, 2011, p. 14.

14 See CASTELLUCCIA, Claude; LE MÉTAYE, Daniel – Understanding algorithmic decision-making: Opportunities and challenges, EPRS, 2019, pp. 3-4.

15 See DA SILVA, Frederico Oliveira; DRAZEWSKI, Kasper – Regulating AI to protect the consumer, BEUC Position Paper, 2021, p. 13; SANCHO, Diana – Automated Decision-Making and Article 22 GDPR, Towards a more substantial regime for solely automatic decision-making. In: Algorithms and Law (Martins Ebers & Susana Navas Eds.), 2020, p. 145; WP29 – Guidelines on Automated decision-making and Profiling for the purpose of Regulation 2016/679 (WP25rev.01), adopted on 6 February 2018, p. 8; and FERRETTI, Federico; VANDONE, Daniela - Personal debt in Europe: The EU financial market and consumer insolvency, Cambridge University Press, UK, 2019, pp. 168-170.

16 See ZERILLI, John et. al. – Algorithmic decision-making and the control problem. In: Minds and Machines, vol. 29, no. 4, pp. 556.

produces “legal” effects on borrowers’ status, bounding them to a set of obligations arising from the final agreement relationship¹⁷.

Furthermore, since an AI-based credit scoring system is premised on the fast collection, storage and untraceable analysis of vast amounts of personal data, some privacy concerns have been raised upon discrimination risks¹⁸. Hence, selecting qualitative data sets poses the intricacy of intentional discrimination since ADM may reflect biased human decisions based on factors such as race, gender, or age at a more extensive and quicker scale¹⁹. Even though European policymaking and jurisprudence on personal data protection should be grounded primarily “on its usage and impact, and secondarily on its source”²⁰, both inputs and outputs label sensitive data, following the prohibition laid down in Article 9(1) of the GDPR, accordingly.

In fact, some ML-based models (and, most importantly, each dataset attached to the training, testing and implementation phases) execute hidden-layered fuzzy reasoning. For this particular reason, from a self-determination perspective²¹, it is conceivable to doubt the existence, scope and feasibility of a tailored right to “explanation”, hereinafter deemed as the fictional ‘(EU)-friendly’ or suitable safeguard allegedly enacted thereof in Articles 13(2)(f), 14(2)(g), 15(1)(h), and 22(3), all of which established in the GDPR²².

17 See MORGADO REBELO, Diogo; ANALIDE, Cesar; COVELO DE ABREU, Joana –O Mercado Único Digital e a ‘(Leigo)ritmia’ da Pontuação de Crédito na era da Inteligência Artificial, vol. 2, no. 1, 2020, pp. 37-38;

18 See HURLEY, Mikella; ADEBAYO, Julius - Credit scoring in the era of big data. In: Yale journal of law and technology, vol. 18, 2017, p. 159.

19 See FERRETTI, Federico; VANDONE, Daniela – op. cit., p. 171.

20 Cit. WACHTER, Sandra; MITTELSTADT, Brent - A right to reasonable inferences ... supra, p. 616.

21 The right to self-determination, established under the avant-gard German Federal Constitutional Court in December 1983, circumscribes “the capacity of an individual to determine in principle the disclosure and use of (...) personal data”, cit. ROUVROY, Antoinette; POULLET, Yves - The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In: Reinventing data protection?. Springer, Dordrecht, 2009. pp. 45.

22 See EDWARDS, Lilian; VEALE, Michael – Slave to the algorithm? Why a ‘right to an explanation’ is probably not the remedy you are looking for. In: Duke Law and Technology, vol. 16, no. 1, p. 80-82.

Particularly concerning CWA, Article 18(6)(b) and Recital 48 of the PRCC strengthen the monodisciplinary technophobic tendency of European normative acts on Law and Technology. This EC proposal establishes consumers must be granted the right to “meaningful explanation”. Prior to the agreement, clients of banking institutions in AI-based credit scoring may “request and obtain from the creditor a clear explanation of the assessment of creditworthiness, including on the logic and risks involved in the automated processing of personal data and its significance and effects on the decision”. Recital 39 - vis-à-vis whatever shall be an “adequate explanation” entitled in Article 12 – also asserts that creditors and, where applicable, intermediary joint controllers²³ should adapt how such explanations are given to the particular circumstances and the consumer’s need for assistance, especially considering the consumer’s knowledge. Furthermore, it elucidates, in fine, such explanations should not in itself constitute a personal recommendation²⁴.

First and foremost, if entered into force, it is not clear how such an explanation can be complaint with the dictates of an interpretation as proposed by Article 13(1) of the Proposal for a Regulation of the European Parliament and of the Council, laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021 206 final), of 21 April 2021 (hereinafter, AI Act Proposal)²⁵. From technical to policy solutions, JRC clarified in its 2020 Report that a second approach on explainability would emphasise the most prominent attributes that come into play in credit-related ADM.

23 See European Union FRA – Handbook on European data protection law, Luxembourg: Publications Office of the European Union, 2018, p. 106.

24 See European Commission- Proposal for a Directive of the European Parliament and of the Council on consumer credits (COM(2021) 347 final), of 30 June 2021, p. 21.

25 See European Commission - Proposal for a Regulation of the European Parliament and of the Council, laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021 206 final), of 21 April 2021, p. 50.

Counterfactual explanations²⁶ can undeniably constructively reveal “what could be changed to receive a desired result in the future, based on the current decision-making model”²⁷. Secondly, as Recital 63 of the GDPR pointed out, the way AI operates at the scale of credit-related scoring is also sheltered by an ‘umbrella’ of IP rights, being part of protecting Trade Secrets Directive²⁸. In this regard, on 28th January 2014, the German Federal Court of Justice (Bundesgerichtshof, BGH) ruled that information remits regarding personal data protection only compel data controllers to provide consumers information underlying the general functioning of the software. For instance, disclosing formulas, practices, processes, designs, instruments, patterns, or compilations of financial information is under the protection of banking institutions’ trade secrets²⁹. Hence, although transparency and explainability have become critical worries in governing AI, it is not yet clear for all to perceive what this would mean in terms of legal requirements³⁰.

Amid the upcoming legal pathway, the existing ‘law-by-books’ literature demands that such a right might be accomplished either ex-ante – i.e., offering simple or general information about the system functionality before processing – or ex-post – by providing

26 See WATCHER, Sandra; MITTELSTADT, Brent; RUSSEL, Chris – Counterfactual Explanations without opening the Black Box, Automated Decisions and the GDPR. In: Harvard Law Review, vol. 31, no. 2, p. 843.

27 See HAMON, Ronan; JUNKLEWITZ, Henrik; SANCHEZ, Ignacio – Robustness and Explanation of Artificial Intelligence, From technical to policy solutions, JRC Technical Report, Publications Office of the European Union, Luxembourg, 2020, p. 12., pp. 12-13.

28 See Article 2(1) of the Directive (EU) 2016/943, of the European Parliament and of the Council, of 8 June 2016, on the protection of undisclosed know-how and business information (trade secrets) against unlawful acquisition, use and disclosure, ex vi IGLESIAS, Maria; SHAMUILIA, Sheron; ANDERBERG, Amanda – Intellectual Property and Artificial Intelligence, A literature review, JRC Technical Report, Publications Office of the European Union, Luxembourg, 2019, p. 20.

29 See Bundesgerichtshof, BGH, Böhlinger-Mangold, VI ZR 156/13, 28th January 2014, para 34.

30 See IGLESIAS, Maria; SHAMUILIA, Sheron; ANDERBERG, Amanda – Intellectual Property and Artificial Intelligence, A literature review, JRC Technical Report, Publications Office of the European Union, Luxembourg, 2019, pp. 20-21; and FERRETTI, Federico; VANDONE, Daniela – op. cit., p. 169.

a legible full description of the concrete decision³¹.

Given the debate triggered by the Recital 71³², some legal experts argue the notation “explanation” attempt to encompass the internal state of models, operating at the scale of applications³³. However, the average level of digital illiteracy does not let data subjects fully understand the logic involved - i.e., how the machine follows the rules - regardless of how unaware they might be of the importance and the consequences of such processing. Until now, neither data subjects have sufficient know-how, nor realize the GDPR legal criteria to decide when and within what limits sensitive information about credit applications should be committed to the lack of transparency in the data processing. As a consequence, credit-related candidates or borrowers in the actual state of the art provide uninformed consents³⁴.

4. The Right to Suggestive-Monetization of an IDSS MAS-based classifier

From theory to practice, Fábio Silva’s 2011 IDSS Distributed AI case study already stressed today’s imbroglío of a right to explanation ex-ante at the agent’s level. His work focused on how

31 See WP29 – Guidelines on Automated decision-making and Profiling for the purpose of Regulation 2016/679 ... supra, p. 25; and WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano - Why a right to explanation of automated decision-making does not exist in the general data protection regulation. In: International Data Privacy Law, vol. 7, no. 2, 2017, p. 81.

32 As a matter of principle, the Court of Justice of the European Union (CJEU) states that recitals have not any direct binding effect. See *Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung*, Case 215/88, ECLI:EU:C:1989:331, para 31, p. 2808.

33 See GOODMAN, Bryce; FLAXMAN, Seth – EU Regulations on Algorithmic Decision Making and a Right to an Explanation”. In: ICML Workshop on Human Interpretability in ML, 2016, p. 55.

34 See DA SILVA, Frederico Oliveira; DRAZEWSKI, Kasper – Regulating AI to protect the consumer ... supra, p. 5; FERRETTI, Federico; VANDONE, Daniela - op. cit., p. 168.

and BURRELL, Jenna - How the machine ‘thinks’, Understanding opacity in machine learning algorithms. In: Big Data & Society, vol. 3, no. 1, 2016, p. 4.

the Multi-Agent system³⁵ works out while realigning “interpretability” with the proposal of a right to suggestive counterfactuals³⁶. It exhorts a kind of agonistic practice that brings the data-driven MAS-based solution into lending legal environment while simultaneously bringing it under future-proof Rule of Law³⁷.

Firstly, Artificial Neural Network (ANN) starts training and testing updated classifiers, performing tasks such as DM. Consumers’ profile autonomously drawn up by the Model-based Agents categorizes potential clients in their future creditworthiness condition. When put into practice, the Multilayer Perceptron with a Decision Tree for feature selection strengthens the lawful distinction to the 20 predictors of a given dataset that may be more relevant and not too sensitive for the Decision Agent model³⁸. With a brief overview of the technicity undergone ANN classifications, we conclude that exposing the relations between pieces of information (or knowledge) from inputs to outputs do not have to be explicitly specified. Data subjects will not, in any case, realize what is:

- (1) a feedforward neural net with depth that equals 1;
- (2) a fully 3 inter-layered architecture running through a topology of 20-5-1 nodes in each level; and
- (3) the importance of training, testing and applying the Back-propagation algorithm on inputs to perform predictions with 97.2% accuracy³⁹.

When a customer has its credit denied, the ModelBuilder

35 A software agent refers to an autonomous system that exhibits mentalistic notions of knowledge, beliefs, intention or obligations and has the social ability, reactivity and pro-activeness attributes. See WOLLDRIDGE, Michael; JENNINGS, Nicholas – Intelligent agents: theory and practice. In: *The Knowledge Engineering Review*, 1995, pp. 116-117.

36 See SILVA, Fábio – op. cit. pp. 38-40; and SILVA, Fábio; ANALIDE, Cesar - Information asset analysis: credit scoring and credit suggestion. In: *International Journal of Electronic Business*, 2011, vol. 9, no. 3, pp. 214-215.

37 See HILDEBRANDT, Mireille - Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. In: *Theoretical Inquiries in Law*, vol. 20, no. 1, 2019, p. 107.

38 See SILVA, Fábio; ANALIDE, Cesar – op. cit. p. 210.

39 See idem, p. 211.

applies evolutionary computation, revealing Silva's constructive approach to the current 'black box dilemma' as it is not tangible to the average human being⁴⁰. By design, this genetic scheme provides counterfactual interpretations of which parameters were individually lacking, allowing "consultants from financial institutions to better advise their clients or perform cross selling operations recommending (...) products which improve a client's credit score"⁴¹. To its extent, favourable elucidations are added to the nominal solvency profiles drawn up in classification and learning stages⁴². Especially in the case of a credit refusal, the Suggestion Agent grades a list of possibilities for the missing features to reach more practical and alternative solutions. Those missing features prove to be an advantageous mechanism to meet the explicit requirements and background aims of Article 13(2)(f), Article 14(2)(g), and Article 22, all of the GDPR. Furthermore, since no clients' attributes have to be disclosed, understanding missing features through counterfactual interpretation is less likely to infringe on trade secrets or other data subjects' rights and freedoms.

For a feasible future-proof GDPR landscape, it is essential to avoid the disclosure of knowledge about customers without exact awareness about the effects, thus making consent ineffective. So, national legislators must once and for all perceive data as a real asset. The relative nature of the data sets, according to Recital 4 of the GDPR, cannot perpetuate forever its fundamental nature as a personal right to avoid commoditisation⁴³. Data is the new 'oil' of creditors. It is the data itself, not the programmers anymore, that classifies what happens next in credit with much more precision levels. Consequently, banking institutions shall be obliged to

40 See RUDIN, Cynthia. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. In: *Nature Machine Intelligence*, vol. 1, no. 5, 2019, p. 206.

41 Cit. SILVA, Fábio – op. cit., p. 51.

42 See SILVA, Fábio; ANALIDE, Cesar – *Information Asset Analyses ... supra*, pp. 212-214; and SILVA, Fábio – op. cit. pp. 45-51.

43 See DATOO, Akber - *Data in the post-GDPR world*. In: *Computer Fraud & Security*, vol. 2018, no. 9, 2018, pp. 17-18.

ascertain the duty by which clients would achieve specific transactional and personal advantages for providing missing data. Implicitly, GDPR announces the shift in strength it outlines from production control to commercially driven data analytics and the relative role AI-based techniques play in inferences portrayed within Big Data Analytics⁴⁴.

5. Conclusion

To sum up, our work tries to get AI-based credit scoring in Banking 4.0 back on its 'feet', commoditizing missing attributes provided when credit application is denied. Once again, we conclude that EU Law in books on Data Protection is not yet prius, nor posterius. It is entirely away for AI credit-related workflows, prompting unreasonable hindrances in the is the fascinating era of tech breakthroughs. EU policymaking are far from being considered the world standard-setter for AI Regulation, at least, in what concerns AI-based credit scoring practices. Provisions such as the one established in Article 18(2) of the PPCC exhorts solely a political black boxing legal framework that cannot be put into practice in the actual state of the art. The solution is plain for all to perceive: GDPR proclaims the challenge of shifting the strength it outlines from production control to commercially driven data analytics.

References

AHO, Brett; DUFFIELD, Roberta - Beyond surveillance capitalism, Privacy, regulation and big data in Europe and China. In: *Economy and Society*, vol. 49, no. 2, 2020, pp. 187-212. DOI: <https://doi.org/10.1080/03085147.2019.1690275>.

ANDERSON, Raymond - The credit scoring toolkit: theory and
44 See AHO, Brett; DUFFIELD, Roberta - Beyond surveillance capitalism, Privacy, regulation and big data in Europe and China. In: *Economy and Society*, vol. 49, no. 2, 2020, pp. 102.

practice for retail credit risk management and decision automation. Oxford University Press, 2007. ISBN: 9780199226405.

BIATAT, Viani A. Djeundje, et al. - Enhancing credit scoring with alternative data. In: Expert Systems with Applications, vol. 63, no. 113766, 2021. DOI: <https://doi.org/10.1016/j.eswa.2020.113766>.

BPI; Covington & Burling LLP - Artificial Intelligence Discussion Draft: The future of credit underwriting – Artificial Intelligence and its role in Consumer Credit, 2019. [Accessed 2021-10-02]. Available at <https://bpi.com/artificial-intelligence-discussion-draft/>.

Bundesgerichtshof, BGH, Böhringer-Mangold, VI ZR 156/13, 28th January 2014.

BURRELL, Jenna-How the machine ‘thinks’, Understanding opacity in machine learning algorithms. In: Big Data & Society, vol. 3, no. 1, 2016, pp. 1-12. DOI: <https://doi.org/10.1177/2053951715622512>.

Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung, Case 215/88, ECLI:EU:C:1989:331.

CASTELLUCCIA, Claude; LE MÉTAYE, Daniel – Understanding algorithmic decision-making: Opportunities and challenges, EPRS, 2019, pp. 1-86. [Accessed 2021-10-02]. Available at [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2019\)624261](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)624261).

CHEN, Ting-Hsuan - Do you know your customer? Bank risk assessment based on machine learning. In: Applied Soft Computing, vol. 86, no. 105779, 2020, pp. 1-20. DOI: <https://doi.org/10.1016/j.asoc.2019.105779>.

DA SILVA, Frederico Oliveira; DRAZEWSKI, Kasper – Regulating AI to protect the consumer, BEUC Position Paper, 2021. [Accessed 2021-10-09]. Available at https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf.

DATOO, Akber - Data in the post-GDPR world. In: Computer Fraud & Security, vol. 2018, no. 9, 2018, pp. 17-18. DOI: <https://doi.org/10.1016/j.cfs.2018.09.001>.

org/10.1016/S1361-3723(18)30088-5.

EDWARDS, Lilian; VEALE, Michael – Slave to the algorithm? Why a ‘right to an explanation’ is probably not the remedy you are looking for. In: *Duke Law and Technology*, vol. 16, no. 1, p. 1-84. [Accessed 2021-10-09]. Available at

<https://pureportal.strath.ac.uk/en/publications/slave-to-the-algorithm-why-a-right-to-an-explanation-is-probably->

European Commission- Proposal for a Directive of the European Parliament and of the Council on consumer credits, of 30 June (COM(2021) 347 final). [Accessed 2021-10-10]. Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:347:FIN>.

European Commission - Proposal for a Regulation of the European Parliament and of the Council, laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021) 206 final), of 21 April 2021. [Accessed 2021-10-10]. Available at

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>.

European Union FRA – Handbook on European data protection law, Luxembourg: Publications Office of the European Union, 2018. [Accessed 2021-10-10]. Available at <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>.

FERRETI, Federico - The Never-Ending European Credit Data Mess, BEUC Position Paper, 2017. [Accessed em 2021-09-30]. Available at <https://www.beuc.eu/press-media/news-events/never-ending-credit-data-mess-new-study-out>.

FERRETTI, Federico; VANDONE, Daniela - Personal debt in Europe: The EU financial market and consumer insolvency, Cambridge University Press, UK, 2019. ISBN: 9781108426732.

GOODMAN, Bryce; FLAXMAN, Seth – EU Regulations on Algorithmic Decision Making and a Right to an Explanation”. In:

ICML Workshop on Human Interpretability in ML, 2016, pp. 50-57. DOI: <https://doi.org/10.1609/aimag.v38i3.2741>.

HAMON, Ronan; JUNKLEWITZ, Henrik; SANCHEZ, Ignacio – Robustness and Explanation of Artificial Intelligence, From technical to policy solutions, JRC Technical Report, Publications Office of the European Union, Luxembourg, 2020. ISBN: 9789279146605.

HILDEBRANDT, Mireille - Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. In: Theoretical Inquiries in Law, vol. 20, no. 1, 2019, pp. 83-121. DOI: <https://doi.org/10.1515/til-2019-0004>.

HURLEY, Mikella; ADEBAYO, Julius - Credit scoring in the era of big data. In: Yale journal of law and technology, vol. 18, 2017, pp. 148-216. [Accessed 2021-10-02]. Available at <https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5>.

IGLESIAS, Maria; SHAMUILIA, Sheron; ANDERBERG, Amanda – Intellectual Property and Artificial Intelligence, A literature review, JRC Technical Report, Publications Office of the European Union, Luxembourg, 2019. ISBN 978-92-76-14178- 5.

KAKLAUSKAS, Arturas - Introduction to Intelligent Decision Support Systems. In: Biometric and Intelligent Decision-Making Support, Springer, Cham, 2015, pp. 2-29. DOI: https://doi.org/10.1007/978-3-319-13659-2_1.

LOUZADA, Francisco; ARA, Anderson; FERNANDES, Guilherme, Classification methods applied to credit scoring: Systematic review and overall comparison. In: Surveys in Operations Research and Management Science, 2016, vol. 21, no. 2, pp. 117-134. DOI: <https://doi.org/10.1016/j.sorms.2016.10.001>.

MORGADO REBELO, Diogo; ANALIDE, Cesar; COVELO DE ABREU, Joana – O Mercado Único Digital e a '(Leigo)ritmia' da Pontuação de Crédito na era da Inteligência Artificial, vol. 2, no. 1, 2020, pp. 1-69. [Accessed 2021-10-02]. Available at <https://blook.pt/publications/publication/66689aed966b/>.

ROUVROY, Antoinette; POULLET, Yves - The right to informational

self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In: Reinventing data protection?. Springer, Dordrecht, 2009. pp. 45-76. DOI: https://doi.org/10.1007/978-1-4020-9498-9_2.

RUDIN, Cynthia. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. In: Nature Machine Intelligence, vol. 1, no. 5, 2019, pp. 206-215. DOI: <https://doi.org/10.1038/s42256-019-0048-x>.

SANCHO, Diana – Automated Decision-Making and Article 22 GDPR, Towards a more substantial regime for solely automatic decision-making. In: Algorithms and Law (Martins Ebers & Susana Navas Eds.), 2020, pp. 136-156. ISBN: 97811083424820.

SARTOR, Giovanni – The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, EPRS Study, June 2020, pp. 1-84. [Accessed 2021-10-02]. Available at [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530).

SILVA, Fábio – Credit scoring as an asset for decision making in intelligent decision support systems, Master's Thesis on Computer Science, University of Minho, Braga, 2011, pp. 1-86. [Accessed 2021-10-02]. Available at <http://hdl.handle.net/1822/27891>.

SILVA, Fábio; ANALIDE, Cesar - Information asset analysis: credit scoring and credit suggestion. In: International Journal of Electronic Business, 2011, vol. 9, no. 3, 203-218. DOI: <https://doi.org/10.1504/IJEB.2011.042542>.

THOMAS, Lyn; CROOK, Jonathan; EDELMAN, David - Credit scoring and its applications, Society for industrial and Applied Mathematics, Philadelphia, 2017. ISBN: 9781611974553.

VOJTEK, Martin; KOÂENDA, Evien – Credit-Scoring Methods. In: Czech Journal of Economics and Finance (Finance a uver), Prague, vol. 56, no. 3-4, 2006, pp. 103-167. [Accessed 2021-10-02]. Available at http://journal.fsv.cuni.cz/storage/1050_s_152_167.pdf.

WACHTER, Sandra; MITTELSTADT, Brent - A right to reasonable

inferences: re-thinking data protection law in the age of big data and AI. In: *Columbia Business Law Review*, vol. 2012, no. 2, 2019, pp. 494-620. DOI: <https://doi.org/10.7916/cblr.v2019i2.3424>.

WATCHER, Sandra; MITTELSTADT, Brent; RUSSEL, Chris – Counterfactual Explanations without opening the Black Box, Automated Decisions and the GDPR. In: *Harvard Law Review*, vol. 31, no. 2, pp. 841-886. [Accessed 2021-10-10]. Available at <https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf>.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano – Why a right to explanation of automated decision-making does not exist in the general data protection regulation. In: *International Data Privacy Law*, vol. 7, no. 2, 2017, pp. 76-99. DOI: <https://doi.org/10.1093/idpl/ix005>.

WOLLDRIDGE, Michael; JENNINGS, Nicholas – Intelligent agents: theory and practice. In: *The Knowledge Engineering Review*, 1995, pp. 115-152. DOI: [10.1017 /S0269888900008122](https://doi.org/10.1017/S0269888900008122).

WP29 – Guidelines on Automated decision-making and Profiling for the purpose of Regulation 2016/679 (WP25rev.01), adopted on 6 February 2018, pp. 1-37. [Accessed 2021-10-09]. Available at <https://ec.europa.eu/newsroom/article29/items/612053>.

ZERILLI, John et. al. – Algorithmic decision-making and the control problem. In: *Minds and Machines*, vol. 29, no. 4, pp. 555-578. DOI: <https://doi.org/10.1007/s11023-019-09513-7>.

Biased algorithms: a risky violation of article 14 of the European Convention on Human Rights

Jacqueline Hellman¹

Summary: 1. Introduction; 2. Algorithms and the non-discriminatory principle: an uneasy relationship; 2.1. A brief approach towards the non-discriminatory principle; 2.2. The implications of Article 14 of the European Convention on Human Rights; 2.3. Algorithms that jeopardize Article 14 of the European Convention on Human Rights. 3. Conclusions.

Abstract: Artificial intelligence has been conceived with the aim of having machines developing functions similar to those of the human being. This implies, inter alia, that they must be able to perceive their “environment”. Within this context, we must mention that algorithms constitute an essential element. However, it should be noted that those, on occasions, may promote a different and harmful treatment. This, fundamentally, happens when the aforementioned algorithms are fed by biased data or when they have intrinsic defects in their coding. Being aware about the impact that the use of non-rigorous algorithms has, we will analyze in detail article 14 of the European Convention on Human Rights in order to prevent unlawful discriminatory situations.

Keywords: artificial intelligence; algorithms; biased information; article 14 of the European Convention on Human Rights.

1. Introduction

The beginnings of “Artificial Intelligence” (hereinafter: AI) date back to the fifties of the last century. Specifically, in 1950, Alan Turing wondered if a machine could think². Six years later, John

1 Associate Professor Universidad Europea de Madrid
Jacqueline.hellman@universidadeuropea.es

2 We are referring to the essay entitled “Computational Machine and Intelligence”, published in the 49th issue of Mind magazine. DELGADO, Miguel. “La Inteligencia Artificial. Realidad de un mito moderno”, Discurso de apertura Universidad de Granada, 1996, p. 13.

McCarthy coined the term AI³. In the following decades, the research work carried out in this relatively new and incipient scientific field multiplied. However, it is not possible to extract an unanimously accepted definition of what is to be understood by AI. In any case, taking as a reference the definition provided by Minsky (in 1968) or by Barr and Feigenbamm (in 1981), we see that it is related to the creation of machines that have abilities similar to those of the human being. Thus, we can say that the technological systems that use AI perceive and interact with their “environment” in order to, ultimately, execute or perform tasks efficiently. Moving to a more technical field, we must understand AI as a set of advanced mathematical data processing techniques according to which decisions are made or certain types of problems are solved regarding diverse aspects of our day to day.

Regardless of the different procedures that are currently used in AI, it is crucial to underline the role that algorithms play around this scientific discipline. There is no doubt that they constitute a key aspect, since - constructed as a set of rules that are applied in a systematic⁴ way - they take on the “arduous task” of facing problems or making decisions⁵. In short, AI uses models or algorithmic combinations according to which machines appear to perform functions that were previously reserved for human beings. In this vein, it should be noted that the aforementioned algorithms are fed by data. Furthermore, in some cases, AI uses algorithms that

3 John McCarthy embodied this term in a proposal that he formulated together with Marvin L. Minsky, Nathaniel Rochester and Claude E. Shannon in 1956 on the occasion of the conference that would take place in Dartmouth a year later. The object of the latter revolved around the idea of whether a machine could solve problems in a way similar to that of human beings. This document highlighted the following: “(...) every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it”. Cfr. McCARTHY, John, MINSKY, Marvin, ROCHESTER, Nathaniel and SHANNON, Claude. “A proposal for the Dartmouth Summer Research Project on Artificial Intelligence”, *AI Magazine*, 4, 2006, p. 12.

4 PEÑA MARÍ, Ricardo. *De Euclides a Java: la historia de los algoritmos y de los lenguajes de programación*, Nívola, Madrid, 2006, p. 10

5 DÍAZ LÓPEZ, Ernesto. “Una implementación de la meta-heurística. Optimización en Mallas Variables en la arquitectura CUDA”, *Revista Cubana de Ciencias Informáticas*, 3, 2016, p. 43.

act on the information that the technological system in question has been able to store in order to “learn” and “train”.

In line with the considerations that have been previously made, we must point out - as said before - that these technological systems, which operate through the aforementioned algorithms, have a strong impact on our daily lives. Consequently, it is of interest to focus all our attention on these to the extent that the mathematical information processing techniques on which they operate are capable of generating discriminatory situations. In fact, this is the case when the “learning system” of a machine is articulated by means of biased information. In other words, if an AI system acts (whether intentionally or not) on non-objective data it may likely reinforce stereotypes of a sexist, racist, class character, etc., which are found latent in our society. This situation worsens when we verify that AI is applied to a large field of subjects that come from both the private and public sectors. As an example, we can bring up the decisions made by a public entity when, through the use of the aforementioned technology, it determines who is going to receive a certain help for the acquisition of a home or who is going to obtain an unemployment benefit. Likewise, within the private sphere, we must mention the banking sector, which is characterized by implementing this type of technology according to which it can be determined whether or not a person will receive a loan and, if so, what interests will be applied. Through these simple examples, we appreciate not only that AI is very present, but that it is crucial that the latter is designed in such a way that it does not lead to a discriminatory treatment. Consequently, hereafter, the existing international norms on human rights will be brought up. More specifically, we will examine the European Convention on Human Rights (hereinafter: ECHR) and we will stress the importance of ensuring strict compliance with the international legality.

2. Algorithms and the non-discriminatory principle: an

uneasy relationship

It is clear that AI brings positive advances that justifies the implementation of this type of technology in many and diverse fields⁶. This can be observed when it is used, for example, to detect diseases, organize traffic in a city, grant public aids, etc.⁷ In short, the utility and benefits that advanced technological systems provide - at different levels - are noted. This statement is supported today more solidly than in the past. There is no doubt that during these long months of global crisis motivated by the COVID-19 pandemic the dependence and confidence shown towards technology has increased substantially.

Being aware of the above, we must indicate that AI is capable of generating - on occasions - “perverse” situations that may result in differentiated or unfair treatment. This may happen when algorithms have defects in its coding or when they have been fed by non-neutral information. Taking into account the purpose of our study, we will focus in the last situation that has been mentioned. Consequently, we will analyze what have the supranational rules determined in relation to discriminatory parameters with the aim of identifying and addressing the challenges that a “faulty algorithm” poses.

6 In accordance with the main body of the text, the following statement should be brought up: “The power, scale, and speed of AI systems can improve efficiency and effectiveness in numerous domains, including healthcare, transport, education, and public administration”. Cfr. LESLIE, David, et. al.. “Artificial Intelligence, Human Rights, Democracy, and the rule of law: a primer”, The Council of Europe, 2021, p. 14.

7 In this sense, more examples can be brought up. Thus, Yavuz highlights when he states the following: “Today, artificial intelligence (AI) is widely used in diversified areas. In healthcare, it assists in detecting tumor and cancer, discovering new medicine, and operating surgery. The algorithm of Netflix, YouTube, and Spotify dominate online content consumption and suggest movies, videos, and songs to people. Virtual assistants (Siri and Alexa) ease daily life, web mapping services (Google Maps) forecast the best route; search engines enable the Internet users to find relevant information on the Internet. Many AI applications are so well-integrated in daily life that people do not realize the use of them”. Cfr. YABUZ, Can. “Machine Bias: Artificial Intelligence and Discrimination”, Master Thesis Lund University, 2019, p. 1. Link hereby provided:

<https://lup.lub.lu.se/luur/download?func=downloadFile&recordId=8987035&fileId=8987040>

2.1. A brief approach towards the non-discriminatory principle

At this point of our explanation we must provide a clear idea about what we should understand by discrimination. And, for this reason, we must focus our attention on the content of the applicable international regulation. Consequently, we must highlight the importance of the Universal Declaration of Human Rights insofar as since its adoption, in 1948, “(...) human rights were grounded in a respect for all individuals that derived from our equal status as bearers of inherent human dignity⁸”. It should be noted that, as of the mentioned date not only numerous supranational legal agreements on human rights have proliferated, but all of them have been sponsored and articulated under two essential principles: equality and non-discrimination⁹. Therefore, it is not possible to deny the strong impact displayed by the principle object of our present study. This is confirmed by the Human Rights Committee when it indicates the following: “[n]on-discrimination, together with equality before the law and equal protection of the law without any discrimination, constitute a basic and general principle relating to the protection of human rights¹⁰”. Therefore, we are before an essential principle.

Having clarified the important role that the principle of non-discrimination plays, it is essential to emphasize the way in which it should be interpreted. For this, it is of interest to bring up the definition provided in this regard by the aforementioned Committee

8 Cfr. LATONERO, Mark. “Governing Artificial Intelligence: upholding Human Rights & Dignity”, *Data&Society*, 2020, p. 8.

9 According to what has been explained in the main body of the text, the following should be noted: “Equality and nondiscrimination are foundational to practically every major human rights instrument that has emerged from debate and input from representatives from the world’s nations”. *Ibidem*. P. 9.

10 See the report issued by the Human Rights Committee in 1989 on non-discrimination:
https://www.oursplatform.org/wp-content/uploads/HRI.GEN_.1.Rev_.9Vol.I_GC18_en.pdf

in accordance with the provisions of the International Covenant on Civil and Political Rights:

“(...) the term ‘discrimination’ as used in the Covenant should be understood to imply any distinction, exclusion, restriction or preference which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms¹¹”.

In line with what has been previously commented, it is crucial to emphasize that not every distinction entails discrimination. In short, the principle of equality and non-discrimination, which constitute the two sides of the same coin, should not lead us to the wrong idea that all people should necessarily be treated in the same way. In fact, the Human Rights Committee maintains the following: “the principle of equality sometimes requires States parties to take affirmative action in order to diminish or eliminate conditions which cause or help to perpetuate discrimination prohibited by the Covenant¹²”. All of which leads the latter to argue that: “(...) not every differentiation of treatment will constitute discrimination, if the criteria for such differentiation are reasonable and objective and if the aim is to achieve a purpose which is legitimate under the Covenant¹³”.

Following on from what has been said, when referring to the applicable rules in the European continent, we must take into consideration Article 14 of the ECHR which prohibits all forms of discrimination; however, -due to the judgments issued by the Court located in Strasbourg- we must say that in a similar way to what has been expressed by the Human Rights Committee the differentiation in treatment does not entail always a breach of legality. In other words, the aforementioned prohibition does not imply the impossibility of establishing different deals. This was reflected in the case *Relating*

11 Ibidem.

12 Vid. Supra. Nota 10.

13 Ibidem.

to certain aspects of the laws on the use of languages in education in *Belguim v. Belguim* (1968) according to which it was proclaimed that the violation of the principle of equality can be argued if the distinction does not have an objective or reasonable justification. Likewise, it is of interest to refer to the guide provided by the European Court of Human Rights (hereinafter: ECtHR) on how the aforementioned rule should be interpreted insofar as it, *inter alia*, highlights that the prohibition on discrimination does not have its own entity, but it is linked to the freedoms and rights provided in the aforementioned legal agreement¹⁴.

Be that as it may, the aforementioned elements relating to objectivity and reasonableness become essential when determining whether or not there has been a difference in treatment that implies a violation of the aforementioned legal precept contained in the ECHR. For these purposes, we must bring up the case *Thlimmenos v. Greece* by virtue of which the following was stipulated: “The Court has so far considered that the right under Article 14 not to be discriminated against in the enjoyment of the rights guaranteed under the Convention is violated when States treat differently persons in analogous situations without providing an objective and reasonable justification”. In addition, it adds (in paragraph 44 of the mentioned judgement) that the aforementioned article is also violated when the States, without giving an objective or reasonable justification, do not provide different treatment with respect to people who have significant differences between them. Therefore, it is easy to verify that the spirit of the international and regional regulation regarding the issue hereby addressed is the same. Having clarified main aspects of the referred principle, we will analyze in the next section, concrete aspects of the mentioned regional norm.

14 The mentioned document is hereby provided:

https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf

It must be noted that the ECtHR clarifies that the articulation of the aforementioned precept must not necessarily imply the prior violation of another legal provision.

2.2. The implications of Article 14 of the European Convention on Human Rights

Firstly, we must stress that Article 14 of the ECHR does not provide any definition about what we should understand by discrimination. Fortunately, the court decision issued on *Biao v. Denmark* clarifies much of the issue. Consequently, it is of interest to reproduce paragraph 89 of the latter: “(...) only differences in treatment based on an identifiable characteristic, or “status”, are capable of amounting to discrimination within the meaning of Article 14. Moreover, in order for an issue to arise under Article 14 there must be a difference in the treatment of persons in analogous, or relievingly [sic] similar, situations”. Thus, a discriminatory situation is noticed when people who are in a similar situation are treated differently. In that case, we must point out that we would be facing direct discrimination. All of which forces us to determine what an indirect discrimination consists of. In this context, the aforementioned guide is extremely useful, since it indicates that such situation takes place when a measure produces negative effects in a certain group. Moreover, in accordance with the stipulations of the aforementioned document, this type of discrimination may arise from a neutral norm or a *de facto* situation. In short, it is not necessary to notice a discriminatory intention to conclude that there is a breach of the law.

Within this context, we must bear in mind that the scope of the aforementioned European rule has been expanded through Article 1 of Protocol number 12 as it states that the violation of the principle contained in Article 14 of the ECHR can be concluded in the event of any violation of rights provided for by law. Furthermore, according to *Savez crkava “Riječ života” and others v. Croatia*, it is possible to observe violations beyond what it has been established by the regulations. We see, therefore, that the scope of application of Article 14 of the ECHR is not limited to its literal wording; on the contrary, its effects clearly go beyond to what it has been expressly

stated.

Moving forward on all these issues, we must mention that Article 14 provides a list of reasons according to which it can be determined that a discriminatory situation has taken place. At this point we must emphasize that it does not constitute an exhaustive list. Thus, Gerards maintains that: “Article 14 only mentions the various grounds as examples, perhaps to make clear that the drafters of the provision considered these grounds to constitute the most problematic ones to base decision-making or regulation on¹⁵”. This idea is corroborated by the ECtHR itself when, in innumerable legal proceedings¹⁶, supports its argument on the first paragraph of Article 14 that refers to “any other situation”. In this way, the Court located in Strasbourg encourages a wide scope of application of the aforementioned rule.

After clarifying essential issues on the analyzed topic, it is convenient to return to the idea that was previously expressed: an unequal treatment does not generate a legal breach. As we have already said, this will not happen if we observe the existence of an objective and reasonable justification aimed at legitimizing the difference in treatment at issue. This is, of course, a delicate question. There is no doubt that the ECtHR has spent its time explaining the aforementioned elements, which must be present to justify such an exception. In this sense, the case *Molla Sali v. Greece* proclaimed (in paragraph 135) the following: “a difference of treatment is discriminatory if it has no objective and reasonable justification, that is, if it does not pursue a legitimate aim or if there is not a reasonable relationship of proportionality between the means

15 Cfr. GERARDS, Janneke, “The Discrimination Grounds of Article 14 of the European Convention on Human Rights”, *Human Rights Law Review*, n 13, 2012, p. 104. In line with what has been stated, it is worth noting that most of the judicial pronouncements in which discrimination is observed refer to questions of race, sex and religion; while the rest usually refer to: “(...) situations in which specific social groups typically are not sufficiently represented in and thus protected by the political process”. Cfr. PETERSEN, Niels. “The Principle of Non-discrimination in the European Convention on Human Rights and in EU Fundamental Rights”, *Contemporary Issues in Human Rights*, 2017, p. 134.

16 In this sense, the case charges interest *Clift v. United Kingdom* and, also, *Engel and others v. The Netherlands*.

employed and the aim sought to be realized”. This idea, obviously, appears in other judicial processes¹⁷. In any case, to further clarify this issue, it is convenient to follow the steps recommended in the mentioned guide in order to clarify whether or not we are facing a discriminatory situation:

“When deciding cases of discrimination, the Court will apply the following test: 1. Has there been a difference in treatment of persons in analogous or relevantly similar situations – or a failure to treat differently persons in relevantly different situations? 2. 1. If so, is such difference – or absence of difference – objectively justified? In particular, does it pursue a legitimate aim? 2. Are the means employed reasonably proportionate to the aim pursued?¹⁸”

Consequently, as we have already seen, the ECtHR does not prohibit differences in treatment, as long as the conditions indicated above are met. Taking into account this important premise, we will analyze in our next section concrete situations that are putting at stake the aforementioned principle.

2.3. Algorithms that jeopardize Article 14 of the European Convention on Human Rights

In light of what has been previously explained, we have no doubt that the machines that take advantage of the benefits that AI entails must carry out their functions in accordance with the principle of non-discrimination contained in Article 14 of the ECHR. To better understand the importance of this premise, it is crucial to note that this type of technology operates - as we already anticipated - on previously collected information according to which any kind of bias should be avoided. In relation to this issue we should refer to real situations that have shown the existing collision between algorithms and the mentioned article. In this sense, we must bring up the case of Amazon, the well-known multinational company, that promoted in

¹⁷ According to what is stated in the main body of the text, the case *Fabián v. Hungary* or *Abdulaziz, Cabales y Balkandali v. United Kingdom* are of great interest.

¹⁸ *Vid. Supra.* 14.

2014 a discriminatory treatment as a result of the use of a computer program developed to filter job applications. The controversy arose when it was found that the machine “had been trained” on the basis of male resumes. This meant that men had preference over women. Undoubtedly, the aforementioned program presented a gender bias according to which the latter were unfairly discriminated¹⁹. This case shows that inadequate data “training” implies a great risk. Likewise, the controversy arising from technological devices that have a facial recognition system corroborates this same idea. We are clearly thinking of the unquestionable difficulties that arose when recognizing certain groups, which had huge negative consequences for their members²⁰.

The above incidents show the dangerous challenges posed by the use of algorithms that “work” on inaccurate data insofar as they favor the creation of situations with a high discriminatory potential²¹. Thus, it is essential to bring up Article 14 of the ECHR and point out that although establishing differences does not constitute a problem per se, the controversy clearly breaks out when they do not find a specific basis or justification. Undoubtedly, the aforementioned elements, objectivity and reasonableness, become essential, since in accordance with these we can determine whether or not we are facing a discriminatory situation. Naturally, it is necessary to analyze each one of the situations that generate “suspicions” in order to find out in which way the unequal treatment is taking place. Likewise, it is essential to examine the consequences

19 Information hereby provided: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>

20 Information hereby provided: <https://www.biometricupdate.com/202105/bbc-addresses-facial-recognition-bias-issues-in-new-click-episode>

21 We must not fail to mention the positive aspects that the use of algorithms entails. Thus, the European Agency for Fundamental Rights stipulates, on page 69, the following: “Under certain circumstances and in some areas, using algorithms could positively contribute by reducing bias and stereotyping. Algorithmic data analysis may produce results that could dispel prejudicial attitudes. For example, predictive policing might, in some contexts, lead to more equitable and non-discriminatory policing by reducing reliance on subjective human judgments”. Information hereby provided: <https://eu2020-bmjv-european-way-on-ai.de/storage/documents/FRA-2020-AI-and-fundamental-rights.pdf>

that the difference entails, as well as to examine whether or not there is an adequate justification. Obviously, the person causing the discriminatory treatment must objectively and reasonably prove (if possible) that the situation does not imply a breach of the law. It is therefore clear that the ECHR plays a fundamental role in this area. In short, the aforementioned legal agreement acts as if it were a retaining wall when trying to avoid situations that, at the hands of the AI, could involve a violation of an essential right.

3. Conclusions

As we have already explained, it is clear that there are many benefits that AI brings. However, we must be aware that the use of algorithms in this field can encourage discriminatory situations. Consequently, the principle of non-discrimination contained in - among others - Article 14 of the ECHR plays a very important role. Likewise, the technological revolution in which we find ourselves has given rise to a considerable jurisprudential development around the referred principle. However, we must emphasize that in the view of recent and controversial cases, the existing regulations and the judicial decisions that have been rendered seem to not be enough. Therefore, it is a priority to seek new mechanisms that aim to ensure and protect in a more forceful way the rights that individuals in this framework have. From our point of view, this should include an impulse of additional regulation that should refer to - inter alia - data protection, as well as to promote a greater degree of transparency regarding the way in which machines that use AI work.

Bibliography references:

DELGADO, Miguel. La Inteligencia Artificial. Realidad de un mito moderno. Discurso de apertura Universidad de Granada, p. 7-49, 1996

DÍAZ LÓPEZ, Ernesto. Una implementación de la meta-heurística. Optimización en Mallas Variables en la arquitectura CUDA. Revista Cubana de Ciencias Informáticas, 3, p. 42-56, 2016.

GERARDS, Janneke. The Discrimination Grounds of Article 14 of the European Convention on Human Rights. Human Rights Law Review, n 13, p. 99-124, 2012.

LATONERO, Mark. Governing Artificial Intelligence: upholding Human Rights & Dignity. Data&Society, p. 1-57, 2020.

LESLIE, David, et. al. Artificial Intelligence, Human Rights, Democracy, and the rule of law: a primer, The Council of Europe, p. 1-46, 2021

McCARTHY, John, MINSKY, Marvin, ROCHESTER, Nathaniel and SHANNON, Claude. A proposal for the Dartmouth Summer Research Project on Artificial Intelligence, AI Magazine, 4, p. 2-14, 2006.

PEÑA MARÍ, Ricardo. De Euclides a Java: la historia de los algoritmos y de los lenguajes de programación, Nívola, Madrid, 2006.

PETERSEN, Niels. “The Principle of Non-discrimination in the European Convention on Human Rights and in EU Fundamental Rights”, Contemporary Issues in Human Rights, p. 122-142, 2017.

YABUZ, Can. “Machine Bias: Artificial Intelligence and Discrimination”, Master Thesis Lund University, 2019.

Democracia e Liberdade de Expressão na Era Digital: aplicação de restrições a canais de notícias virtuais como mecanismo de combate à polarização e à desinformação

Democracy and Freedom of Expression in the Digital Era: application of restrictions to virtual news channels as a mechanism to combat polarization and disinformation

Mariana Caroline Pereira Félix¹

Lucas Nogueira Holanda²

Sumário: 1. Introdução; 2. Os desafios da democracia na era das mídias digitais; 3. Contexto das mídias digitais nas eleições presidenciais brasileiras de 2018; 4. A necessidade de cooperação entre o poder público e as mídias digitais na proteção à democracia; 5. Conclusão; 6. Referências.

Resumo: O desenvolvimento da Sociedade da Informação e o uso das mídias sociais traz à tona a necessidade de a Democracia se reinventar para se proteger do crescente aumento de fenômenos como a polarização e a desinformação, potencialmente ampliados pelos algoritmos utilizados nas Mídias Sociais. A pesquisa visa a analisar o contexto das Eleições Presidenciais Brasileiras de 2018, bem como analisar a decisão do TSE que determinou restrições a canais de notícias virtuais conduzidos por apoiadores ao atual Presidente da República do Brasil. A relevância do tema se dá em razão do impactante potencial que as redes sociais dispõem para influenciar as eleições, o que pode acarretar em sérias perturbações à prática democrática. A liberdade de expressão é um direito assegurado a todos, mas que não deve ser utilizado desenfreadamente, encontrando limites constitucionais e democráticos à sua realização. Quanto à metodologia, utiliza-se uma abordagem qualitativa, de caráter explicativo, baseada em fontes bibliográficas e documentais. O potencial de aumento

1 Mestre em Direito pela Universidade Federal do Ceará - UFC. Pós-Graduada em Direito e Processo Tributário pela Universidade de Fortaleza - UNIFOR. Pesquisadora do Grupo Ágora e do Núcleo de Pesquisa em Interpretação e Decisão Judicial - NUPID. Advogada. E-mail: marianapfelig@gmail.com

2 Mestrando em Direito Constitucional pela Universidade Federal do Ceará. Pós-Graduado em Direito e Processo Tributário pela Universidade de Fortaleza. E-mail: lucasholandaadv@gmail.com

da polarização e da desinformação nas mídias digitais é preocupante para a democracia brasileira, bem como a falta de regulamentação legal quanto a essa questão. No entanto, a decisão do TSE foi um importante passo no combate aos efeitos negativos das mídias sociais à democracia, elucubrando a importância de cooperação entre Poder Público e iniciativa privada nessa jornada.

Palavras-Chave: Democracia; Mídias Digitais; Eleições Presidenciais; Polarização; Desinformação.

Abstract: The development of the Information Society and the use of social media brings to light the need for Democracy to reinvent itself to be protected against the growing increase in phenomena such as polarization and misinformation, potentially amplified by the algorithms used in social media. The research aims to analyze the context of the 2018 Brazilian Presidential Elections, as well as to analyze the decision of the TSE that determined restrictions to virtual news channels conducted by supporters of the current President of the Republic of Brazil. The relevance of the theme is due to the impactful potential that social networks have to influence elections, which can cause serious disturbances to democratic practice. Freedom of expression is a right guaranteed to everyone, but it should not be used unbridled, finding constitutional and democratic limits to its realization. As for the methodology, it is used a qualitative approach, of an explanatory nature, based on bibliographical and documental sources. The potential for polarization and misinformation increasing in digital media is a concern for Brazilian democracy, as well as the lack of legal regulation on this issue. However, the TSE's decision was an important step in combating the negative effects of social media on democracy, highlighting the importance of cooperation between the Government and the private sector in this journey.

Keywords: Democracy; Digital Media; Presidential elections; Polarization; Misinformation.

1. Introdução

As mídias digitais garantem que a informação circule com mais agilidade, proporcionando mais acesso à informação e amplitude na participação democrática. No entanto, algumas particularidades no funcionamento das redes e mídias digitais podem gerar uma exposição seletiva do conteúdo político, criando um ambiente propício para o aumento da polarização e da desinformação. Esses

fenômenos são prejudiciais à democracia, um regime de governo fundamentado na pluralidade, na tolerância e no dissenso.

A pesquisa versa sobre o cenário das Eleições Presidenciais brasileiras de 2018, buscando constatar se houve ou não indícios da ocorrência de polarização e desinformação na campanha eleitoral do atual Presidente eleito, Jair Bolsonaro, bem como entender as razões que levaram o Tribunal Superior Eleitoral (TSE) a determinar restrições por parte de determinadas Mídias Digitais a canais de informação de apoiadores do Presidente.

Será realizada uma abordagem qualitativa, de cunho explicativo, baseada em fontes bibliográficas e documentais. Na primeira seção analisa-se a polarização e a desinformação como empecilhos ao sucesso da democracia nas mídias digitais. Na segunda seção observa-se o contexto das Eleições Presidenciais de 2018 com intuito de investigar se houve ocorrência desses dois fenômenos. Por fim, na terceira seção, examina-se a decisão do TSE e suas repercussões, bem como sua importância em um contexto de democracia digital.

2. Os desafios da democracia na era das mídias digitais

Sendo um modelo de governo marcado pela participação popular e pela liberdade de expressão, a democracia tem sido desde então uma das maiores conquistas da humanidade, desde o tempo da Grécia Antiga até o seu apogeu no Século XX, quando o número de nações de regime democrático mais cresceu. Contudo, a história da democracia sempre foi repleta de obstáculos impostos à sua sobrevivência. Com o desenvolvimento da Sociedade da Informação, os desafios adquiriram uma faceta virtual, decorrentes da Revolução Digital e das mudanças na forma de circulação das informações, especialmente via mídias digitais.

Quando se trata de mídias digitais, pode-se incluir redes sociais como Facebook e Instagram, espaços virtuais de exposições

de vídeos como Youtube e Twitch, ou até mesmo aplicativos de mensagem privada, como o Whats App. Essas mídias garantem mais praticidade e velocidade na circulação de informações, pois não há mais a dependência de um veículo de imprensa que publique periódicos impressos em locais restritos para que a informação chegue a cada cidadão. Isso, entretanto, nem sempre traz efeitos positivos.

Em razão do largo pool de notícias circulando na internet, é natural que usuários procurem notícias que mais os agradam, provenientes de canais que usam metodologias de publicidade que lhe são mais aprazíveis. Dessa forma, muitas das mídias sociais se utilizam de algoritmos para identificar as preferências do usuário e encaminhar-lhe conteúdo similar ao tipo de informação que ele costuma consumir, o que resulta na criação de bolhas informativas.

No Facebook e no Youtube, por exemplo, quando o usuário marca um conteúdo com um like, ou “curtida” no português do Brasil, está sinalizando que aprecia aquele conteúdo moderadamente, enquanto um share, ou compartilhamento, sinaliza que ele aprecia ainda mais aquele conteúdo³. Dessa forma, o algoritmo passa a destacar mais conteúdos provenientes do mesmo canal de informação ou de canais similares para o usuário, personalizando o seu feed de notícias. Trata-se, portanto, de um filtro personalizado que não é controlado pelo usuário⁴.

Quando se trata de mero entretenimento, esses algoritmos são convenientes para afastar notícias consideradas “chatas” pelo usuário, afinal nem todos os conteúdos lhe interessam. No entanto, quando se trata do debate político, segundo a pesquisa de opinião

3 BESSI, A. et al. Users Polarization on Facebook and Youtube. PlosOne, 2016, p. 3.

4 KISCHINHEVSKY, M.; FRAGA, R. O jornalismo refém do algoritmo do Facebook: desafios regulatórios para a circulação de notícias numa sociedade de plataformas. Fronteiras – Estudos Midiáticos, v. 22, n. 2, 2020, p. 130.

do Instituto DataSenado⁵, 45% dos cidadãos consomem essas notícias e tem posicionamento político influenciado pelas redes sociais, de maneira que a filtragem destas informações pode reter conteúdos importantes ao dissenso democrático, favorecendo a polarização política.

A polarização é marcada pela forte rivalidade entre segmentos políticos, com a substituição de debates racionais entre posicionamentos divergentes pelo uso de uma argumentação moral e binária⁶. Trata-se de um fenômeno que já existia antes das redes sociais e que dificilmente deixará de existir. No entanto, há indícios de que os algoritmos e a filtragem na exposição de conteúdos digitais ampliam a polarização, o que pode refletir numa ameaça à democracia.

Em termos práticos, quando se tem, por exemplo, um eleitor alinhado a pensamentos mais conservadores, este vai preferir conteúdos políticos de opinião conservadora, e o algoritmo tende a filtrar opiniões mais progressistas, consideradas “de esquerda”, ocasionando um abismo ideológico entre pessoas de diferentes posicionamentos políticos. O usuário passa a ver mais ideias que compactuam com as suas e menos ideias que divergem das suas, ficando preso numa “bolha de opinião”⁷, fenômeno que favorece também a proliferação das “câmaras de eco”, comunidades polarizadas marcadas pela pouca variedade no tipo de conteúdo consumido⁸.

5 BAPTISTA, Rodrigo. Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado. Agência Senado, 12 de dezembro de 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/12/12/redes-sociais-influenciam-voto-de-45-da-populacao-indica-pesquisa-do-datasenado>. Acesso em: 11 set. 2021.

6 MACHADO, J. MISKOLCI, R. Das Jornadas De Junho À Cruzada Moral: O Papel Das Redes Sociais Na Polarização Política Brasileira. *Sociologia e Antropologia*, v. 9, n. 3, 2019, p. 958

7 MACHADO, J. MISKOLCI, R. Das Jornadas De Junho À Cruzada Moral: O Papel Das Redes Sociais Na Polarização Política Brasileira. *Sociologia e Antropologia*, v. 9, n. 3, 2019, p. 955.

8 DEL VICARIO, M. et al. Echo Chambers: Emotional Contagion and Group Polarization on Facebook. *Scientific Reports*, p. 2.

De acordo com Bessi⁹, algoritmos são o principal determinante no crescente efeito polarizador das redes sociais, assim como Del Vicario¹⁰ afirma que o ambiente virtual do Facebook é propício para emergência das câmaras de eco. Ademais, a polarização não é o único problema potencialmente ampliado pelas bolhas de opinião e as câmaras de eco. Outro problema tão prejudicial à democracia quanto à polarização, é a desinformação, prática que a Carta Portuguesa de Direitos Humanos na Era Digital¹¹ define como:

[...] Toda a narrativa comprovadamente falsa ou enganadora criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que seja suscetível de causar um prejuízo público, nomeadamente ameaça aos processos políticos democráticos, aos processos de elaboração de políticas públicas e a bens públicos.

A desinformação, consequência da propagação de Fake News, assim como a polarização, está presente na história da humanidade desde o princípio. Entretanto, tendo em vista que a Internet se trata de um ambiente de rápida circulação de notícias, é evidente que as falsas notícias também circularão mais rápido. Antes da explosão das mídias digitais, as notícias eram propagadas apenas por veículos oficiais fortemente regulamentados pelo Estado, contudo, as mídias garantiram que qualquer notícia, independentemente da fonte, possa ganhar repercussão e isso impacta tanto na clareza quanto à verdade fática.

Uma vez dentro de uma câmara de eco, a desinformação encontra um ambiente propício para crescer e alcançar cada vez mais usuários, pois os que acessam esse tipo de conteúdo político demonstram preferências por pontos de vista similares ao seu, muitas vezes sem verificar a veracidade das informações.

Em análise das notícias falsas compartilhadas no âmbito das

9 BESSI, A. et al. Users Polarization on Facebook and Youtube. PlosOne, 2016, p. 7.

10 DEL VICARIO, M. et al. Echo Chambers: Emotional Contagion and Group Polarization on Facebook. Scientific Reports, p. 7.

11 PORTUGAL. Lei nº 27/2021. Carta Portuguesa dos Direitos Humanos na Era Digital. 1ª Série, n. 95.

eleições presidenciais brasileiras de 2018, Jardelino¹² aponta que as Fake News têm potencial para interferir nas eleições. Em meio às bolhas de opinião, o nível de engajamento das notícias falsas pode se tornar tão alto a ponto de não adiantar “desmentir” as notícias, uma vez que a credibilidade pode continuar a depender da influência do interlocutor e da vulnerabilidade do receptor.

Com as mídias sociais é possível ter “[...] mentiras específicas, pensadas para audiências específicas em nível pessoal, graças aos algoritmos que estamos constantemente alimentando em nosso uso diário da internet e das mídias sociais”¹³. Vê-se uma adaptação do discurso à plateia, e quem mais perde com isso é o regime democrático. A ligação entre polarização política e desinformação está no fato de que notícias falsas geralmente possuem um apelo emocional, um engajamento por meio do ódio ao lado político oposto¹⁴.

Se torna inviável a um eleitor escolher corretamente seus representantes, quando sua opinião é maculada por fatos forjados. Inviabilizada a democracia, é inviabilizada também a liberdade de expressão, instituto essencial para o sucesso das mídias digitais no mundo, de forma que cabe também às grandes empresas de redes digitais a responsabilidade pelo combate à polarização e à desinformação.

3. Contexto das mídias digitais nas eleições presidenciais brasileiras de 2018

Em 2018, o Brasil passava por um forte pessimismo político, em virtude de diversos escândalos de corrupção trazidos à tona, que ocorreram na égide do Governo do Partido dos Trabalhadores

12 JARDELINO, F. et al. A proliferação das fake news nas eleições brasileiras de 2018. *Comunicação Pública*, v. 15, n. 28, 2020, p. 17.

13 PARDO, M. Democracia Hackeada: hacking, legitimidade e opinião pública. *Tensões Mundiais*, v. 16, n. 30, 2020, p. 163

14 SANTOS, G.F. Social media, disinformation, and regulation of the electoral process: a study based on 2018 Brazilian election experience. *Investigações Constitucionais*, v. 7, n. 2, 2020, p. 436.

(PT), de 2002 a 2016, quando ocorreu o impeachment da então presidente Dilma Rousseff, que estava na presidência desde de 2010, ocasião em que sucedeu o ex-presidente Lula. Em virtude de alguns equívocos na política econômica e financeira, bem como a associação do partido a pautas esquerdistas, tornou-se crescente a insatisfação com o Governo em diversos grupos sociais de caráter conservador.

Assim, em 2018, o então deputado federal Jair Bolsonaro decidiu lançar sua candidatura a Presidente da República, concorrendo com diversos outros candidatos, dentre eles, Fernando Haddad, apoiado pelos ex-presidentes petistas, e Ciro Gomes, o mais forte nome da terceira via. Até então, Bolsonaro fazia parte de um partido de pouca representatividade no cenário político brasileiro, mas realizou a sua campanha eleitoral essencialmente pela Internet, com mídias digitais, se utilizando muito pouco da mídia tradicional e até mesmo fazendo diversas críticas a esta.

Ao final do 1º turno das eleições, Bolsonaro ficou em primeiro lugar com 46%, Haddad com 29% e Ciro Gomes com apenas 12% dos votos¹⁵. No entanto, segundo pesquisa do Ibope realizada antes do resultado no 1º turno, Bolsonaro, que liderava nas pesquisas, tinha a rejeição altíssima de 44%, assim como Haddad, que tinha 38%, ao passo que o terceiro, Ciro Gomes, tinha apenas 18% de rejeição¹⁶.

No 2º turno das eleições, disputado entre Bolsonaro e Haddad, houve uma vitória de Bolsonaro de 57% a 47% sobre Haddad¹⁷, contudo, a pesquisa indicava que, se Ciro Gomes estivesse no

15 BRASIL. Tribunal Superior Eleitoral. Divulgação de Resultado de Eleições, online. Disponível em: < <http://divulga.tse.jus.br/oficial/index.html>> Acesso em 28 ago. 2021.

16 ELEIÇÕES 2018. Pesquisa Ibope para presidente: Bolsonaro, 31%; Haddad, 21%; Ciro, 11%; Alckmin, 8%; Marina, 4%, online, G1, 01 out. 2018. Disponível em: < <https://g1.globo.com/politica/eleicoes/2018/noticia/2018/10/01/pesquisa-ibope-para-presidente-bolsonaro-31-haddad-21-ciro-11-alckmin-8-marina-4.ghtml>> Acesso em 28 ago. 2021.

17 BRASIL. Tribunal Superior Eleitoral. Divulgação de Resultado de Eleições, online. Disponível em: < <http://divulga.tse.jus.br/oficial/index.html>> Acesso em 28 ago. 2021.

segundo turno, tanto Bolsonaro quanto Haddad perderiam¹⁸. Esses resultados indicam claramente que os altos percentuais de Bolsonaro e Haddad se deram mais por ódio dos eleitores ao candidato concorrente do que identificação com as propostas do próprio candidato apoiado, demonstrando uma nítida polarização nas eleições de 2018.

Segundo Reis¹⁹, fazendo uma análise do Youtube, os seguidores de Bolsonaro ganharam muito mais espaço da mídia social que os de outros candidatos, mas foi com uso indevido da rede, o que não contribui com o necessário esclarecimento sobre diferentes posições políticas. A campanha de Jair Bolsonaro de 2018 foi marcada pela divulgação de notícias falsas, principalmente a notícia de que teria havido fraude nas urnas eleitorais a seu desfavor, apesar de sua vitória; a notícia de que Haddad havia distribuído material pornográfico, vulgo “kit gay”, para crianças em escolas públicas e a notícia de que a vice da chapa de Haddad, Manuela D’Ávila teria declarado que Jesus era um travesti, afrontando a comunidade religiosa. Houve prova posterior de que todas as notícias eram falsas²⁰.

Em pesquisa realizada pelo Instituto Reuters²¹, em parceria com a Universidade de Oxford, o percentual de desconfiança de notícias no Brasil em 2019 era de 85%, o maior dentre todos os países analisados na pesquisa, em comparação com alto percentual de 67% nos Estados Unidos e 38% na Alemanha. Em

18 ELEIÇÕES 2018. Pesquisa Ibope para presidente: Bolsonaro, 31%; Haddad, 21%; Ciro, 11%; Alckmin, 8%; Marina, 4%, online, G1, 01 out. 2018. Disponível em: < <https://g1.globo.com/politica/eleicoes/2018/noticia/2018/10/01/pesquisa-ibope-para-presidente-bolsonaro-31-haddad-21-ciro-11-alckmin-8-marina-4.ghtml>> Acesso em 28 ago. 2021.

19 REIS, R. et al. A conveniência dos algoritmos: o papel do YouTube nas eleições brasileiras de 2018. *Compólitica*, v. 10, 2020, p. 55.

20 JARDELINO, F. et al. A proliferação das fake news nas eleições brasileiras de 2018. *Comunicação Pública*, v. 15, n. 28, 2020, p. 2-6.

21 NEWMAN, N. et al. Reuters Institute Digital News Report 2019, online. Disponível em < <https://www.digitalnewsreport.org/survey/2019/overview-key-findings-2019/>> Acesso 28 ago. 2021.

2021, o percentual foi 82%²².

Dessa forma, a ascensão do atual presidente na política foi marcada pelo uso de mídias digitais, mas não necessariamente pelo uso correto e devido. A polarização e a desinformação, fortalecidas por estratégias bolsonaristas, foram muito fortes na campanha eleitoral de 2018, e isso enfraquece a democracia, e fragiliza o processo eleitoral.

Dentre as notícias falsas destacadas, o presidente ainda segue com a alegação de que houve fraude nas eleições, apesar de sua vitória, e defende a instituição de voto impresso e auditável, posicionamento reforçado por diversos canais de comunicação digital favoráveis ao governo, mas que configura um verdadeiro retrocesso eleitoral ao Brasil.

No entanto, muitos desses canais foram punidos pelo Tribunal Superior Eleitoral (TSE) em decisão proferida no Inquérito Administrativo nº 0600371-71.2021.6.00.0000 no dia 16 de agosto de 2021, que determinou a suspensão de repasses de valores oriundos de monetização, pagamento de publicidades, inscrição de apoiadores, bem como a desabilitação dos algoritmos que fortalecem tais canais de informação especificamente por parte de mídias sociais como Youtube, Twitch, Twitter, Instagram e Facebook²³.

4. A necessidade de cooperação entre o poder público e as mídias digitais na proteção à democracia

No Inquérito Administrativo supramencionado, a Polícia Federal brasileira apontou diversos canais de notícias que fariam parte de uma rede de divulgação de informações falsas. Em decorrência dos algoritmos das mídias sociais, sempre que uma informação

22 NEWMAN, N. et al. Reuters Institute Digital News Report 2021, online. Disponível em < https://reutersinstitute.politics.ox.ac.uk/sites/default/files/20216/Digital_News_Report_2021_FINAL.pdf> Acesso 28 ago. 2021.

23 BRASIL. Tribunal Superior Eleitoral. Inquérito Administrativo nº 0600371-71.2021.6.00.0000. Brasília, Distrito Federal, 16 ago. 2021.

falsa era contribuída, outra informação falsa de conteúdo similar era direcionada ao usuário, fortalecendo assim a desinformação e a polarização, conforme se constata em relato policial:

No evento citado, identifica-se um processo de dupla sustentação: os canais que repercutem as insinuações ganham com o número de visualizações geradoras da monetização; de outro lado, fortalece-se a narrativa do emissor pela multiplicidade de canais que reiteram a mensagem. Além disso, há os canais que se realimentam mutuamente com difusões de outros canais (ex. lives), ampliando o lucro com a monetização. Quanto mais polêmica e afrontosa às instituições for a mensagem, maior o impacto no número de visualizações e doações, reverberando na quantidade de canais e no alcance do maior número de pessoas, aumentando a polarização e gerando instabilidade por alimentar a suspeição do processo eleitoral, ao mesmo tempo que promove a antecipação da campanha de 2022 por meio das redes sociais (grifo nosso)²⁴.

A decisão reporta uma atuação sistemática para conferir descrédito ao sistema eleitoral brasileiro por meio de notícias falsas, sem sequer indicação de fonte, gerando uma movimentação perigosa para a democracia. Uma medida rigorosa que coibiria o ataque à democracia seria a censura desses canais, mas isso atentaria contra a liberdade de expressão.

O Tribunal, contudo, constata que os canais de informação que participam desta rede lucram com os ataques ao sistema eleitoral, em razão da monetização dos vídeos, bem como de repasses financeiros em decorrência dos anúncios publicitários. A Justiça Eleitoral, em vez de tentar censurar os canais de informação, apenas intimou as empresas por trás das mídias sociais ordenando a desmonetização dos vídeos e destinação de eventuais repasses financeiros para uma conta judicial vinculada, à qual os canais não tinham acesso, ordenando ainda a desabilitação de sugestão desses canais por meio dos algoritmos. O conteúdo falso continuou na Internet para quem desejasse consultar, contudo, desmonetização diminuiu consideravelmente o seu alcance, impedindo a desinformação de se propagar como antes.

24 BRASIL. Tribunal Superior Eleitoral. Inquérito Administrativo nº 0600371-71.2021.6.00.0000. Brasília, Distrito Federal, 16 ago. 2021.

Seria talvez uma medida arbitrária, se não fosse esse também o interesse das mídias sociais. O próprio Facebook já agiu em 2018 para retirar do ar páginas de apoiadores de Bolsonaro que promoviam polarização e desinformação sem a necessidade de uma ordem judicial²⁵, o que demonstra o interesse da rede em combater práticas danosas à democracia. No momento, o Youtube já anunciou que cumpriria a decisão²⁶.

Ao contrário de Portugal, o Brasil ainda não tem uma legislação específica para o combate à desinformação, mas o Senado Federal já aprovou Projeto de Lei²⁷ com esse objetivo, estando pendente de aprovação na Câmara dos Deputados. A decisão representou um primeiro passo no caminho para regulamentação do uso de mídias digitais e um possível indício de cooperação do Poder Público e das mídias sociais na proteção da democracia.

5. Considerações finais

A polarização e a desinformação são fenômenos extremamente danosos para o exercício da democracia, uma vez que fortalecem o discurso autoritário, que normalmente se disfarça de conservador. As mídias digitais não são a causa direta desses fenômenos, contudo, o ambiente virtual e seus algoritmos fornecem uma visão customizada da realidade e criam ambientes propícios para a propagação de Fake News.

As eleições brasileiras de 2018 foram marcadas pelo aumento no uso das mídias digitais, mas o foram também pelas notícias

25 CANAVILHA, J. et al. Conteúdos virais no facebook: estudo de caso na pré-campanha das eleições presidenciais brasileiras de 2018. *Brazilian Journal*, v. 15, n. 3, 2019, p. 615.

26 ALVES, Aluisio. YouTube suspends payments to Brazilian accounts over election disinformation. Reuters, 26 ago. 2021. Disponível em: < <https://www.reuters.com/world/americas/youtube-suspends-payments-brazilian-accounts-over-election-disinformation-2021-08-27/>> Acesso: 12 set. 2021.

27 BRASIL. Senado Federal. Projeto de Lei nº 2630 de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em < <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>> Acesso: 12 set. 2021

falsas e pelo aumento da polarização, principalmente por parte do candidato vencedor, o atual presidente Jair Bolsonaro. Não se pretendeu por meio desta pesquisa deslegitimar a vitória do Presidente, contudo, ataques à lisura do sistema eleitoral são preocupantes, não podendo o Poder Judiciário se abster de conter a proliferação de acusações infundadas. Tal desconfiança pode inclusive incentivar ou legitimar eventual manobra política antidemocrática se não for contida a tempo.

A retirada do ar de canais que fortalecem a polarização por meio do discurso de ódio ou que contribuem com a divulgação de desinformação pode ser interpretada como censura e violação à liberdade de expressão. Todavia, a desmonetização dos canais e inviabilização dos repasses financeiros pelas mídias digitais é uma medida eficaz para enfraquecer as tentativas de polarização e desinformação.

A falta de regulamentação de direitos digitais no Brasil ainda é preocupante, mas a decisão do TSE destacou a possibilidade de uma cooperação entre as mídias digitais, que não desejam ser veículo de conteúdo descredibilizado, e o Poder Público, que tem o dever de investigar e apurar veracidade de informações que tratam de assuntos tão sérios, como fraudes no sistema eleitoral brasileiro.

6. Referências

ALVES, Aluisio. YouTube suspends payments to Brazilian accounts over election disinformation. Reuters, 26 ago. 2021. Disponível em: < <https://www.reuters.com/world/americas/youtube-suspends-payments-brazilian-accounts-over-election-disinformation-2021-08-27/>> Acesso: 12 set. 2021.

BAPTISTA, Rodrigo. Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado. Agência Senado, 12 de dezembro de 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/12/12/redes-sociais-influenciam-voto-de-45-da-populacao-indica-pesquisa-do-datasenado>. Acesso em:

11 set. 2021.

BESSI, A. et al. Users Polarization on Facebook and Youtube. PlosOne, 2016, p. 7.

BRASIL. Tribunal Superior Eleitoral. Inquérito Administrativo nº 0600371-71.2021.6.00.0000. Brasília, Distrito Federal, 16 ago. 2021.

BRASIL. Tribunal Superior Eleitoral. Divulgação de Resultado de Eleições, online. Disponível em: < <http://divulga.tse.jus.br/oficial/index.html>> Acesso em 28 ago. 2021.

BRASIL. Senado Federal. Projeto de Lei nº 2630 de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em < <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>> Acesso: 12 set. 2021

CANAVILHA, J. et al. Conteúdos virais no facebook: estudo de caso na pré-campanha das eleições presidenciais brasileiras de 2018. Brazilian Journal, v. 15, n. 3, 2019, p. 615.

DEL VICARIO, M. et al. Echo Chambers: Emotional Contagion and Group Polarization on Facebook. Scientific Reports, p. 2.

ELEIÇÕES 2018. Pesquisa Ibope para presidente: Bolsonaro, 31%; Haddad, 21%; Ciro, 11%; Alckmin, 8%; Marina, 4%, online, G1, 01 out. 2018. Disponível em: < <https://g1.globo.com/politica/eleicoes/2018/noticia/2018/10/01/pesquisa-ibope-para-presidente-bolsonaro-31-haddad-21-ciro-11-alckmin-8-marina-4.ghtml>> Acesso em 28 ago. 2021.

JARDELINO, F. et al. A proliferação das fake news nas eleições brasileiras de 2018. Comunicação Pública, v. 15, n. 28, 2020, p. 2-6.

KISCHINHEVSKY, M.; FRAGA, R. O jornalismo refém do algoritmo do Facebook: desafios regulatórios para a circulação de notícias numa sociedade de plataformas. Fronteiras – Estudos Midiáticos, v. 22, n. 2, 2020, p. 130.

MACHADO, J. MISKOLCI, R. Das Jornadas De Junho À Cruzada Moral: O Papel Das Redes Sociais Na Polarização Política Brasileira. *Sociologia e Antropologia*, v. 9, n. 3, 2019, p. 955.

NEWMAN, N. et al. Reuters Institute Digital News Report 2019, online. Disponível em < <https://www.digitalnewsreport.org/survey/2019/overview-key-findings-2019/>> Acesso 28 ago. 2021.

NEWMAN, N. et al. Reuters Institute Digital News Report 2021, online. Disponível em https://reutersinstitute.politics.ox.ac.uk/sites/default/files/20216/Digital_News_Report_2021_FINAL.pdf/. Acesso 28 ago. 2021.

PARDO, M. Democracia Hackeada: hacking, legitimidade e opinião pública. *Tensões Mundiais*, v. 16, n. 30, 2020, p. 163.

PORTUGAL. Lei nº 27/2021. Carta Portuguesa dos Direitos Humanos na Era Digital. *Diário da República*, 1ª Série, n. 95, 17 mai. 2021.

REIS, R. et al. A conveniência dos algoritmos: o papel do YouTube nas eleições brasileiras de 2018. *Compólitica*, v. 10, 2020, p. 55.

SANTOS, G.F. Social media, disinformation, and regulation of the electoral process: a study based on 2018 Brazilian election experience. *Investigações Constitucionais*, v. 7, n. 2, 2020, p. 429-436.

Os riscos da inteligência artificial

The Risks of Artificial Intelligence

Ana Isabel Guerra¹

Patrícia Anjos Azevedo²

Sumário: 1. Introdução. 2. A Inteligência Artificial enquanto fator de desenvolvimento. 3. Custos e especialização associada à utilização da Inteligência Artificial. 4. A ameaça à empregabilidade provocada pela excessiva utilização da Inteligência Artificial. 5. Questões Éticas e Sociais da Utilização da Inteligência Artificial. 6. Conclusões.

Resumo: Apesar dos inúmeros benefícios que a inteligência artificial traz para o desenvolvimento socio económico de qualquer sociedade moderna, a sua utilização excessiva pode comportar inúmeros riscos, que não podem, de modo algum, ser esquecidos, atenta a gravidade das consequências que poderão trazer a nível individual, organizacional e societário. O custo elevado da manutenção das máquinas que utilizam inteligência artificial e a alta especialização que exigem também são uma grande desvantagem. Existem também inúmeras questões éticas que a sua utilização acarreta, tanto para os humanos, como para alguns, para as próprias máquinas. Neste domínio, convém não esquecer que por mais sistemas de inteligência que as máquinas possuam, essa inteligência é sempre artificial e deriva do poder de criação da mente humana que é única e inigualável nas suas características. O ser humano deverá fazer uma utilização responsável e assertiva deste tipo de inteligência no seu quotidiano, de modo a que os modelos e algoritmos utilizados na Inteligência Artificial não suplantem o mercado financeiro, dominando-o através da manipulação dos grandes grupos empresariais, nem sem utilizada como arma de guerra, através do seu mau uso, ou uso ofensivo. Coloca-se também a questão de saber se as máquinas têm direitos. A verdade é que, por muito importantes que sejam os mecanismos de Inteligência Artificial, defendemos que os dispositivos aqui em causa não

1 Prof.^a Adjunta Convidada na Escola Superior de Tecnologia e Gestão do Politécnico do Porto e Professora Auxiliar da Licenciatura em Direito da Universidade Portucalense. Membro Colaborador do JusGov -FCT- E-Tec no Centro de Investigação em Justiça e Governação da Universidade do Minho. Endereço eletrónico do autor: aimg@estg.ipp.pt e ana.guerra@mail.upt.pt.

2 Prof.^a Adjunta Convidada na Escola Superior de Tecnologia e Gestão do Politécnico do Porto. Membro integrado do CIICESI/P. Porto. Membro colaborador do Instituto Jurídico Portucalense. Endereço eletrónico do autor: pamv@estg.ipp.pt .

podem, de modo algum, ser equiparados a humanos naquilo a que aos seus direitos diz respeito.

Palavras-chave: Inteligência artificial; Tecnologia Emergente; Riscos; Ética; Robots.

Abstract: Despite the numerous benefits that artificial intelligence brings to the socio-economic development of any modern society, its excessive use can entail numerous risks, which cannot, in any way, be forgotten, given the seriousness of the consequences that may bring to individual, organizational and societal level. The high maintenance cost of machines that use artificial intelligence and the high specialization they require are also a major disadvantage. There are also numerous ethical issues that its use entails, both for humans and for some, for the machines themselves. In this domain, it should not be forgotten that no matter how many intelligence systems machines have, this intelligence is always artificial and derives from the creative power of the human mind, which is unique and unparalleled in its characteristics. Human beings should make responsible and assertive use of this type of intelligence in their daily lives, so that the models and algorithms used in Artificial Intelligence do not supplant the financial market, dominating it through the manipulation of large business groups, even without being used as a weapon of war, through its misuse, or offensive use. There is also the question of whether machines have rights. The truth is that, no matter how important the Artificial Intelligence mechanisms are, we defend that the devices in question here cannot, in any way, be equated with human beings as far as their rights are concerned.

Keywords: Artificial intelligence; Emerging Technology; Risks; Ethic; Robots.

1. Introdução

Quando falamos em inteligência artificial, devemos desde logo procurar uma definição abrangente daquilo que a mesma significa, uma vez que esta é passível de se materializar num qualquer dispositivo tecnológico que pode ser usado e aplicado em inúmeras áreas como a indústria, a saúde, nas plataformas de gestão de negócios, na venda a retalho, nas escolas, no campo militar, dos transportes e em crescendo em cada vez mais áreas do nosso quotidiano³.

3 Neste sentido vide Christoph, Bartneck et al., An Introduction to Ethics in Robotics and AI, Springer, 2021, Switzerland.

Os variadíssimos dispositivos tecnológicos na qual é aplicada este tipo de inteligência reúnem de forma multidisciplinar contributos informáticos e matemáticos que se dedicam a reproduzir capacidades cognitivas humanas para tratar dados, otimizar procedimentos, corrigir erros, fazer mecanicamente objetos com precisão, fazer raciocínios e resolver problemas baseados em modelos e algoritmos próprios. Devemos também ter em consideração que o conceito de inteligência artificial é um conceito que está em constante evolução consoante o surgimento de novos dispositivos em que seja utilizada este tipo de inteligência⁴.

Atendência e o nível de crescimento de utilização de dispositivos tecnológicos movidos a inteligência artificial é indicativo de que a curto/médio prazo a inteligência artificial possa começar a ser utilizada de forma massiva, o que apesar das inúmeras vantagens também comporta riscos reais diretos, ou seja os que advém de um uso imprudente e indiretos, isto é, aqueles que decorrem de falhas ou erros não intencionais. Certo é que o mundo ainda não tem condições para avaliar as ameaças personalizadas e conjuntas que a inteligência artificial pode trazer na medida em que esta é uma ferramenta recente na vida das sociedades modernas, pelo que toda a prudência não será demais. Para isso, será necessária uma estratégia multidisciplinar de avaliação de risco que tem necessariamente que envolver os responsáveis máximos do tecido empresarial, chefias de departamentos, especialistas informáticos, avaliadores de risco, departamentos jurídicos e todos aqueles que possam dar o seu contributo acerca da experiência que tem na utilização de dispositivos que utilizam inteligência artificial em todos os setores que dela fazem uso⁵.

Dado o potencial económico que apresenta o uso da inteligência artificial de forma massiva, essa ponderação e

4 Vide Stuart J. Russel, and Peter Norvig, *Artificial intelligence: a modern approach*, 3rd ed. Upper Saddle River, N.J.: Prentice Hall, 2010, London.

5 Neste sentido vide Zlotowski Jakub, Diane Proudfoot, Kumar Yogeewaran e Christoph Bartneck, *Anthropomorphism: Opportunities and Challenges in Human-Robot Interaction*, *International Journal of Social Robotics* 7 (3).

identificação do maior número de riscos possível é essencial para o desenvolvimento tecnológico crescente das sociedades modernas.

2. A Inteligência Artificial enquanto fator de desenvolvimento

Quando pensamos em inteligência artificial, somos intuitivamente tentados a pensar em robots. Porém, a inteligência artificial transcende a ideia dos robots humanoides que nos foi vendida pela criação da robot Sophia. A Inteligência Artificial, hoje em dia, aparece quase que enraizada no nosso cotidiano e em variadíssimas áreas. Basta pensarmos no corretor ortográfico do computador, nos sistemas de navegação GPS, nos sites da internet que na sua publicidade sugerem produtos que foram objeto de pesquisa, nos assistentes de voz, no reconhecimento facial nas redes sociais, na indústria, na engenharia aeroespacial, na medicina, na exploração de mares e oceanos, no ensino, nas empresas de recursos humanos, no atendimento ao cliente, nomeadamente quando este é feito por chat robots, nas operações financeiras, em atividades repetitivas, na monitorização de stocks, nas atividades de gestão, nos drones, na área militar, entre muitas outras⁶.

Pela variedade de setores onde a inteligência artificial se aplica, podemos facilmente perceber a dimensão da sua importância já que a sua implementação permitiu a modernização de inúmeros setores de atividade trazendo nomeadamente soluções que permitiram ganhar celeridade na resolução de questões, trouxe inovação, permite a realização de trabalho prolongado sem pausas, precisão nas atividades desenvolvidas, rapidez de comunicação, acesso através de máquinas a lugares inacessíveis a humanos, redução de repetição de tarefas por erros e modernização. As vantagens deste tipo de inteligência são inegáveis estimando-se que até 2030 possam trazer ganhos mundiais que ultrapassem os treze triliões

6 Vide Antonio Fernandez - Caballero, Pascual Gonzalez, Maria Teresa Lopez, Elena Navarro, Socio-Cognitive and Affective Computing, MDPI Journal, 2018, Basel – Switzerland.

de dólares por ano⁷.

Além de empiricamente termos todas as vantagens que acabamos de enunciar, as máquinas dotadas de inteligência artificial superam-se na sua resistência podendo muitas vezes fazer mais e melhor do que os humanos que as criaram com esse objetivo. Porém convém indagarmos até que ponto as máquinas dotadas de inteligência artificial conseguem fazer raciocínios lógicos e inteligentes. As máquinas são programadas e a sua autonomia racional está limitada aos dados que os humanos nela introduzem, sendo certo que este tipo de dispositivo por mais inteligente que seja nunca possuirá aquela que é a característica mais valiosa do ser humano: o livre arbítrio. Ainda que as máquinas possam ser mais precisas e rigorosas que os humanos porque para isso são preparadas e programadas, não são seres vivos dotados de criatividade, imaginação e cérebro livre⁸.

A evolução das máquinas dotadas de inteligência artificial só acontece porque os humanos criam essa possibilidade, daí ser tão importante não cometer erros na sua programação e preparação, de modo que acidentalmente a criação se possa virar contra o criador. Qualquer regra moral artificial que as máquinas possam ter será sempre predefinida e predeterminada pelo Homem⁹.

3. Custos e especialização associada à utilização da Inteligência Artificial

Dentro dos custos que a inteligência artificial apresenta estão os riscos na sua utilização. Existem desde logo três tipos de riscos: os individuais, os organizacionais e os sociais.

Vejam em primeira análise os riscos individuais. Os

7 Neste sentido vide Benjamin Cheatham et al., *Confronting The Risks of Artificial Intelligence*, Mckinsey Quarterly, 2019, Philadelphia – USA.

8 Neste sentido vide Philip Goff, *Galileo's Error: Foundations for a New Science of Consciousness*, Pantheon Books, 2019, New York.

9 Vide Kenneth Einar Himma, *Artificial agency, consciousness and the criteria for moral agency: what properties must an artificial agent have to be a moral agent*, *Ethics and Information Technology* (2009) 11, Springer, 2009, Seattle – USA

dispositivos que são dotados de inteligência artificial podem trazer a um qualquer indivíduo ameaças à sua segurança física ou digital, no caso de as máquinas dotadas de inteligência artificial os ferirem fisicamente ou exporem os seus dados na internet, à sua privacidade ou reputação se existirem falhas nos sistemas de proteção de dados que exponham informação sensível ou confidencial, à sua vida financeira, se os mecanismos de inteligência artificial subtraírem valores às suas contas bancárias ou produtos financeiros que detenham, e ao seu direito a um tratamento igualitário e justo, se um indivíduo for substituído por uma máquina no desempenho das suas funções laborais está a ser alvo de um tratamento injusto na medida em que um ser humano nunca terá a resistência física de uma máquina nem tampouco conseguirá ter níveis de desempenho equiparáveis dadas as características próprias do ser humano¹⁰.

No que aos riscos organizacionais diz respeito, o desenvolvimento de modelos e sua implementação nas empresas e instituições quer sejam públicas ou privadas pode originar erros de implementação que poderão levar a resultados tendenciosos ou discriminatórios e que produzam resultados desadequados no que diz respeito quer ao seu desempenho financeiro e organizacional como também no que diz respeito ao cumprimento de normas ou questões jurídicas que podem implicar danos na sua integridade ou reputação¹¹.

Já os riscos sociais tendem a ser mais abrangentes podem manifestar-se em questões de segurança nacional se eventualmente algum dispositivo dotado de inteligência artificial cometer um erro militar que afete as relações diplomáticas entre Estados, a estabilidade político-social que pode ser posta em causa em caso de ocorrência de erros graves de sistemas de inteligência artificial que causem danos que afetem as populações, como cortes de

10 Neste sentido vide Matias Scheutz *The inherent dangers of unidirectional emotional bonds between humans and social robots*, Cambridge MIT Press, 2014, Massachusetts – USA.

11 Vide Siu-Cheung Kong, and Harold Abelson, *Computational Thinking Education*, Springer Open, 2019.

energia, emissão de poluição nociva, apagões ou exposição de dados digitais, ou na integridade de infraestruturas se falharem dispositivos que controlam por exemplo dispositivos médicos, pontes, edifícios públicos ou monumentos¹².

Todos estes riscos têm como denominador comum falhas de interface entre o Homem e a máquina que dão origem a um mau funcionamento tecnológico que se materializa na deteção lenta de problemas e questões de desempenho que podem constituir ameaças sérias aos humanos quer individualmente, quer coletivamente de variadíssimas formas¹³.

Uma forma eficaz de minimizar esses riscos será antecipar alguns possíveis cenários de modo a construir uma “intuição de risco” até então inexistente quanto à inteligência artificial. A conscientização de 3 elementos essenciais pode ser bastante importante nesta matéria: a necessidade de os dados introduzidos nas máquinas dotadas de inteligência artificial estarem corretos, a possibilidade de ocorrerem vulnerabilidades tecnológicas e assumir que existem sempre falhas de segurança possíveis¹⁴.

Além disso, devemos ter em conta que a inteligência artificial está dependente da relação entre as pessoas e as máquinas, sendo que uma falha nesse processo interativo pode comprometer os modelos de gestão, a programação e a inserção de dados nos dispositivos que utilizam inteligência artificial.

As máquinas que utilizam inteligência artificial necessitam de hardware e software adequados, que regra geral, implica custos elevados. Acresce que existe a necessidade de serem programadas por especialistas em tecnologia que serão responsáveis também pela sua manutenção. Ora esta necessidade implica que exista a

12 Vide Jerry Kaplan, *Artificial Intelligence: What Everyone Needs to Know*, Oxford University Press, 2016, Oxford.

13 Neste sentido vide Stefan Oeter et al. *IT Law in The Era of Cloud Computing – A comparative analysis between EU and US Law on the Case Study of Data Protection and Privacy*, Nomos, 2018, Hamburg University, Baden – Germany

14 Neste sentido vide Benoit Dupont, *Cybersecurity Futures: How Can We Regulate Emergent Risks?* Technology Innovation Management, TimReview.ca, 2013, Montreal – Canadá.

formação crescente de especialistas em tecnologia capazes de realizar esta tarefa. Porém convém que estes especialistas tenham formação em vários domínios além da tecnologia: como a ética, finanças, linguagem e segurança. Ademais, devem ter aptidões naturais para integrar equipas multidisciplinares colaborando ativamente para melhorar os dispositivos dotados de inteligência artificial. Devemos ter em conta que a inteligência artificial deve ser usada para promover o desenvolvimento humano, mas não deve ficar descontrolada. Assim sendo, os especialistas em tecnologia devem fazer um uso responsável da inteligência artificial, devendo estar também preparados para lidar de forma assertiva com erros ou ataques cibernéticos¹⁵.

4. A ameaça à empregabilidade provocada pela excessiva utilização da Inteligência Artificial

Se pensarmos que existem máquinas capazes de fazer atendimentos aos clientes nos supermercados e portagens, que executam tarefas repetitivas por exemplo de corte e embalagem na indústria, percebemos que existem milhares de postos de trabalho ameaçados todo o mundo, pelos dispositivos que usam inteligência artificial.

Mas não só os trabalhadores substituídos são “vitimas” das máquinas, perdendo o seu rendimento, também aqueles que ficam e que ocupam cargos não substituíveis pelas máquinas, vão sofrer algum tipo de isolamento social, com as consequências físicas e mentais que daí advêm¹⁶.

5. Questões Éticas e Sociais da Utilização da Inteligência Artificial

15 Vide Ciza Thomas et al., Computer Security Threats, IntechOpen, 2020, London.

16 Neste sentido Martin Ford, Rise of Robots: Technology and Threat of a jobless future, Basic Books, 2015, London.

Introduzir máquinas dotadas de inteligência artificial em ambientes humanos pode levantar questões éticas e sociais. Apesar de estes dispositivos, nomeadamente os robots estarem presentes no ensino em creches e em salas de aula, em ambientes médicos e de cuidados pessoais, as questões que se colocam passam por saber se os robots devem seguir padrões morais e em que medida e se devem ter direitos e de que natureza. Esta questão é muito controversa em termos doutrinários, isto porque depende do papel que consideramos que tem a máquina inteligente.

Devemos é não esquecer que a inteligência destas máquinas é pré-concebida pelos humanos e não é própria, como o nome bem indica é meramente artificial, ou seja, não é natural nem inata, mas sim é antes criada pelos humanos para incorporar a máquina. Os robots não vivem a experiência da vida num corpo humano, nem tem vida, mas sim um botão de ligar e desligar¹⁷. Devemos fazer uma separação ontológica porque a tecnologia não é uma parte do ser humano. Apesar de os robots contribuírem positivamente, quando utilizados de forma inofensiva, para a experiência humana, eles não são seres humanos eles próprios. Porém, existem humanos que veem os dispositivos com inteligência artificial como artefactos passíveis de serem objeto de direitos de propriedade, outros como “seres” passíveis de estabelecerem relacionamentos com humanos. Isto levanta a questão de saber qual é o papel da máquina inteligente¹⁸.

Existe uma parte da doutrina que entende que os robots devem ter direitos humanos como os conhecemos porque também os humanos não estão sujeitos a uma moral que seja garante dos seus direitos humanos¹⁹. Outros entendem que os robots deverão ter os direitos correspondentes às obrigações legais que consigam

17 Neste sentido vide Joshua C. Gellers, *Rights for Robots Artificial Intelligence*, Animal and Environmental Law, Routledge, 2021.

18 Vide Sean Welsh *Ethics and Security Automata*. Ethics, Emerging Technologies and International Affairs, Routledge, 2017, Abingdon.

19 Neste sentido vide Lexo Zardiashvili and Eduard Fosch-Villaronga, “Oh, Dignity Too?” Said The Robot: Human Dignity as The Basis for The Governance of Robotics, Springer, 2020, Netherlands.

cumprir²⁰. Existindo ainda uma terceira corrente, com a qual nos identificamos que entende que os robots são meros artefactos inteligentes, sem dimensão relacional que apenas são propriedade dos humanos²¹. Convém não esquecer que os robots não têm componente moral e é construído pelos humanos.

Os direitos de personalidade só podem aplicar-se a quem tenha consciência, intencionalidade, livre-arbítrio e raciocínio. Além disso os direitos legais das pessoas só podem ser atribuídos a quem esteja vivo, e saiba viver em comunidade com base nos interesses próprios e recíprocos. Ademais, se os robots não sabem o que é a moral, eles não podem ter direitos morais. Seria até pouco ético pôr os direitos humanos a competir com interesses de entidades artificiais. Os robots e as máquinas dotadas de inteligência artificial não são um ser humano e como tal não lhe podem ser garantidos ou negados quaisquer tipos de direito²².

6. Conclusões

Pela variedade de setores onde a inteligência artificial se aplica, podemos facilmente perceber a dimensão da sua importância já que a sua implementação permitiu a modernização de inúmeros setores de atividade trazendo nomeadamente soluções que permitiram ganhar celeridade na resolução de questões, trouxe inovação, permite a realização de trabalho prolongado sem pausas, precisão nas atividades desenvolvidas, rapidez de comunicação, acesso através de máquinas a lugares inacessíveis a humanos, redução de repetição de tarefas por erros e modernização.

Todavia, e apesar das múltiplas vantagens que a Inteligência Artificial traz no desenvolvimento das sociedades modernas nos

20 Vide Wendell Wallach and Colin Allen, *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press, 2008, Oxford.

21 Neste sentido vide Jacob Turner *Robot Rules: Regulating Artificial Intelligence*, Palgrave MacMillan, 2019, United Kingdom.

22 Vide Henrik Skaug Saetra, *The Parasitic Nature of Social AI: Sharing Minds with The Mindless*, *Integrative Psychological and Behavioral Science* 54 (2), Springer, 2020.

mais diversos âmbitos, a mesma tem custos e riscos que não podem ser esquecidos atenta a gravidade das consequências que poderão trazer a nível individual, organizacional e societário.

No que diz respeito aos riscos individuais, podem existir falhas nos sistemas de proteção de dados que exponham informação sensível ou confidencial. Quanto aos riscos organizacionais, o desenvolvimento de modelos e sua implementação pode originar erros que poderão levar a resultados tendenciosos ou discriminatórios e que produzam resultados desadequados. Já os riscos sociais podem manifestar-se em questões de segurança nacional, de estabilidade político-social ou em variadíssimos danos que afetem as populações, tais como cortes de energia, emissão de poluição nociva, apagões ou exposição de dados digitais, por exemplo. Todos estes riscos têm em comum falhas de interface entre o Homem e a máquina, que dão origem a um mau funcionamento tecnológico, podendo constituir ameaças sérias aos humanos quer individualmente, quer coletivamente.

Além disso, é necessário criar uma “intuição de risco” concebendo a priori um conjunto de falhas possíveis nos dispositivos de inteligência artificial de modo que a resposta às mesmas seja mais eficiente e comporte consequências menos gravosas.

Verifica-se também que o mundo ainda não apresenta condições para avaliar as ameaças personalizadas e conjuntas que a inteligência artificial pode trazer, na medida em que esta é uma ferramenta recente na vida das sociedades modernas.

Independentemente de tudo, ressalve-se que os dispositivos portadores de inteligência artificial não podem de modo algum ser equiparados a humanos naquilo a que aos seus direitos diz respeito.

Bibliografia

BARTNECK, Christoph, et al., An Introduction to Ethics in Robotics and AI, Springer, 2021, Switzerland, ISBN 978-3-030-51110-4 (

ebk);

CHEATHAM, Benjamin, et al., *Confronting The Risks of Artificial Intelligence*, Mckinsey Quarterly, 2019, Philadelphia – USA, disponível em <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/confronting-the-risks-of-artificial-intelligence> consultado em 8 de setembro de 2021;

DUPONT, Benoit, *Cybersecurity Futures: How Can We Regulate Emergent Risks?* Technology

Innovation Management, TimReview.ca, 2013, Montreal – Canadá, disponível em https://timreview.ca/sites/default/files/article_PDF/Dupont_TIMReview_July2013.pdf pp.6–11, consultado em 2 de agosto de 2021;

FERNANDEZ – CABALLERO, Antonio, GONZALEZ, Pascual, LOPEZ, Maria Teresa, NAVARRO, Elena, *Socio-Cognitive and Affective Computing*, MDPI Journal, 2018, Basel – Switzerland, ISBN 978-3-03897-199-3 (PDF), disponível em http://www.mdpi.com/journal/applsci/special_issues/socio_cognitive_and consultado em 8 de setembro de 2021;

FORD, Martin, *Rise of Robots: Technology and Threat of a jobless future*, Basic Books, 2015, London, ISBN: 978-0465097531;

GELLERS, Joshua C., *Rights for Robots Artificial Intelligence, Animal and Environmental Law*, Routledge, 2021, New York, ISBN 978-042-92-88-159 (ebk);

GOFF, Philip, *Galileo's Error: Foundations for a New Science of Consciousness*, Pantheon Books, 2019, New York, ISBN: 9781524747978 (ebk);

HIMMA, Kenneth Einar, *Artificial agency, consciousness and the criteria for moral agency: what properties must an artificial agent have to be a moral agent*, *Ethics and Information Technology* (2009) 11, Springer, 2009, Seattle – USA, DOI: 10.1007/s10676-008-9167-5;

JAKUB, Zlotowski, PROUDFOOT, Diane, YOGEESWARAN, Kumar

e BARTNECK, Christoph, Anthropomorphism: Opportunities and Challenges in Human-Robot Interaction, *International Journal of Social Robotics* 7 (3), DOI <https://doi.org/10.1007/s12369-014-0267-6> ;

KAPLAN, Jerry, *Artificial Intelligence: What Everyone Needs to Know*, Oxford University Press, 2016, Oxford, ISBN-13: 978-0190602390;

KONG, Siu-Cheung, and ABELSON, Harold, *Computational Thinking Education*, Springer Open, 2019, Hong Kong/USA, ISBN 978-981-13-6528-7 (ebk), DOI: <https://doi.org/10.1007/978-981-13-6528-7>;

OETER, Stefan, et al. *IT Law in The Era of Cloud Computing – A comparative analysis between EU and US Law on the Case Study of Data Protection and Privacy*, Nomos, 2018, Hamburg University, Baden – Germany, ISBN 978-3-8487-5362-8 (Print); 978-3-8452-9562-6 (e-pdf);

RUSSELL, Stuart J., and NORVIG, Peter, *Artificial intelligence: a modern approach*, 3rd ed. Upper Saddle River, N.J.: Prentice Hall, 2010, London, ISBN 9780132071482;

SAETRA, Henrik Skaug, *The Parasitic Nature of Social AI: Sharing Minds with The Mindless*, *Integrative Psychological and Behavioral Science* 54 (2), Springer, 2020, DOI:10.1007/s12124-020-09523-6;

SCHEUTZ, Matias, *The inherent dangers of unidirectional emotional bonds between humans and social robots*, Cambridge MIT Press, 2014, Massachusetts - USA, ISBN: 978-0262526005;

THOMAS, Ciza, et al., *Computer Security Threats*, IntechOpen, 2020, London, ISBN 978-1-83962-381-3 (ebk);

TURNER, Jacob, *Robot Rules: Regulating Artificial Intelligence*, Palgrave MacMillan, 2019, United Kingdom, ISBN: 978-3-319-96-235-1 (ebk);

WALLACH, Wendell, and ALLEN, Colin, *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press, 2008, Oxford, ISBN-13: 9780195374049;

WELSH, Sean, *Ethics and Security Automata. Ethics, Emerging Technologies and International Affairs*, Routledge, 2017, Abingdon, ISBN-13: 978-1138050228;

ZARDIASHVILI, Lexo and FOSCH-VILLARONGA, Eduard, “Oh, Dignity Too?” Said The Robot: Human Dignity as The Basis for The Governance of Robotics, Springer, 2020, Netherlands, disponível em <https://doi.org/10.1007/s11023-019-09514-6> consultado em 8 de setembro de 2021.

Direito de Manifestação e Cedência de Dados Pessoais

Right to Protest and the Transfer of Personal Data

Mário Simões Barata¹

Jorge Barros Mendes²

Sumário: 1 – Introdução; 2 – O direito de reunião e de manifestação; 3 – A Lei nº 406/74; 4 – Apreciação crítica; 5 - Regulamento Geral de Proteção de Dados; 6 - Conclusão.

Resumo: O trabalho ora apresentado visa analisar o artigo 45º da Constituição da República Portuguesa que consagra um direito de reunião e um direito de manifestação. De seguida, considera o Decreto-Lei nº 406/74, de 29 de agosto, que garante um direito de reunião e regula a possibilidade de se realizar uma manifestação em lugar público ou aberto ao público. Examina ainda o regime de aviso prévio consagrado na lei. Este não contempla a cedência de dados pessoais dos promotores de uma manifestação para além daquela que terá de ocorrer entre o presidente da câmara municipal e as autoridades policiais, de modo a cumprir com a lei. Para que tal cedência ocorra é necessário consentimento expresso por parte dos titulares dos dados, nos termos do Regulamento Geral de Proteção de Dados, bem como está o responsável pelo tratamento obrigado à elaboração de uma avaliação de impacto de proteção de dados.

Palavras-chave: Direito de manifestação; aviso prévio; cedência de dados pessoais; Regulamento Geral de Proteção de Dados; avaliação de impacto de proteção de dados, dados sensíveis.

Abstract: The article seeks to analyse Article 45 of the Portuguese Constitution that enshrines a right of assembly and a right to protest. It then considers Decree-Law No 406/74, of 29 August 1974, which guarantees a right of assembly and regulates the possibility of holding a demonstration in a public place or open to the public. It also examines the notice system laid down by law. This mechanism does not include the transfer of personal data from the promoters of a demonstration other than the one that will take place between the mayor

1 Professor Adjunto do Politécnico de Leiria. Investigador do Instituto Jurídico da Portucalense (IJP – IP Leiria). E-mail: mario.barata@ipleiria.pt

2 Professor Adjunto do Politécnico de Leiria. Advogado. E-mail: jorge.mendes@ipleiria.pt

and the police to comply with the law. For such a transfer to take place, explicit consent is required from the data subjects, in accordance with the General Data Protection Regulation, and the controller is required to prepare a data protection impact assessment.

Keywords: Right to protest; prior notice; transfer of personal data; General Data Protection Regulation, Data Protection Impact Assessment, Sensitive Data.

1. Introdução

No passado mês de junho, a comunicação social noticiou que a Câmara Municipal de Lisboa tinha cedido os dados pessoais dos promotores de diversas manifestações realizadas na capital às Embaixadas dos países visadas pelas mesmas. As notícias veiculadas pelos diversos órgãos de comunicação social expuseram os procedimentos internos da Câmara Municipal de Lisboa que remontam à 2011 e que foram gizados na sequência da extinção do cargo de Governador Civil. Em concreto, o procedimento adotado no seio do município da capital implicava a cedência dos dados pessoais dos promotores das manifestações a diversas entidades, incluindo as Embaixadas, o que coloca em causa a segurança dos mesmos e, eventualmente, dos seus familiares que ainda residem nesses países. Contudo, a cedência de dados pessoais às Embaixadas não está contemplada na lei e viola o Regulamento Geral de Proteção de Dados, doravante GDPR. Assim, este trabalho visa analisar a norma constitucional que consagra o direito de manifestação, a lei que regula o direito de reunião que foi adotada em 1974, na sequência do 25 de Abril, bem como as implicações jurídicas da cedência de dados pessoais dos promotores, à luz do regime jurídico da proteção de dados.

2. O direito de reunião e de manifestação

O Artigo 45º da Constituição da República Portuguesa consagra o direito de reunião e de manifestação. A disposição

estabelece o seguinte:

Artigo 45º - Direito de reunião e de manifestação

1. Os cidadãos têm o direito de se reunir, pacificamente e sem armas, mesmo em lugares abertos ao público, sem necessidade de qualquer autorização.
2. A todos os cidadãos é reconhecido o direito de manifestação.

De acordo com Gomes Canotilho e Vital Moreira o direito de reunião e de manifestação encontra-se entre os direitos, liberdades e garantias pessoais. Estes direitos estão ligados, nas palavras daqueles Professores de Coimbra, à formação da opinião pública e por conseguinte constituem “um pressuposto necessário do Estado de direito democrático”.³

A doutrina não é unanime quanto à possibilidade de se distinguir entre estes direitos. Para Jorge Miranda e Rui Medeiros uma “manifestação é uma reunião qualificada”.⁴ Pelo contrário, Gomes Canotilho e Vital Moreira escrevem o seguinte: “o direito de reunião é necessariamente um direito de ação coletiva, mas os seus titulares são os cidadãos em si mesmos. Pode ser exercido em privado ou público, não tem de supor a expressão de uma mensagem contra ou dirigida a terceiros e pode servir os mais variados propósitos e motivações (recreativos, culturais, profissionais, políticos e religiosos). O direito de manifestação não é necessariamente um direito coletivo (pode haver manifestações individuais (...)), tem de revestir uma forma de exercício público, supõe a expressão de uma mensagem dirigida contra ou em direção a terceiros (pelo menos a «opinião pública») e serve normalmente propósitos ou motivações políticas. Uma manifestação é quase sempre também uma reunião; uma reunião, mesmo em lugar

3 José Joaquim Gomes Canotilho & Vital Moreira, Constituição da República Portuguesa Anotada: Artigos 1º a 107º, 4ª edição, Coimbra: Coimbra Editora, 2007, p. 636.

4 Jorge Miranda & Rui Medeiros, Constituição Portuguesa Anotada, Volume I: Preambulo, Princípios Fundamentais, Direitos e Deveres Fundamentais, Artigos 1º a 79º, 2ª edição revista, Lisboa: Universidade Católica Editora, 2017, p. 685.

publico, não tem de ser uma manifestação. Uma manifestação não é necessariamente uma reunião num lugar público”.⁵

O direito de reunião e o direito de manifestação comportam vários componentes. Assim, de acordo com Gomes Canotilho e Vital Moreira é possível recortar pelo menos quatro componentes. Em primeiro lugar, aqueles direitos apontam para uma liberdade de reunião e de manifestação sem qualquer tipo de impedimento e sem necessidade de autorização prévia quer quanto à liberdade de convocar reuniões ou manifestações quer quanto à liberdade de participar nas mesmas. Em segundo lugar, os autores apontam para uma componente que se relaciona com o direito de não ser perturbado por outrem no exercício desses direitos. Esta componente inclui o direito à proteção do Estado contra qualquer tipo de ataque (por exemplo: ataques oriundos de contramanifestantes). Um terceiro componente associado a estes direitos prende-se com o direito à utilização de locais e vias pública, sem prejuízo da salvaguarda de outros direitos fundamentais em situações de colisão. Por último, o direito de reunião e o direito de manifestação englobam o direito à autodeterminação do local, hora, forma e conteúdo.⁶

A Constituição da República Portuguesa de 1976 não sujeita o direito de reunião e o direito de manifestação a qualquer regime de autorização prévia. Por outras palavras, tal regime violaria a lei fundamental. No entanto, a Constituição não proíbe a exigência de uma comunicação prévia dos promotores às autoridades. Esta comunicação tem um fundamento ou uma justificação quando a reunião ou a manifestação decorre em espaço público (por exemplo: largo, praça ou via), na medida em que as autoridades têm de tomar todas as providências para que a reunião ou a manifestação decorra sem qualquer tipo de incidente (por exemplo: desvio de trânsito; prevenção de contramanifestações; garantir a segurança

5 José Joaquim Gomes Canotilho & Vital Moreira, Constituição da República Portuguesa Anotada: Artigos 1º a 107º, pp. 636 e 637.

6 Idem, p. 638. No mesmo sentido, Jorge Miranda & Rui Medeiros, Constituição Portuguesa Anotada, pp. 686 e 687.

dos participantes).⁷

3. O Decreto-Lei nº 406/74

Na sequência da Revolução de 25 de Abril e a fim de dar cumprimento ao disposto no Programa do Movimento das Forças Armadas, o Governo Provisório adotou o Decreto-Lei nº 406/74, de 29 de agosto.⁸

O referido ato normativo garante a todos os cidadãos o livre exercício do direito de se reunirem pacificamente em lugares públicos, abertos ao público e particulares, independentemente de autorizações, para fins não contrários à lei, à moral, aos direitos das pessoas singulares ou coletivas e à ordem e à tranquilidade pública.⁹ Porém, a norma não alude às manifestações, o que parece indicar que o legislador não distinguia entre os conceitos de reunião e de manifestação.

O nº 1 do artigo 2º consagra um regime de aviso ou de comunicação prévia. Assim, as pessoas ou entidades que pretendam realizar reuniões ou manifestações em lugares públicos ou abertos ao público devem avisar por escrito e com a antecedência mínima de dois dias úteis o governador civil do distrito ou o presidente da camara municipal conforme o local da aglomeração se situe ou não na capital de distrito.¹⁰

O ato normativo regula ainda o conteúdo do aviso. Este deve ser assinado por três dos promotores que deverão fornecer os seguintes elementos de identificação às autoridades: nome; profissão; morada. No caso de o promotor ser uma associação, esta deverá identificar a respetiva direção.¹¹ Para além da identificação dos promotores, o aviso deve indicar a hora, local e o objeto da

7 Idem, p. 640.

8 Publicado no Diário da República, I Série, nº 201, de 29 de agosto.

9 Ver o nº 1 do Artigo 1º do Decreto-Lei nº 406/74.

10 O cargo de governador civil foi extinto pela Resolução do Conselho de Ministros 13/2011

11 Ver o nº 1 do artigo 2º do Decreto-Lei nº 406/74.

reunião e quando se trate de manifestação a indicação do trajeto a seguir.¹²

A justificação ou fundamento para o regime de aviso ou de comunicação prévia parece residir nos artigos 6º e 7º do diploma. Em primeiro lugar, existem razões conexas com o bom ordenamento de trânsito de pessoas e de veículos nas vias públicas.¹³ Em segundo lugar, o aviso prévio visa dar tempo às autoridades para se preparem e tomar todas as providências para que as reuniões ou manifestações em lugares públicos decorram sem a interferência de contramanifestantes, que poderão pôr em causa o livre exercício dos direitos dos participantes.¹⁴

O Decreto-Lei nº 406/74 introduz escassas limitações ao direito de reunião e de manifestação. A primeira confere o poder às autoridades para interromper a realização de reuniões ou manifestações quando forem afastados da sua finalidade pela prática de atos contrários à lei ou à moral ou que perturbem grave e efetivamente a ordem e tranquilidade públicas e o livre exercício dos direitos das pessoas bem como quando se verifica uma ofensa à honra dos órgãos de soberania e das Forças Armadas.¹⁵ A segunda situação prende-se com a possibilidade de alterar o trajeto programada por questões de regulação do trânsito.¹⁶ Em terceiro lugar, o ato normativo proíbe as reuniões ou manifestações com ocupação abusiva de edifícios públicos ou particulares.¹⁷ Por fim, as autoridades podem impedir a realização de reuniões ou manifestações em lugares públicos a menos de 100 metros das sedes dos órgãos de soberania, instalações militares ou de forças militarizadas, estabelecimentos prisionais, representações diplomáticas ou consulares, bem como as sedes de partidos políticos.¹⁸

12 Ver o nº 1 do artigo 3º do Decreto-Lei nº 406/74.

13 Ver o nº 1 do artigo 6º do Decreto-Lei nº 406/74.

14 Ver o artigo 7º do Decreto-Lei nº 406/74.

15 Ver o nº 1 do artigo 5º do Decreto-Lei nº 406/74.

16 Ver o nº 1 do artigo 6º do Decreto-Lei nº 406/74.

17 Ver o artigo 12º do Decreto-Lei nº 406/74.

18 Ver o artigo 13º do Decreto-Lei nº 406/74.

4. Apreciação crítica

A análise do artigo 45º da CRP bem como os preceitos que integram o Decreto-Lei nº 406/74 não disciplinam a cedência de os dados pessoais dos promotores de uma determinada manifestação com a exceção daquela que terá de ocorrer entre o presidente de uma determinada câmara municipal e às autoridades com a competência para assegurar a ordem pública (leia-se polícia). Dito de outro modo, qualquer procedimento interno que contempla a cedência de dados conexos com a identificação dos promotores ou a direção da pessoa coletiva a uma embaixada ou consulado de país visado por uma manifestação não tem qualquer tipo de apoio na Constituição ou na lei, e configura um ato suscetível de violar as normas legais que protegem os dados pessoais.

5. Regulamento Geral de Proteção de Dados

O Regulamento (UE) 2016/679 do Parlamento e do Conselho foi aprovado a 27 de abril de 2016 e publicado a 4 de maio do mesmo ano e passou a ser aplicável no ordenamento jurídico europeu a 25 de maio de 2018. No nosso ordenamento jurídico, a Lei 58/2019, de 8 de agosto, veio regulamentar algumas normas do Regulamento.

O GDPR aplica-se ao tratamento¹⁹ de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros

19 Atento o disposto no artigo 4.º, n.º 2 GDPR, tratamento é: uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

ou a ele destinados²⁰, bem como se aplica ao tratamento de dados pessoais que ocorram quer dentro, quer fora do território da União Europeia, desde que os dados pertençam a cidadãos europeus, ou que se encontrem em território europeu²¹.

O próprio regulamento define o que são dados pessoais no artigo 4.º - trata-se de toda a informação relativa a uma pessoa singular identificada ou identificável. É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Ora, como vimos supra, o Município de Lisboa – responsável pelo tratamento²² - no âmbito da realização das manifestações, transferiu dos promotores da manifestação o nome, profissão, número do cartão do cidadão ou do título de residência, número de telefone e morada.

O artigo 5.º do GDPR estabelece os princípios fundamentais relativos aos dados pessoais e consagra expressamente que a recolha de dados pessoais só poderá existir para fins específicos, além de se estabelecer a minimização dos dados, ou seja, a recolha dos dados deve limitar-se ao estritamente necessário e para um fim em concreto, o que não foi o caso, considerando que o tratamento dos dados levada a cabo foi desproporcionado.

Além disso, consagra o GDPR o princípio da limitação da conservação, ou seja, os dados deverão ser conservados de uma

20 Cfr. artigo 2.º GDPR. Deverá ter-se em atenção que qualquer organização que detenha um simples ficheiro word ou excel que contenha dados de natureza pessoal, ou um simples arquivo em papel deverá, como veremos, de cumprir com as obrigações impostas pelo GDPR. Para o diploma, atento o disposto no n.º 6 do artigo 4.º é considerado ficheiro qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

21 Cfr. artigo 3.º GDPR.

22 Cfr. artigo 4.º, al. 7) do GDPR.

forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados. Depois de tal momento acontecer, os dados deverão ser destruídos. No caso em concreto, o Município de Lisboa não tinha instituído qualquer data para a sua destruição²³.

Prevê-se, no entanto, que os dados pessoais possam ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos²⁴.

É ainda estabelecido que o processo de recolha de dados tem de ser transparente, leal e lícito. Ora, para que os dados possam ser tratados de forma lícita²⁵, tem o titular dos dados de consentir para que a recolha se processe, caso tal recolha não resulte de imposição legal. No caso em apreço, a recolha dos dados resulta de imposição legal²⁶.

Atento o disposto no artigo 13.º GDPR, e nomeadamente nos termos do disposto no artigo 14.º GDPR, o titular dos dados tem de ser informado, no momento da recolha, da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento – a CML – deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente dos dados, tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados.

Além do Município de Lisboa não ter informado os titulares da partilha dos dados, também não pediu o consentimento para os partilhar. Aliás, a partilha só seria lícita, se tivesse existido consentimento²⁷ - manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante

23 Cfr. Artigo 5.º, n.º 1, al. e) GDPR.

24 Cfr. artigo 89.º GDPR. O artigo 89.º é uma das normas que se espera que venha a ser objeto de regulamentação pelo legislador nacional.

25 Cfr. artigo 6.º GDPR.

26 Cfr. artigo 2º, n.º do D.L. 406/74.

27 Cfr. artigo 7.º GDPR.

declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento²⁸.

Acresce que o Regulamento prevê a proibição de tratamento de categorias especiais de dados e isto porque, no que diz respeito aos dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos²⁹, dados biométricos³⁰ para identificar uma pessoa de forma inequívoca, dados relativos à saúde³¹ ou dados relativos à vida sexual ou orientação sexual de uma pessoa, o tratamento de dados é proibido, dados esses tratados de forma ilícita, por falta de fundamento da licitude, nos termos do disposto no art.º 5.º, n.º1, al.) GDPR.

Não podemos olvidar que o GDPR ao consagrar o princípio da minimização dos dados, vem impor a obrigação de ser prestado ao titular dos dados a informação referente às finalidades para as quais os dados pessoais são tratados, quando possível, do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências.

A Diretiva 95/46/CE estabelecia já uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo. Além de esta obrigação originar encargos administrativos

28 Cfr. artigo 4.º, n.º 11 GDPR.

29 Nos termos do artigo 4.º, n.º 13 GDPR são considerados dados genéticos os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

30 Nos termos do artigo 4.º, n.º 14 são considerados dados biométricos os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

31 Nos termos do artigo 4.º, n.º 15, são considerados dados de saúde os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais, tal como é reconhecido nos considerandos do GDPR. Isto levou a que a opção do legislador europeu fosse no sentido de suprimir e substituir tais procedimentos com uma avaliação de impacto sobre a proteção de dados, nos termos do disposto no artigo 35.º GDPR. Esta avaliação de impacto ocorrerá nas operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades, nomeadamente, quando a operação envolva a utilização de novas tecnologias.

Nesses casos, o responsável pelo tratamento deverá proceder, antes do tratamento, a uma avaliação do impacto sobre a proteção de dados, a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco. Essa avaliação do impacto deverá incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.

Tal deverá aplicar-se, nomeadamente, às operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados, em especial quando tais operações dificultem aos titulares o exercício dos seus direitos.

No caso em concreto, o Município de Lisboa não elaborou qualquer avaliação de impacto de proteção de dados.

Sempre que uma avaliação de impacto relativa à proteção de dados indicar que o tratamento, na falta de garantias e de medidas e procedimentos de segurança para atenuar os riscos, implica um elevado risco para os direitos e liberdades das pessoas singulares e o responsável pelo tratamento considerar que o risco não poderá ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação, a autoridade de controlo deverá ser consultada antes de as atividades de tratamento terem início³².

O Município de Lisboa incorre na eventual condenação ao pagamento de diversas contraordenações, a generalidade de montante máximo de 20 000 000,00 euros e pela ausência de avaliação de impacto o de proteção de dados a coima de 10 000 000,00 euros³³.

6. Conclusão

Para que exista a transferência de dados pessoais, nomeadamente de dados sensíveis a terceiros, ou esta é levada a cabo no âmbito de uma obrigação legal, ou através de um pedido de consentimento expresso junto dos titulares de dados.

Para que tal tratamento de dados ocorra é sempre necessária a elaboração de uma avaliação de impacto de proteção de dados. Além de que a intervenção do encarregado de proteção, quando exista na organização, é fundamental.

A violação de tais disposições acarreta o pagamento de coimas, pois constituem contraordenações muito graves, nos termos do GDPR.

Bibliografia

32 No âmbito desse processo de consulta, o resultado de uma avaliação do impacto sobre a proteção de dados efetuada relativamente ao tratamento em questão pode ser apresentado à autoridade de controlo, em especial as medidas previstas para atenuar o risco para os direitos e liberdades das pessoas singulares.

33 Cfr. artigo 83.º, n.º 4 e 5.º do GDPR.

AAVV, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford: Oxford University Press, 2020. ISBN: 978-0-19-882649-1.

CANOTILHO, J. J. Gomes - Direito Constitucional, 7ª edição, Coimbra: Almedina, 2003.

CANOTILHO, J. J. Gomes & MOREIRA, Vital - Constituição da República Portuguesa Anotada: Artigos 1º a 107º, 4ª edição, Coimbra: Coimbra Editora, 2007. ISBN: 978-972-32-1462-8.

CORDEIRO, A. Barreto Menezes – Direito da Proteção de Dados, Coimbra: Almedina, 2020. ISBN: 978-972-40-8304-9.

MIRANDA, Jorge & MEDEIROS, Rui – Constituição Portuguesa Anotada, Volume I: Preambulo, Princípios Fundamentais, Direitos e Deveres Fundamentais, Artigos 1º a 79º, 2ª edição revista, Lisboa: Universidade Católica Editora, 2017. ISBN: 9789725405413.

Entre a transparência e o controle nas Assembleias gerais virtuais em cooperativas

Between transparency and control in virtual general assemblies in cooperatives

Leonardo Rafael de Souza¹

Cinthia Obladen de Almendra Freitas²

Sumário: 1. Introdução. 2. Reflexões éticas sobre a sociedade do controle na sociedade da transparência. 3. O exemplo brasileiro da virtualização da gestão democrática cooperativa pelas assembleias gerais virtuais. 4. Da transparência ao controle: os riscos à gestão democrática das cooperativas. 5. Considerações finais.

Resumo: Com a pandemia da Covid-19 e o distanciamento social, as interações sociais foram transformadas por novas tecnologias estabelecidas para harmonizar seus usuários pela transparência, permitindo novas formas de controle pela modulação para orientar e impor temas nos distintos debates da vida cotidiana. A partir da realidade específica das cooperativas brasileiras e a sua repentina necessidade de realização de assembleias gerais digitais para o pleno exercício do Princípio Cooperativo da Gestão Democrática pelos Membros, o artigo reflete, pelo método do levantamento bibliográfico, sobre como a transparência harmonizadora admite o estabelecimento de uma Sociedade de Controle que, por meio da modulação tecnológica, condiciona o agir dos indivíduos. Já pelo método qualitativo de observação não participante de oito assembleias gerais digitais realizadas no Brasil, o artigo identificou formas de modulação dos associados no ambiente assemblear, as quais ignoraram os aspectos fundamentais dos valores democráticos inerentes à atividade cooperativa, como a participação e o debate. Como conclusão, o processo de virtualização das assembleias gerais nas

1 Doutorando em Direito no Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Paraná – PUCPR. Bolsista CNPq. E-mail: leonardo.rafael@pucpr.edu.br

2 Doutora. Professora Titular e Coordenadora do Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Paraná – PUCPR. E-mail: cinthia.freitas@pucpr.br

O artigo é resultado de projeto de pesquisa fomentado pelo CNPq - Programa MAI/DAI.

cooperativas brasileiras revela um simples processo de digitization dos procedimentos assembleares atuais. Isso precisa ser substituído por um processo de digitalization que promova a verdadeira ação democrática de forma transparente e sem controles, atendendo as premissas axio-principiológicas do movimento cooperativo.

Palavras-chave: Sociedade da Transparência; Sociedade de Controle; Cooperativas; Assembleias Gerais; Virtualização.

Abstract: With the Covid-19 pandemic and social isolation, social interactions were transformed by new technologies established to harmonize their users through transparency, allowing new forms of control through modulation to guide and impose themes in the different debates of life. Based on the specific reality of Brazilian cooperatives and their sudden need to hold digital general meetings for the full exercise of the Cooperative Principle of Democratic Member Control, the article reflects, through the method of bibliographic survey, on how harmonizing transparency allows for the establishment of a Control Society that, through technological modulation, conditions the actions of individuals. By the qualitative method of non-participant observation of eight digital general assemblies held in Brazil, the article identified ways of modulating members in the assembly environment, which ignored the fundamental aspects of democratic values inherent to cooperative activity, such as participation and debate. In conclusion, the process of virtualization of general assemblies in Brazilian cooperatives reveals a simple process of digitization of current assembly procedures. This needs to be replaced by a digitalization process that promotes true democratic action in a transparent and uncontrolled way, meeting the value and principle premises of the cooperative movement.

Keywords: Transparency Society; Control Society; Cooperatives; General Assemblies; Virtualization.

1. Introdução

Com o advento da Internet, referenciais teóricos hoje consagrados como o de Manuel Castells previam transformações fundamentais nas relações sociais em rede, as quais seriam pautadas pela renovação das diversas formas de interação entre os indivíduos, especialmente diante da capacidade de universalização

do acesso. Na era da informação, porém, os meios de disciplinar as ações humanas, como pensados por Michel Foucault em sua *Sociedade Disciplinar*, mutaram para meios de controle. Agora à distância, com o uso das tecnologias digitais, as ações humanas na *Sociedade da Informação* passaram a ser moduladas por ferramentas que enquadram os indivíduos pela orientação e imposição de temas nos mais diversos debates da vida cotidiana, como refletido por Gilles Deleuze e Maurizio Lazzarato.

Ocorre que a partir da eclosão repentina da pandemia da Covid-19 e o consequente distanciamento social, plataformas digitais de interação social passaram ser utilizadas/desenvolvidas sem as devidas reflexões sobre a transparência exigida pelos usuários. Destinadas a harmonizar as ações do indivíduo, como pondera Byung-Chul Han, o imperativo da transparência pelas plataformas digitais se tornou, na prática, em distintas formas de controle dos indivíduos. Essa realidade, no caso das cooperativas, impactou diretamente na capacidade de reunião dos sócios e, por consequência, na força do Princípio Cooperativa da Gestão Democrática pelos Membros.

Assim, o artigo tem por objetivo geral refletir, na realidade brasileira, sobre como as assembleias gerais das cooperativas, essência da gestão democrática, foram impactadas pelas plataformas digitais que, sob o pretexto da transparência da gestão, podem se tornar meio de controle social pela modulação da dinâmica assemblear.

A partir do levantamento bibliográfico para consideração dos pressupostos teóricos da *Sociedade da Transparência* e da *Sociedade de Controle*, analisa-se, pelo método qualitativo da observação não participante, 08 (oito) assembleias gerais digitais realizadas por cooperativas brasileiras que se valeram de plataformas digitais para a realização dos seus conclaves. Como critério de análise, foram identificadas ações que possam representar formas de modulação dos associados no exercício da

democracia cooperativa pela tecnologia, tudo à luz das reflexões teóricas de Sérgio Amadeu da Silveira.

Entendeu-se a partir das observações a existência de dependência e passividade dos associados aos dispositivos digitais utilizados, os quais sob o pretexto de amplificar a gestão democrática pelo uso transparente das assembleias gerais digitais, criaram formas de controle que modularam a participação ativa, como a limitação ao debate e à interação entre os indivíduos, ao contrário do imaginado por Castells e pela Identidade Cooperativa.

2. Reflexões éticas sobre a sociedade do controle na sociedade da transparência

Ainda que não se pretenda nesse estudo estabelecer um conceito de ética – seja pela sua complexa e extensa conformação teórico-filosófica, seja pelo objetivo metodológico anteriormente já traçado –, é necessário esclarecer que o mesmo foi admitido a partir do que Nicola Abbagnano chama de “ciência da conduta”, quer dizer, uma reflexão de ideias sobre a conduta humana na vida em sociedade, fruto de diversas perspectivas desde a antiguidade.³

Esta delimitação inicial é importante na medida em que as transformações ora discutidas integram a compreensão do fenômeno da informação atualmente vivida no contexto do que Manuel Castells chamou de Sociedade da Informação⁴. Nessa sociedade, o acesso à informação e a consequente orientação da conduta humana são transformadas pelos meios digitais, apresentando um novo entrelaçamento de reflexões éticas que precisam ser discutidas no âmbito de uma sociedade a cada dia mais transparente e controlada.

Uma das realidades hoje vividas com a consolidação da Sociedade da Informação, também chamada de Sociedade em

3 ABBAGNANO, Nicola. Dicionário de filosofia. São Paulo: Martins Fontes, 2007, p. 391.

4 CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 2020.

Rede, é a acelerada troca de informações a partir de um rápido fluxo de dados que, por sua vez, exige a harmonização e a urgência da vida em sociedade. Essa condição mudou a conduta dos indivíduos que, segundo David Schenk, eliminaram os filtros críticos para aceitar uma padronização que os permite lidar com mais e mais informações, conforme as recebem.⁵ Consequência disso, reflete Byung-Chul Han, é o surgimento de uma sociedade que perde a capacidade de exercer a sua singularidade em nome da homogeneização, do idêntico, porém mais fluido, rápido.⁶

Nesse processo de aceleração, torna-se necessário operacionalizar e harmonizar os procedimentos em busca de uma melhor comunicação, exercendo a transparência um papel coercitivo em busca de harmonização. Para Han, a “transparência estabiliza e acelera o sistema, eliminando o outro ou o estranho.

Essa coação sistêmica transforma a sociedade da transparência em sociedade uniformizada.”⁷ Assim, a razão da sociedade da transparência não pode ser resumida à visão simplista de abertura total ao escrutínio sob o pretexto de boas práticas. A transparência na conduta humana da Sociedade da Informação busca também a harmonização dos indivíduos pela exposição, limitando cada vez mais as reflexões e as individualidades nos processos de comunicação. O importante é dar espaço à livre circulação de informações, sem perturbações.

Embora para Han o apelo pela transparência na Sociedade da Informação seja muito mais um imperativo econômico do que moral ou biopolítico, o próprio autor reconhece a transformação da conduta humana para uma sociedade que aceita a auto exposição como controle de um único olho panóptico, como pensado desde Jeremy Bentham e Michel Foucault.⁸ Em outras palavras, a

5 SHENK, David. Data smog: surviving the information glut. New York: Harper Collins Publishers, 1997.

6 HAN, Byung-Chul. Sociedade do cansaço. Petrópolis: Editora Vozes, 2015, p. 40.

7 HAN, Byung-Chul. Sociedade da transparência. Petrópolis: Editora Vozes, 2017, p. 11.

8 HAN, Byung-Chul. Op. Cit., 2017, p. 54-55.

Sociedade da Transparência, uniformizada pelo absoluto escrutínio dos seus indivíduos, acabou por transformar a própria Sociedade Disciplinar como pensada por Foucault: técnicas disciplinares de biopoder, baseada no confinamento, com o objetivo de docilizar os comportamentos de uma multiplicidade qualquer.⁹

Com o advento da tecnologia, pondera Gilles Deleuze, a coerção física dos indivíduos na Sociedade Disciplinar como moldes de comportamento passou a ser desnecessária. Agora, na Sociedade do Controle, a disciplina dos comportamentos é transformada por um capitalismo onde “a linguagem numérica do controle é feita por cifras, que marcam o acesso à informação, ou a rejeição. Não se está mais diante do par massa-indivíduo. Os indivíduos tornaram-se ‘divisíveis’, e as massas tornaram-se amostras, dados, mercados ou bancos.”¹⁰

Nesta Sociedade de Controle no contexto da Sociedade Informacional, acrescenta Maurizio Lazzarato, o poder exercido pelas tecnologias ocorre de maneira sutil, à distância de uma mente sobre a outra: “se as disciplinas moldavam os corpos ao constituir hábitos, principalmente na memória corporal, as sociedades de controle modulam os cérebros, constituindo hábitos sobretudo na memória mental.”¹¹ Esta ideia de modulação, aliás, é apresentada por Deleuze como uma moldagem que enquadra os indivíduos a partir da orientação e da imposição de temas nos debates da vida cotidiana.¹²

Como visto, transparência e controle se tensionam mais intensamente a cada passo do desenvolvimento tecnológico. Hoje, com a evolução das tecnologias digitais, a absoluta transparência dos indivíduos abre possibilidades para uma modulação mais fluída que delimita, reconfigura e influencia comportamentos,

9 LAZZARATO, Maurizio. As revoluções do capitalismo. Rio de Janeiro: Civilização Brasileira, 2006, p. 73.

10 DELEUZE, Gilles. Post-Scriptum Sobre as Sociedades de Controle. In DELEUZE, Gilles. Conversações. 3ª Ed. Tradução Peter Pál Pelbart. São Paulo: Editora 34, 2013, p. 224-226.

11 LAZZARATO, Maurizio. Op. Cit., 2006, p. 86.

12 DELEUZE, Gilles. Op. Cit., 2013, p. 225.

transformando-se numa poderosa ferramenta de controle social em suas distintas dimensões. E como forma de exemplificar este tensionamento, o presente estudo passa a refletir sobre o comportamento dos indivíduos dentro do microssistema democrático das cooperativas. Atualmente também transformadas pela virtualização das suas assembleias gerais, as cooperativas podem, sob o pretexto axiológico da transparência, levar a formas de controle dos cooperados pela modulação.

3. O exemplo brasileiro da virtualização da gestão democrática cooperativa pelas assembleias gerais virtuais

Não obstante as especificidades legais existentes em cada país, a compreensão das cooperativas enquanto empresa com uma natureza jurídica própria passa pela Declaração Sobre a Identidade Cooperativa, um documento global publicado pela Aliança Cooperativa Internacional (ACI) que, ratificada tanto pela Resolução 54/114 da ONU quanto pela Recomendação 193 da OIT, apresenta as matrizes de um código de valores acordado a nível internacional e que compõe o núcleo do Direito Internacional Público Cooperativo.¹³

Nesta Declaração, as cooperativas se destacam dos demais modelos de negócio por serem empresas de propriedade comum e democraticamente geridas a partir de objetivos econômicos, sociais e culturais coletivos, todos pautados por valores e princípios próprios que compõem o núcleo do que se convencionou chamar de Identidade Cooperativa.¹⁴

Dentre estes princípios está o Princípio da Gestão Democrática pelos Membros, o qual estabelece que as cooperativas são organizações essencialmente democráticas porque controladas

13 HENRÿ, Hagen. Guidelines for cooperative legislation. 3. ed. Geneva: ILO, 2012, p. 30.

14 ACI. Notas de Orientación para Los Principios Cooperativos. Ginebra: ACI, 2015, p. 2.

ativamente pelos seus sócios na determinação de suas políticas e na tomada de decisões, as quais ocorrem por meio das assembleias gerais (democracia participativa) e dos órgãos de representação eleitos democraticamente (democracia representativa). Na prática, este princípio instrumentaliza valores cooperativos imutáveis, como os valores da democracia, da responsabilidade e da transparência.¹⁵

Muito embora a evolução das tecnologias ainda não tivesse impactado tão profundamente a gestão democrática das cooperativas, até então caracterizada pela pessoalidade, com a pandemia da Covid-19 diversas foram as iniciativas globais de virtualização das assembleias gerais, ou seja, a sua realização à distância com o suporte das Tecnologias da Informação e Comunicação (TICs). Isso ocorreu porque diante da obrigatoriedade da realização das assembleias gerais nas cooperativas por distintas legislações¹⁶, tornou-se necessário estabelecer formas de reunião que não afrontassem as restrições de circulação de pessoas em todo o mundo. Assim, muitos países buscaram autorizações legais de urgência para a utilização das TICs na realização dessas assembleias.¹⁷

No Brasil as transformações foram ainda mais profundas e definitivas, especialmente porque com a Lei nº 14.030/2020, a Lei Geral das Sociedades Cooperativas (Lei nº 5.764/1971) teve acrescida ao seu texto legal o artigo 43-A, que dispôs sobre a possibilidade do associado “participar e votar a distância em reunião ou em assembleia, que poderão ser realizadas em meio digital”, desde que “respeitados os direitos legalmente previstos de participação e de manifestação dos associados e os demais

15 ACI. Op. Cit.. 2015, p. 20.

16 Como exemplos da obrigatoriedade legal na realização das assembleias apresentamos o exemplo do Brasil (artigo 44 da Lei nº 5.764/1971), de Portugal (artigo 34, 2, do Código Cooperativo – Lei nº 119/2015), da Argentina (artigo 47 da Lei nº 20.337/1973) e da França (artigo 8º da Lei nº 47-1775/1947).

17 Na Espanha o Real Decreto ley 8/2020 autorizou a realização de assembleias telemáticas na Pandemia, o que também ocorreu em Portugal com o Decreto-Lei nº 10-A/2020, e na Argentina com a Resolução 358/2020 do Instituto Nacional de Asociativismo y Economía Social (INAES).

requisitos regulamentares.”¹⁸

Conforme previsão legal, este novo dispositivo legal foi devidamente regulamentado pelo órgão responsável – o Departamento Nacional de Registro Empresarial e Integração (DREI) –, que por meio da Instrução Normativa DREI nº 79/2020 estabeleceu critérios para a realização de assembleias gerais semipresenciais (simultaneamente em local físico e à distância – artigo 1º, §1º, inciso I) ou digitais (sem a realização em local físico específico – artigo 1º, §1º, inciso II). Em ambos os casos, porém, o artigo 6º da referida Instrução Normativa estabeleceu a necessidade de garantias mínimas para a realização desses conclaves, como as certificações de segurança e transparência (inciso I), a efetiva participação dos associados (inciso II) e o livre e seguro exercício do voto (inciso IV), entre outros.¹⁹

Com autorização legal para a realização das assembleias gerais de forma virtual, as cooperativas brasileiras passaram a buscar no mercado ou a desenvolver dentro de suas próprias estruturas, ferramentas digitais para a realização dessas assembleias. Desde pequenas reuniões assembleares realizadas e gravadas em aplicativos conhecidos do mercado como Zoom, Google Meet e Microsoft Teams, por exemplo, até o desenvolvimento de plataformas próprias produzidas por cooperativas como o Sicoob Moob, Assembleias Sicredi e Curia, entre outros. O que se observou, nos anos de 2020 e 2021, foi uma profusão de assembleias digitais

18 BRASIL. Presidência da República. Lei nº 14.030, de 28 de julho de 2020. Dispõe sobre as assembleias e as reuniões de sociedades anônimas, de sociedades limitadas, de sociedades cooperativas e de entidades de representação do cooperativismo durante o exercício de 2020; altera as Leis nº 5.764, de 16 de dezembro de 1971, 6.404, de 15 de dezembro de 1976, e 10.406, de 10 de janeiro de 2002 (Código Civil); e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14030.htm>. Acesso em 30 ago. 2021.

19 BRASIL. Departamento Nacional de Registro Empresarial e Integração. Instrução Normativa DREI nº 79, de 14 de abril de 2020. Dispõe sobre a participação e votação a distância em reuniões e assembleias de sociedades anônimas fechadas, limitadas e cooperativas. Disponível em <<https://www.in.gov.br/web/dou/-/instrucao-normativa-drei-n-79-de-14-de-abril-de-2020-252498337>>. Acesso em 30 ago. 2021.

que simplesmente realizaram a digitization²⁰ dos procedimentos até então realizados presencialmente, sem qualquer reflexão sobre possíveis transformações digitais aplicáveis.

4. Da transparência ao controle: os riscos à gestão democrática das cooperativas

Como visto até aqui, ao simplesmente apresentar a transparência como uma noção de abertura total ao escrutínio sob o pretexto de boas práticas, a Sociedade da Transparência parece não refletir que a harmonização dos indivíduos leva a auto superexposição ao risco de efetivo controle da sociedade, o qual na visão de Deleuze e Lazzarato se traduz na modulação das ações humanas pelas tecnologias, que alteram os processos de comunicação de forma a orientar e até mesmo impor temas e objetivos nos debates sociais.

Para Sérgio Amadeu da Silveira²¹, essa modulação está acentuada pelo desenvolvimento de plataformas digitais cuja arquitetura de informação é completamente centralizada ao mesmo tempo em quem clama pela total transparência dos seus usuários. Nesta condição, a transparência se transforma em controle quando o fluxo de acesso aos conteúdos acaba sendo definido pelos gestores das plataformas, ou seja, modula-se aos usuários as opções e os caminhos de interação e de acesso ao conteúdo. E nas grandes plataformas, acrescenta, a utilização de algoritmos

20 O uso do termo em inglês se justifica pela sua dificuldade de tradução para o português. No campo da tecnologia digitization e digitalization são expressões distintas que, quando traduzidas, são reduzidas ao termo “digitalização”. Enquanto a digitization é compreendida como o processo de simples mudança da forma analógica para o digital, sem quaisquer alterações, a digitalization busca explicar um processo de mudança do próprio modelo de negócio para os meios digitais, ou seja, considera a capacidade das tecnologias digitais em construir alternativas ao analógico. Vide <https://www.gartner.com/en/information-technology/glossary>.

21 DA SILVEIRA, Sérgio Amadeu. A noção de modulação e os sistemas algorítmicos. In: SOUZA, Joyce; SOUZA; AVELINO, Sérgio; DA SILVEIRA, Sérgio Amadeu (Org.). A Sociedade de Controle: manipulação e modulação nas redes sociais. São Paulo: Hedra, 2018, p. 37.

estrutura processos de modulação que delimitam, influenciam e reconfiguram silenciosamente o comportamento dos usuários.²²

Foi sob essa perspectiva que, no caso das cooperativas brasileiras, realizou-se a observação não participante de 02 (duas) assembleias gerais digitais em cooperativas de trabalho e 06 (seis) assembleias gerais digitais em cooperativas crédito que usaram tanto plataformas já existentes no mercado para reuniões digitais (no caso, Plataformas Zoom e Google Meet) quanto plataformas desenvolvidas pelas próprias cooperativas. Em todas as assembleias observadas, o ponto comum estabelecido como critério de análise foi a existência de ações (na própria plataforma ou pelos gestores no comando das assembleias) que pudessem representar formas de modulação pela tecnologia.

Apesar de reconhecermos que as assembleias gerais são atos jurídicos solenes que precisam observar os requisitos legais previstos na Lei nº 5.764/1971 e outras leis específicas²³, o que as observações revelaram foi a simples digitization dos procedimentos, ou seja, preocuparam-se as cooperativas tão somente em transpor para o formato digital toda a liturgia e solenidade dos atos assembleares, tratando a transparência meramente como a abertura das informações em seus websites e a gravação das assembleias.

Esta postura se mostrou negativa à gestão democrática na assembleia geral digital considerando que as reuniões se tornaram excessivamente longas, formais (chegando a três horas de duração) e unidirecionais (de meras informações da gestão aos associados para ratificação pelo voto), colocando os associados numa condição de absoluta passividade, o que obstruiu a participação e o debate. Quanto ao tema, a própria Aliança Cooperativa Internacional orienta que a utilização das tecnologias pelas cooperativas para a gestão

22 DA SILVEIRA, Sérgio Amadeu. Op. Cit., 2018, p. 42.

23 Tanto as cooperativas de trabalho (Lei nº 12.690/2012) quanto as cooperativas de crédito (Lei Complementar nº 130/2009) possuem legislações específicas. Em ambas, porém, há remissão expressa às regras gerais da Lei nº 5.764/1971, que admite a assembleia geral virtual.

democrática deve ser utilizada de forma a transformar ativamente a participação dos indivíduos, o que significa dizer que a virtualização das assembleias gerais passa pela necessária transformação digital do modelo, adaptando as assembleias à realidade tecnológica²⁴; não o contrário, como ocorre na digitization.

Além disso, em todas as observações foi notório o uso das plataformas para limitar a participação e o debate entre os associados. Modulações como permitir apenas manifestações por escrito quando a plataforma permitia o uso de som e voz, cortar o microfone após determinado tempo de manifestação, não permitir o uso das câmeras e remeter às dúvidas e proposições dos cooperados aos corpos técnicos alheios ao quadro social, mostraram-se como estratégias que, sob o pretexto de otimizar e padronizar a reunião assemblear, mostraram-se como verdadeiro controle à gestão democrática.

Além disso, modulações das próprias plataformas como a sua priorização aos processos de votação em detrimento do debate e a impossibilidade técnica de inclusão de outras proposições eventualmente debatidas nas assembleias gerais digitais pelos associados delimitaram o surgimento de novas ideias ou propostas além daquelas inicialmente apresentadas pelos gestores. Estas modulações também pareceram reprimir o debate, a integração e a participação ativa dos cooperados nas decisões e políticas da sua cooperativa, ao contrário do que expressamente prevê o Princípio da Gestão Democrática.

O que se viu até aqui, portanto, foi a dependência e a consequente passividade dos associados aos dispositivos tecnológicos utilizados, os quais sob o pretexto de amplificar a gestão democrática pelo uso transparente das assembleias gerais digitais, criaram o que Sérgio Amadeu da Silveira chamou de controle pela criação de “perfis comportamentais e opinativos organizados e analisados como parte de um processo que culminará no encurtamento do mundo, na condução da visão e na entrega de

24 ACI. Op. Cit.. 2015, p. 17-18.

opções delimitadas.”²⁵

Esse controle pela modulação põe em risco a gestão democrática das cooperativas na medida em que efetivamente retira dos associados as condições básicas de participação ativa, como quer o movimento cooperativo na defesa da sua Identidade Cooperativa.

5. Considerações Finais

Como refletido, a pandemia da Covid-19 acelerou os processos de digitalização e de transformação digital previstos para a total integração social à era informacional. Entretanto, em diversas formas de interação coletiva a simples digitization dos procedimentos tem perpetuado formas de controle que, antes pensada como a disciplina do corpo pelo confinamento, agora modulam, pelo uso das diversas tecnologias, as ações dos indivíduos sob o pretexto da absoluta transparência em nome das boas práticas.

No caso específico das cooperativas brasileiras e os desafios que o necessário distanciamento social impôs à sua gestão democrática pelos membros, identificou-se nas assembleias gerais digitais observadas a simples digitization dos procedimentos assembleares anteriormente existentes na presencialidade, além de se observar a utilização das plataformas digitais também para modular a ação dos associados justamente naquilo que lhe é fundamentalmente garantido pelo Princípio Cooperativo da Gestão Democrática: o direito ao exercício ativo da participação e do debate com voz e voto.

Por outro lado, pelas observações realizadas notou-se que essas modulações podem também ser interpretadas como um natural processo de adaptação das cooperativas e seus gestores à virtualização rapidamente imposta pela pandemia da Covid-19 e com os limites regulamentares apresentados pela Instrução Normativa

25 DA SILVEIRA, Sérgio Amadeu. Op. Cit., 2018, p. 44.

DREI nº 79/2020, ou seja, frutos de um período de insegurança típico das transformações digitais vividas pela sociedade e nem sempre bem compreendidas pelo Direito.

Por isso, é essencial que futuras pesquisas continuem avaliando as assembleias gerais digitais nas cooperativas para saber se a digitization inicialmente realizada trata de um período de transição para a transformação do modelo pela digitalization ou, na verdade, se estabelecerão, sob o pretexto da transparência da gestão, como formas de efetivo controle do corpo social pela modulação dos associados. Entretanto, pelas raízes históricas e axio-principiológicas do cooperativismo e pelo nítido esforço dos quadros técnicos das cooperativas em bem entender essa nova era informacional, acredita-se que as assembleias gerais digitais poderão se transformar em verdadeiros mecanismos de efetiva gestão democrática, como desejado inclusive pela Aliança Cooperativa Internacional.

Em conclusão, tem-se como necessária a compreensão e a tênue vinculação entre transparência e controle para que se possa reagir a qualquer transformação tecnológica que, na prática, imponha o controle das ações humanas pela modulação das mentes. Aqui, o que se pretende foi dar um primeiro passo para a reflexão a partir da análise de um microssistema que tem na integração ética dos indivíduos a busca de um bem comum.

Referências bibliográficas

ABBAGNANO, Nicola. Dicionário de filosofia. São Paulo: Martins Fontes, 2007.

ACI. Notas de Orientación para Los Principios Cooperativos. Ginebra: ACI, 2015.

BRASIL. Presidência da República. Lei nº 14.030, de 28 de julho de 2020. Dispõe sobre as assembleias e as reuniões de sociedades anônimas, de sociedades limitadas, de sociedades cooperativas e de

entidades de representação do cooperativismo durante o exercício de 2020; altera as Leis nº 5.764, de 16 de dezembro de 1971, 6.404, de 15 de dezembro de 1976, e 10.406, de 10 de janeiro de 2002 (Código Civil); e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14030.htm>. Acesso em 30 ago. 2021.

BRASIL. Departamento Nacional de Registro Empresarial e Integração. Instrução Normativa DREI nº 79, de 14 de abril de 2020. Dispõe sobre a participação e votação a distância em reuniões e assembleias de sociedades anônimas fechadas, limitadas e cooperativas. Disponível em <<https://www.in.gov.br/web/dou/-/instrucao-normativa-drei-n-79-de-14-de-abril-de-2020-252498337>>. Acesso em 30 ago. 2021.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 2020.

DA SILVEIRA, Sérgio Amadeu. A noção de modulação e os sistemas algorítmicos. In: SOUZA, Joyce; SOUZA; AVELINO, Sérgio; DA SILVEIRA, Sérgio Amadeu (Org.). A Sociedade de Controle: manipulação e modulação nas redes sociais. São Paulo: Hedra, 2018.

DELEUZE, Gilles. Post-Scriptum Sobre as Sociedades de Controle. In DELEUZE, Gilles. Conversações. 3ª ed. Tradução Peter Pál Pelbart. São Paulo: Editora 34, 2013.

HAN, Byung-Chul. Sociedade do cansaço. Petrópolis: Editora Vozes, 2015.

HAN, Byung-Chul. Sociedade da transparência. Petrópolis: Editora Vozes, 2017.

HENRÿ, Hagen. Guidelines for cooperative legislation. 3. ed. Geneva: ILO, 2012.

LAZZARATO, Maurizio. As revoluções do capitalismo. Rio de Janeiro: Civilização Brasileira, 2006.

SHENK, David. Data smog: surviving the information glut. New York: Harper Collins Publishers, 1997.

Desafíos a la imputación de responsabilidad por ilícitos anticompetitivos cometidos en sistemas blockchain

Challenges to the imputation of responsibility for anti-competitive crimes committed in blockchain systems

Jesús A. Soto Pineda¹

Antonio J. Villanueva Tobalina²

Sumario: 1. Introducción; 2. Blockchain, derecho de la competencia e imputación de responsabilidad; 2.1 Opacidad en blockchain; 2.2 Arquitectura distribuida de las cadenas de bloques; 2.3 Creciente autonomía de las aplicaciones con base blockchain; 3. Conclusión; 4. Bibliografía

Resumen: Las cadenas de bloques son ampliamente estudiadas como una herramienta tecnológica con grandes utilidades y externalidades positivas, no obstante, resulta vital no pasar por alto los significativos retos jurídicos que plantea, especialmente en materia de libre competencia. Uno de los más severos son los problemas de imputación de responsabilidad que producen las Tecnologías de Registro Distribuido (TRDs), y concretamente blockchain, que a su vez dificultan con creces las funciones de las autoridades de competencia que deseen punir y reparar el deterioro generado en los mercados como consecuencia de prácticas anticompetitivas cometidas a través de la utilización antijurídica de Tecnologías de Registro Distribuido.

El presente documento analiza tales obstáculos a fin de contribuir a la futura solución de los problemas enunciados.

1 Doctor en Derecho por la Universidad Autónoma de Madrid; Profesor Investigador de la Universidad Externado de Colombia; Decano de Schiller International University.

Correo electrónico: jesusalfonso.soto@gmail.com

2 Graduado en Derecho por la Universidad Europea de Madrid; Máster en Abogacía y Máster en Legal Tech por la Universidad Francisco de Vitoria; Investigador de Schiller International University.

Correo electrónico: antonio7villanueva@gmail.com

Palabras-clave: Blockchain, Tecnología de Registro Distribuido, Defensa de la competencia, Responsabilidad, Desafíos

1. Introducción

Hace ahora aproximadamente 13 años, un misterioso individuo -o grupo de individuos- permitió que viera la luz un documento que sentó las bases de una de las tecnologías más revolucionarias de nuestro tiempo.

Aquel documento, titulado Bitcoin: A Peer-to-Peer Electronic Cash System, hizo posible el desarrollo que en la actualidad han experimentado las Tecnologías de Registro Distribuido (en lo sucesivo, TRD), y blockchain en concreto. Así surgió Bitcoin, la primera criptomoneda, basada en un esquema peer-to-peer que hizo posible pagos en línea directos entre sujetos sin necesidad de la anteriormente preceptiva intermediación de entidades financieras, lo cual era ya, de por sí, ampliamente innovador y disruptivo.

El dinero fiduciario convencional utilizado durante los últimos siglos no dependía ya del valor intrínseco del material utilizado para acuñar la divisa -como sucedía en el pasado, cuando la moneda poseía valor por el metal precioso utilizado para fabricarla- sino que dependía de la confianza, confianza depositada sobre los Estados e instituciones financieras que la respaldan. En cierto modo, tales organismos se constituyen como intermediarios que actúan como garantes del valor de la moneda y de que cualquier transacción llevada a cabo con ella será perfectamente válida.

Bitcoin nació con la vocación de evitar la necesidad de tener que recurrir a tales instituciones como generadoras de confianza en el valor de la divisa y, en consecuencia, como intermediarios en la operación realizada, generando a su vez una dinámica transaccional más autónoma de lo que había sido posible hasta la fecha.

Sin embargo, lo que comenzó como un sistema para la creación y soporte de una moneda electrónica completamente

independiente de cualquier institución o autoridad acabó tornándose una tecnología con el potencial para constituirse como uno de los pilares de la quinta revolución industrial.

Blockchain genera un registro permanente e inalterable de cualquier información que se introduzca en él, estructurado de una forma distribuida y favoreciendo la desintermediación en transacciones de toda índole (Deshpande et al., 2017, p. ix). Las posibilidades de esta tecnología son múltiples.

En el ámbito privado, a las oportunidades que ofrecen las criptomonedas y los smart contracts para el comercio y los servicios financieros se suman el almacenamiento de información en registros de todo tipo, la gestión de las cadenas de suministro, la emisión digital, negociación y liquidación de valores en los mercados de capitales, la automatización de pagos en materia de seguros y otros ámbitos (Krause et al., 2017, p. 22), así como la generación y sostenimiento de mercados descentralizados (Lianos, 2018, p. 23 y ss), pudiendo llegar a limitar la hegemonía de algunos de los grandes gigantes tecnológicos.

En el ámbito público, la adopción de tecnología blockchain podría ayudar a (Capobianco, 2018, p. 2): (i) reforzar el cumplimiento de la normativa y ayudar en la adopción de medidas contra la evasión fiscal y la transgresión de otras leyes; (ii) fortalecer la política monetaria y fiscal a través de criptomonedas que gocen del respaldo del Estado; (iii) evidentes beneficios a efectos registrales (Registro de la Propiedad o Registro Mercantil, por citar dos ejemplos); (iv) aumento de la eficacia en la protección de datos, (v) incrementar la transparencia en los procesos públicos, (vi) pagos de pensiones y seguridad social más eficientes, transparentes y económicos a través de blockchain, (vii) datos, registros e historiales médicos de los pacientes compartidos de forma segura a los médicos que deban tener acceso a dicha información.

Las arriba mencionadas son algunas de las aplicaciones de blockchain viables ya en el presente. En el futuro, las sinergias que

las cadenas de bloques pueden generar con paradigmas como el Internet de las Cosas (IoT) y tecnologías como la robótica o la Inteligencia Artificial pueden producir cambios en los mercados que ahora resultan difíciles de predecir.

No obstante, más allá de la mejora de procesos, la reducción en los costes de transacción y demás ventajas derivadas de la implementación de cadenas de bloques en los más diversos ámbitos y sectores productivos, también existen obstáculos que merman el atractivo de sus beneficios.

De entre los notables desafíos que presenta el uso de tecnología blockchain, el objeto del presente documento se encuentra constituido por las dificultades en la atribución de responsabilidad por la comisión de conductas antijurídicas en el seno de estos sistemas, concretamente en lo circunscrito al derecho de libre competencia o antitrust.

2. Blockchain, derecho de la competencia e imputación de responsabilidad

El derecho antitrust se ocupa de la protección de la libre competencia en los mercados, velando por competidores y usuarios a la vez que promueve y persigue la generación de eficiencias en los mismos, equilibrando las posiciones de los distintos competidores, evitando la perpetración de abusos y permitiendo a los consumidores acceder a los mejores servicios a los mejores precios.

Para imputar responsabilidad a uno o varios sujetos por una conducta antijurídica determinada, resulta necesario la puesta en práctica de diligencias y pesquisas previas que constituyen el estamento inferior de la pirámide cuya cúspide es la sanción y/o remedio que las autoridades de competencia buscarán imponer al sujeto infractor como consecuencia de sus actos y del perjuicio que hayan ocasionado a otros competidores, consumidores y/o al

mercado en su conjunto.

No obstante, si las autoridades no son capaces de vincular las conductas anticompetitivas cometidas con los sujetos responsables de su comisión, difícilmente serán capaces de remediar los efectos nocivos producidos en los mercados y disuadir a los operadores de la puesta en práctica de futuros ilícitos anticompetitivos.

A tal efecto, existen diversos elementos que obstaculizan la atribución de responsabilidad por prácticas anticompetitivas llevadas a cabo mediante la utilización de cadenas de bloques: la opacidad en las redes blockchain, su estructura distribuida, así como la creciente autonomía de las aplicaciones que surgen a tenor de esta tecnología. En los sucesivos epígrafes aludiremos, respectivamente, a cada uno de ellos.

2.1. Opacidad en blockchain

La anonimidad es una de las cualidades intrínsecas de las cadenas de bloques, pertenezcan a la tipología a la que pertenezcan.

En redes públicas, las transacciones son visibles pero los participantes y sus identidades no (Deshpande et al., 2017, p. 3), ya sea por hallarse protegidas tras pseudónimos o por ocultarse tras otros mecanismos como “zero-knowledge proofs”³.

Por su parte, en redes privadas, las transacciones pueden ser confidenciales y los participantes pueden encontrarse identificados, pero también pueden no estarlo; otra posibilidad en estas blockchain cerradas es que la información sobre quién es quién en la cadena se encuentre restringida para que únicamente ciertos usuarios tengan acceso (Schrepele, 2019a, p. 290).

A pesar de las peculiaridades que albergan unos mecanismos y otros, así como de las diferencias entre ellos, todos poseen

3 Schrepele (2019b, p. 120) define las “zero-knowledge proofs” como la situación en la que “un ‘probador’ A puede probar que conoce la información X a un ‘verificador’ B sin comunicar ninguna información a B que no sea el hecho de que A conoce X”. Esta herramienta criptográfica permite que A no tenga que desvelar a B detalles como la identidad del destinatario en una transacción, granjeándole un completo anonimato.

un elemento en común: dificultan la identificación de los sujetos participantes en una cadena de bloques -en algunas redes incluso promueven la opacidad en las transacciones- y, como consecuencia, se constituyen como un ímprobo obstáculo a la tarea de imputar responsabilidad a sujetos concretos por actuaciones anticompetitivas específicas llevadas a cabo en el seno de un sistema blockchain.

A lo anterior debemos sumar las barreras de acceso que constituyen las redes “permisionadas” en las que, en adición, no cualquier sujeto puede acceder a la información contenida en la cadena.

En consecuencia, la detección e investigación de prácticas anticompetitivas llevadas a cabo por las autoridades de competencia queda claramente limitada, como también la posibilidad de identificar al infractor y poder, consecuentemente, relacionarle con el ilícito investigado.

2.2. Arquitectura distribuida de las cadenas de bloques

En un contexto de organizaciones descentralizadas como blockchain, que no son reconocidas como entidades legales (Schrepel, 2019a, p. 305) pero que operan en el tráfico jurídico y se encuentran integradas por sujetos cuyo objetivo se orienta en muchas ocasiones, directa o indirectamente, a la obtención de un lucro, resulta esencial la capacidad de dirimir responsabilidades por las posibles prácticas antijurídicas -y, específicamente, anticompetitivas- que puedan tener lugar en su seno.

El problema es que en cadenas de bloques abiertas, el hecho de que nadie dirija la red ni su funcionamiento, así como la circunstancia de que ningún participante posea el control sobre el sistema -y que, al mismo tiempo, sea como si todos los tuvieran- (Schrepel, 2019a, p.323), constituye un inconveniente desde la perspectiva de la posible atribución de responsabilidad a sujetos

concretos por lo que sucede en aquella. Ni los propios creadores de la cadena poseen, una vez puesta en marcha, ningún control sobre su acceso, forma de operar o mantenimiento (Schrepel, 2019b, p. 120).

¿Cómo podría entonces una agencia de competencia ser capaz de vincular a un participante de la cadena con un resultado anticompetitivo determinado mediante un nexo de responsabilidad?

Todo lo anterior es consecuencia de la arquitectura distribuida de las cadenas de bloques, característica congénita de esta tecnología que hace posible gran parte de las aplicaciones que auspicia y la disrupción que favorece pero que, asimismo, plantea interrogantes que pueden dar lugar a situaciones sumamente adversas desde un punto de vista legal.

Por otra parte, esta naturaleza permite la posibilidad de almacenar información en torno a una red internacional distribuida y operativa al margen de instituciones, autoridades centrales o gobiernos, toda vez que “no reside en un área de influencia específica de ninguna regulación o jurisdicción determinada” (Breu, 2017, p. 1).

En consecuencia, los criterios para determinar la jurisdicción competente o la legislación aplicable en estos entornos quedan en el terreno de lo indeterminado, lo que supone a su vez que se desconozca a qué autoridad de competencia corresponderá hacerse cargo de las cuestiones dimanantes de las plataformas blockchain en las que se hayan cometido los correspondientes ilícitos.

Lo anterior, además de constituir un grave problema de imputación de responsabilidad, se traduce en incertidumbre que afecta a cualquier operador que busque desarrollar su actividad con un cierto nivel de seguridad jurídica, circunstancia especialmente necesaria en transacciones de carácter internacional.

2.3. Creciente autonomía de las aplicaciones con base

blockchain

Cada elemento enunciado hasta este punto obstaculiza directa o indirectamente la atribución de responsabilidad por la comisión de conductas anticompetitivas a través de cadenas de bloques. No obstante, existe una realidad adicional que eleva la complejidad de la tarea aludida a un nivel muy diferente.

Se trata de la posibilidad de amalgamar una pluralidad de smart contracts y constituir sobre su base organizaciones, corporaciones y sociedades que operan de forma autónoma e “interactúan entre sí de manera descentralizada y distribuida” (Wright y De Filippi, 2015, p. 15).

Esaredtejidapormediodecontratosinteligentespuededarorigen a las conocidas como Organizaciones Autónomas Descentralizadas (DAOs), Corporaciones Autónomas Descentralizadas (DACs) y Sociedades Autónomas Descentralizadas (DASs).

Como su propia denominación sugiere, estas aplicaciones blockchain se configuran en torno a una estructura de smart contracts y códigos que determinan las directrices que las rigen y en base a las cuales actúan (Wright y De Filippi, 2015, p. 15), desprendiéndose así de la necesidad de ser dirigidas por sujetos concretos a los que poder hallar responsables por las posibles violaciones de la normativa que estas entidades puedan cometer en el desarrollo de su actividad.

El potencial del referido paradigma es extraordinario. El progresivo desarrollo de esta tecnología puede dar lugar a un incremento proporcional en la complejidad de los contratos inteligentes utilizados como sustento de estas entidades autónomas descentralizadas, en un contexto en el cual las DAOs, DACs y DASs desarrollen operaciones previamente programadas, y en el que incluso, eventualmente, prescindan de la necesidad de que terceros sujetos participen en la toma de decisiones, asumiendo tales funciones en una dinámica de creciente autonomía en la que puedan auto-programar sus propias operaciones, vinculadas a una

blockchain concreta (Swan, 2015, p. 23).

Adiferencia de lo que sucede con las entidades y organizaciones convencionales, que dependen de una dirección unitaria que planifica, organiza, implementa decisiones y controla la institución, y a quien se puede responsabilizar -incluso personalmente- por las desviaciones de la legalidad cometidas en su seno, las entidades autónomas descentralizadas a las que blockchain da lugar no dependen de ninguna institución ni autoridad. En consecuencia, ¿corresponde a sus creadores o promotores algún tipo de responsabilidad por lo que sucede en estos entornos?

Adicionalmente, estas entidades autónomas responden -a diferencia de las convencionales- a una estructura no solo políticamente descentralizada sino geográficamente distribuida, lo que implica que no se encuentran localizadas en ubicaciones específicas y que operan, como consecuencia, al margen de jurisdicciones y demarcaciones geográficas determinadas (Wright y De Filippi, 2015, p.54).

Lo antedicho evidencia una significativa incógnita en relación a la imputación de responsabilidad por las potenciales actuaciones antijurídicas llevadas a cabo por estas DAOs, DACs y DASs, que pueden asumir obligaciones, participar en el tráfico jurídico y desarrollar las más diversas actividades, pero que desplazan la voluntad de los sujetos a los que, tradicionalmente, se ha responsabilizado -sea o no de forma limitada- de las operaciones llevadas a cabo por las organizaciones que gestionan.

Como señalan Wright y De Filippi (2015, p.54) “es prácticamente imposible recuperar los daños u obtener una orden judicial contra una organización autónoma descentralizada”. La única excepción a tal afirmación reside en la posibilidad de programar en la estructura de la entidad autónoma la opción de que así sea.

Si blockchain permite prescindir de intermediarios en estas transacciones, y la voluntad de los empresarios o usuarios de estas entidades es desplazada por la capacidad de la propia tecnología

de tomar decisiones autónomas independientemente de terceros imputables, las cadenas de bloques se equiparan -en ese aspecto- a aplicaciones de decisión algorítmica o tecnologías como la Inteligencia Artificial, provocando que se vea gravemente afectada la capacidad de las autoridades concurrenciales para designar responsables y, eventualmente, sancionar las correspondientes vulneraciones de la normativa antitrust.

3. Conclusión

Hace años, se consideraba que blockchain era una tecnología muy prometedora, con gran proyección y potencial; hoy, los líderes de algunas de las mayores empresas del mundo han dejado de ver las cadenas de bloques como una tecnología útil para pasar a considerarlas como “parte integral de su innovación organizacional” (Deloitte, 2020).

Ayer blockchain era un horizonte de posibilidades con cierta volubilidad y que podía llegar a desdibujarse hasta desaparecer, sin haber llegado realmente a materializarse⁴; hoy, lo que ha desaparecido son las dudas acerca del carácter revolucionario de las cadenas de bloques y el crisol de oportunidades que ofrece, así como que se trata de una tecnología que ha venido para quedarse.

Ayer las cadenas de bloques eran el futuro, hoy son el presente. Mañana cambiarán el mundo.

No obstante, una de las tareas clave para los operadores económicos a todos los niveles, como también de autoridades y reguladores, reside en asegurarse de que los beneficios y utilidades que reporten las cadenas de bloques superen los retos e inconvenientes que suponen. En esa disyuntiva, los profesionales del derecho ocupan un lugar preeminente.

Cuando tiene lugar algún tipo de violación de la legalidad

4 Como ha sucedido a lo largo de los años con tecnologías que generaron mucha expectación y que, en cambio, acabaron cayendo en el olvido -¿quién recuerda ahora Google Glass? ¿Y Netscape?-

establecida, resulta imprescindible ser capaz de determinar a qué sujetos imputar responsabilidad, así como en qué medida, para poder posteriormente sancionar a los infractores que los cometieron y paliar, en la medida de lo posible, los efectos perniciosos de su conducta. Es por ello que en cualquier ordenamiento jurídico, ya pertenezca a la tradición del derecho común o continental, existe un sistema bien definido de imputación de responsabilidad.

Si no se puede establecer un nexo entre la conducta antijurídica cometida y un sujeto concreto, no será posible punir tal infracción con los medios de los que disponen las autoridades encargadas de la aplicación de la legislación vigente, y eso es precisamente lo que sucede en entornos blockchain por la anonimidad que facilitan, su naturaleza distribuida y la creciente autonomía de las aplicaciones a las que da lugar.

Ese es el dilema que plantea blockchain en relación a los ilícitos anticompetitivos cometidos en su seno y mediante el uso de las aplicaciones y herramientas que surgen a tenor de esta tecnología. Se trata de una problemática tan severa como para requerir de forma imperativa la pronta búsqueda y hallazgo de respuestas y soluciones efectivas, toda vez que lo contrario puede suponer la puesta en jaque del sistema de protección del derecho de libre competencia.

Bibliografía

Breu, S. (2017), Blockchains and Cybercurrencies Challenging AntiTrust and Competition Law. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081914

Capobianco, A. (2018), Blockchain Technology and Competition Policy – Issues paper by the Secretariat, Comité de Competencia de la Dirección de Asuntos Financieros y Empresariales, Organización para la Cooperación y el Desarrollo Económico (OCDE). Recuperado de [https://one.oecd.org/document/DAF/COMP/WD\(2018\)47/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf)

Deloitte (2020), Deloitte's 2020 Global Blockchain Survey: From promise to reality. Recuperado de https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf

Deshpande, A., Stewart, K., Lepetit, L. y Gunashekar, S. (2017), Understanding the landscape of Distributed Ledger Technologies/Blockchain: Challenges, opportunities, and the prospects for standards, British Standards Institution (BSI). Recuperado de https://www.rand.org/pubs/research_reports/RR2223.html

Krause, S.K., Natarajan, H., Gradstein, H.L. (2017), Distributed Ledger Technology (DLT) and Blockchain, FinTech Note N° 1, Banco Mundial. Recuperado de <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/177911513714062215/distributed-ledger-technology-dlt-and-blockchain>

Lianos, I. (2018), Gaining Competitive Advantage in the Digital Economy: Competition Law Implications, Research Paper Series (8), Centre for Law, Economics and Society. Recuperado de https://www.researchgate.net/publication/331442012_Blockchain_Competition_-_Gaining_Competitive_Advantage_in_the_Digital_Economy_Competition_Law_Implications

Schrepel, T. (2019a), Is Blockchain the death of Antitrust law? The Blockchain-Antitrust Paradox, Georgetown. Law Technology Review, Vol. 3.2. Recuperado de <https://ssrn.com/abstract=3193576> o <http://dx.doi.org/10.2139/ssrn.3193576>

Schrepel, T. (2019b), Collusion by Blockchain and Smart Contracts, Harvard Journal of Law and Technology, 33(1). Recuperado de <https://ssrn.com/abstract=3315182>

Swan, M. (2015), Blockchain, blueprint for a new economy, Estados Unidos: O'Reilly Media.

Szabo, N. (1994), Smart Contracts, Universidad de Ámsterdam. Recuperado de <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>

Wright, A. y De Filippi, P. (2015), Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Recuperado de <https://ssrn.com/abstract=2580664> o <http://dx.doi.org/10.2139/ssrn.2580664>

A utilização do blockchain como prova eletrônica do processo civil na Justiça Brasileira

The use of the blockchain as electronic evidence of civil proceedings in the Brazilian Courts

Miguel Carlos Cristiano ¹

Sumário: i – teoria geral das provas; ii – provas eletrônicas; iii – blockchain; perspectivas das provas eletrônicas; considerações finais; referências bibliográficas

Resumo: O presente artigo partirá de uma realidade social, onde um dos principais aspectos é a sociedade digital, instituída através da utilização do uso dos meios tecnológicos na vida cotidiana, não podendo passar despercebido pelo Poder Judiciário, na forma e instrumentação do processo civil contemporâneo que, apesar de prover substancial celeridade para a entrega da tutela jurisdicional ao cidadão, ainda se discute muito acerca da força probatória de tais instrumentos dentro da lide com inquietações genuínas como fragilidade de manipulação, e a instauração de incidentes de falsificação, chegando até ao desaparecimento da referida prova essencial para a demonstração da verdade, mas que será cada vez mais presente no cotidiano forense. Por isso, pela conjugação dos métodos dedutivo-indutivo e pela revisão de bibliografia jurídicas e tecnológicas, este artigo investigará, em um primeiro momento, o papel das provas no processo civil como instrumento de demonstração da verdade dos fatos e a especificidade da prova eletrônica, seja através da forma nata ou da forma digitalizada para, então, analisar a utilidade de uma ferramenta acessível a todos com a necessidade de pouco investimento, através da tecnologia do Blockchain abstratamente e para o processo civil atual, para, enfim, com base nessas premissas considerar os benefícios e riscos do uso de uma tecnologia de criptografia digital do blockchain como forma de conservar a prova no processo civil contemporâneo.

Palavra chave: Direito Digital; Blockchain, Provas

¹ Advogado e professor universitário junto a Universidade São Judas Tadeu, Mestre em direitos difusos e coletivos pela Universidade Metropolitana de Santos/Brasil, e_mail miguel.cristiano.adv@gmail.com

Abstract: This article will start from a social reality, where one of the main aspects is the digital society, established through the use of technological means in daily life, and cannot go unnoticed by the Judiciary, in the form and instrumentation of contemporary civil proceedings that, despite providing substantial speed for the delivery of jurisdictional protection to the citizen, there is still much debate about the evidential force of such instruments in dealing with genuine concerns such as fragility of manipulation, and the instigation of incidents of forgery, even to the disappearance of the aforementioned essential evidence for the demonstration of truth, but which will be increasingly present in daily forensics. Therefore, by combining deductive-inductive methods and revisiting legal and technological bibliography, this article will initially investigate the role of evidence in civil proceedings as an instrument to demonstrate the truth of facts and the specificity of electronic evidence, either through the innate form or the digitized form to then analyze the usefulness of a tool accessible to everyone with the need for little investment, through the technology of the Blockchain abstractly and for the current civil procedure, to, finally, based on these premises consider the benefits and risks of using a blockchain digital encryption technology as a way to preserve evidence in contemporary civil proceedings.

Keyword: Digital Law; Blockchain, Evidence

I -Teoria geral das provas

Intitula-se como prova todo meio pelo qual procura-se trazer as verdades dos fatos à lide, de modo que estas devem convencer o juiz que a parte possui o direito alegado, bem como deve ter o seu pedido apreciado.

É válido ressaltar que, tendo em vista o princípio da legalidade não será admitida prova ilícita, conforme previsão do art. 5º, LVI do texto constitucional do Brasil, logo é aquela obtida por meio contrário ao aceite em nosso ordenamento jurídico.

Nota-se no art. 369 do Código de Processo Civil Brasileiro que as partes têm o direito de utilizar de todos meios legais e inclusive, aqueles que não estão expostos na lei para provar a verdade dos fatos ou a defesa da imputação do ilícito.

Neste sentido, as provas constituem um papel fundamental

no processo, conforme ensina a doutrina: “a verdade é pressuposto ético do processo justo. Uma das fontes de legitimação da função judiciária é a verdade – veritas, non auctoritas faci iudicium. É necessariamente injusta a decisão baseada em falsa verificação das alegações de fato no processo. Daí existir uma relação teleológica entre prova e verdade – a prova visa à apuração da veracidade das alegações de fato”, esclarecendo, mais adiante, que, em sua concepção, “a verdade é um problema unitário – inexistente a possibilidade de separação entre verdade dentro e fora do processo – e pode ser satisfatoriamente definida a partir da ideia de correspondência.”²

Vale destacar que o direito de apresentar provas está intrinsecamente ligada ao princípio do contraditório e ampla defesa, previsto no art. 5º, LV, CF, e então temos o direito fundamental que deverá ser assegurado. Pedro Paulo Teixeira Manus complementa:

uma vez produzida a prova, é ela incorporada ao processo, resultando deste fenômeno da absorção que se torna irrelevante quem produziu esta ou aquela prova (salvo na análise do ônus da prova), sendo sua observância obrigatória ao julgador.³

Dito isso, com base no princípio do livre convencimento motivado, que tem sua fundamentação no art. 371, da legislação processual brasileira, uma prova não tem peso maior que outra, e em decorrência disso o juiz deve apurar todas que vierem aos autos e assim, proferir o seu entendimento.

Neste contexto o ordenamento Processual Português, em seu artigo 413, indica que:

“O tribunal deve tomar em consideração todas as provas produzidas, tenham ou não emanado da parte que devia produzi-las, sem prejuízo das disposições que declarem irrelevante a alegação de um facto, quando não seja feita por certo interessado.

2 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. São Paulo: Revista dos Tribunais, 2012, p. 656.

3 MANUS, P. P. T. O livre convencimento do juiz e a prova produzida nos autos, Revista Consultor Jurídico, 12 de abril de 2019, <https://www.conjur.com.br/2019-abr-12/reflexoes-trabalhistas-livre-convencimento-juiz-prova-produzida-autos>, acessado em 16/09/2021

Ademais, também estão vedadas as provas ilegítimas, isto é, aquelas que alteram a verdade dos fatos. Esta conduta denomina-se litigante de má-fé, sendo punível com multa de acordo com o art. 81 do Código de Processo Civil Brasileiro, cuja redação segue:

Art. 81. De ofício ou a requerimento, o juiz condenará o litigante de má-fé a pagar multa, que deverá ser superior a um por cento e inferior a dez por cento do valor corrigido da causa, a indenizar a parte contrária pelos prejuízos que esta sofreu e a arcar com os honorários advocatícios e com todas as despesas que efetuou.

Novamente a Legislação processual lusitana também implica sanções no seu artigo 542:

2-Diz-se litigante de má-fé quem, com dolo ou negligência grave:

- a) Tiver deduzido pretensão ou oposição cuja falta de fundamento não devia ignorar;
- b) Tiver alterado a verdade dos factos ou omitido factos relevantes para a decisão da causa;
- c) Tiver praticado omissão grave do dever de cooperação;
- d) Tiver feito do processo ou dos meios processuais um uso manifestamente reprovável, com o fim de conseguir um objetivo ilegal, impedir a descoberta da verdade, entorpecer a ação da justiça ou protelar, sem fundamento sério, o trânsito em julgado da decisão.

Portanto, a produção de provas é um elemento essencial para a efetividade da tutela jurisdicional do Estado, para controle dos conflitos existentes na sociedade através da aplicação da legislação processual, enfatizando que é lícito às partes, em qualquer tempo, juntar provas aos autos decorrentes de fatos posteriores da petição ou aqueles em que os envolvidos não tinham acesso as tais provas (art.435, Código de Processo Civil), sendo necessário intimar a outra parte para se pronunciar a respeito desta nova prova.

II – Provas eletrônicas

As provas eletrônicas foram, inicialmente regulamentadas no Brasil através da Lei n. 12.682 de 9 de julho de 2012, expõe em seu art. 2º, § 4º, o conceito de documento digitalizado, bem como, em

seu § 2º explana sobre a prova digital, senão vejamos:

§ 2º O documento digital e a sua reprodução, em qualquer meio, realizada de acordo com o disposto nesta Lei e na legislação específica, terão o mesmo valor probatório do documento original, para todos os fins de direito, inclusive para atender ao poder fiscalizatório do Estado. (Incluído pela Lei nº 13.874, de 2019)

§ 4º Os documentos digitalizados conforme o disposto neste artigo terão o mesmo efeito jurídico conferido aos documentos microfilmados, nos termos da Lei nº 5.433, de 8 de maio de 1968, e de regulamentação posterior. (Incluído pela Lei nº 13.874, de 2019)

No que tange às transações realizadas de maneira online, a fim de trazer segurança jurídica a relações, foi instuída a Medida Provisória Nº 2.200-2/2001, que regulou a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, visando garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica.

Nas palavras de Antônio Terêncio G. L. Marques, documento eletrônico “[...] nada mais representa que uma sequência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de um fato.”⁴

Como afirma Elpídio Donizetti, “o certificado digital consiste numa estrutura de dados sob a forma eletrônica que associa o nome e atributos de uma pessoa a um par de chaves. Essa estrutura é montada com a utilização da criptografia assimétrica ou de chaves públicas”, pois, para ele:

A criptografia de chaves públicas consiste num método que utiliza duas chaves, constituídas por uma extensa combinação de letras e números (algoritmo), criadas por um programa de computador. A chave privada ou privativa é de domínio do titular do certificado digital, ao passo que a chave pública poderá ser amplamente divulgada. Assinar digitalmente consiste em aplicar sobre a mensagem, constante de um meio virtual (texto escrito no computador, por exemplo), a chave privada (ou privativa), isto é, o código pessoal do usuário, detentor do certificado digital, o que pode ser feito com a inserção, num dispositivo adequado, do

4 MARQUES, Antônio Terêncio G. L. A prova documental na internet. 1. ed. 6ª reimpr. Curitiba: Juruá, 2011, p. 127)

cartão magnético (tal como ocorre nos caixas eletrônicos) ⁵

A inserção do art. 422 no Código de Processo Civil Brasileiro nos trouxe ideias a respeito de fotografias dispostas na internet, em revistas ou jornais e mensagens de textos. Estes meios podem ser utilizados como provas, mas em caso de impugnação deverá ser apresentar a autenticação, e nos casos de revistas e de mensagens, faz-se necessário apresentar o arquivo original.

Em complemento à análise acima, no âmbito eletrônico podemos conceituar que um documento digital, codificado através de código binários, pode ser considerada como digitalizado, sendo a representação digital de um documento produzido em outro formato (físico) e que, por meio da digitalização, foi convertido para o formato digital e o documento nato digital é o documento que nasceu em formato digital, tal como um documento produzido pelo Libreoffice, por uma câmera digital e tantos outros que nascem no formato digital ⁶

Foi publicado, em março de 2020, o Decreto Federal nº 10.278, que dispõe da validade jurídica e legal de documentos digitalizados, visando colocar em prática um dos principais conceitos da Lei da Liberdade Econômica, que é a desburocratização e a modernização do mercado brasileiro.

Vanderlei Batista dos Santos explana sobre arquivo digital, bem como, nos alerta:

“Vale ressaltar que um documento digital não é uma unidade simples, mas sim composto por um conjunto de componentes digitais que definem sua estrutura, tipo, tamanho e cores das fontes, existência de imagens etc”⁷

5 DONIZETTI, Elpidio. Atos praticados por meio eletrônico. PORTAL IED – INSTITUTO ELPIDIO DONIZETTI, 2016. Disponível em: <https://portalied.jusbrasil.com.br/noticias/379242852/atos-praticados-por-meio-eletronico>, acessado em 16/09/2021.

6 ALVARINO, Priscila. Assinatura Digital: Validade Jurídica, aplicações e benefícios, Revista Consultor Jurídico, 11 de agosto de 2021, <https://www.conjur.com.br/2021-ago-11/alvarino-assinatura-digital-validade-aplicacoes-beneficios>, acessado em 19/09/2021

7 SANTOS, Vanderlei Batista dos. A prática arquivística em tempos de gestão do conhecimento. In: SANTOS, Vanderlei Batista dos. Arquivística: temas contemporâneos. Brasília: Senac, 2007. p. 175-223

O autor supracitado expõe que a tecnologia evidenciou um novo paradigma para a preservação do documento na ciência arquivística. Percebe-se que no Direito também enfrentamos esse dilema quando temos que constatar se houve ou não adulteração em uma prova digital, senão vejamos (Sant'Anna, 2001, p.7):

“Tal como o papel se desintegra com o passar dos anos, a informação gravada na superfície metálica magnetizada dos dispositivos de armazenamento mais largamente utilizados, pode também tornar-se irrecuperável”

Com isso, o nosso anseio é preservar a mídia digital e ter ferramenta para apurar quando esta foi modificada ou adulterada.

Esta referida unidade é fruto do Ministério da Ciência, Tecnologia e Inovações (MCTI), que possui como uma das competências promover políticas nacionais de pesquisa científica e tecnológica e de incentivo à inovação. Dessa forma, com a intensificação de pesquisas a respeito de documentos digitais (construção, aspectos alteráveis), é possível que tenhamos mais segurança nesses tipos de arquivos.

Essa ideia de conservar o mesmo conteúdo é muito benéfica quando trazemos essa lógica para uma prova digitalizada, posto que, esta é umas das formas de manter a autenticidade deste arquivo conservando seus elementos.

A medida que a preservação digital for fomentada, gozaremos das provas digitais com maior tranquilidade no Direito. A ideia é que se utilizamos um áudio como meio de prova, é necessário que consigamos identificar se os componentes digitais são ou não os mesmos da data da criação do arquivo. Tornando-se exequível a identificação de possíveis adulterações.

III - Blockchain

O blockchain trata-se de um banco de dados que responde ao nosso dilema delineado no tópico anterior, sendo esclarecido por Natalia Marques do Santos como: a tecnologia propõe

imutabilidade, transparência e descentralização como medida de segurança, funcionando como um livro-razão público sem o intermédio de terceiros. Trata-se de uma base de dados distribuída que guarda um registro de transações permanentes e à prova de violação, não podendo ser alterada, eis que armazena informações em blocos dependentes uns dos outros, formando uma cadeia de blocos.⁸

Essa tecnologia permite realizar e manter transações de forma rápida e segura. A priori, era utilizada apenas para realizar operações com a criptomoeda Bitcoin. No entanto, outras organizações têm utilizado este software conforme sua necessidade de demanda.

Em síntese, cada informação adicionada através da tecnologia blockchain torna-se imutável, e conseqüentemente, um nova informação vai resultar em um novo código, denominado hash.

Cabe ressaltar que a alteração será permitida caso seja feita com a assinatura eletrônica mediante chave privada. Portanto, todos os dados e detalhes do fato permanecem registrados, resultando em uma prova ágil e mais econômica que uma ata notarial.

Essas características do blockchain também são decorrentes do fenômeno da criptografia, cuja funcionalidade é caracterizado em codificar uma transação ou conversa no âmbito digital para que outrem não tenha acesso. Muitos bancos digitais e ferramentas como o WhatsApp já possuem tal proteção.

Portanto, a prova colhida através da ferramenta tecnologica do Blockchain, reveste o referido conteúdo de autenticidade, uma vez que seu conteúdo é armazenado através de uma criptografia que traz autenticidade as informações colhidas, bem como, ao tempo da sua exibição.

IV - Perspectivas da utilização de provas eletrônicas no Processo Civil Brasileiro

8 SANTOS, N.M., As contribuições para o mundo do Direito da tecnologia blockchain, Revista Consultor Jurídico, Disponível em <https://www.conjur.com.br/2020-mai-12/natalia-santos-tecnologia-blockchain-direito>, acessado em 16/09/2021.

O uso da tecnologia advindas do meio digital está cada vez mais intrínseco às nossas vidas. É sabido que até no Direito das Sucessões discute-se sobre a questão dos bens digitais, e em outros ramos não é diferente.⁹

A possibilidade de utilizar o meio eletrônico e as provas digitais correspondem ao princípio da duração razoável do processo, conforme preceituado no art. 5º, LXXVIII, da Constituição Federal, tendo em vista a celeridade e a praticidade destas ferramentas. Por conseguinte, apenas cabe a nós aprender a lidar com tais recursos e assegurar as garantias constitucionais e das demais legislações.

Nessa perspectiva, a validade jurídica do documento eletrônico como meio de prova está condicionada à observância da autenticidade, integridade, perenidade e tempestividade do documento eletrônico. Portanto, resta cristalino que os mecanismos que nos auxiliam nesta autenticação são a assinatura eletrônica, o blockchain e criptografia, por exemplo.

No julgado abaixo verificou-se que o printscreen (foto da imagem do computador) apresentado pela autora não tinha o valor probatório que ela pretendia lhe impingir, conforme voto preferido pela Justiça Estadual de São Paulo:

Sucedê que a simples impressão de tela sistêmica não é suficiente à comprovação de que houve o desencaixe financeiro, por cuidar se de documento produzido unilateralmente, que não permite aferir a veracidade de seu conteúdo, nem afirmar, com segurança, que o pagamento teria efetivamente ocorrido¹⁰

Todavia, vale ressaltar que o juiz “[...]” poderá se valer de outras provas capazes de esclarecer a origem e assegurar a veracidade do documento eletrônico, que não passou pelos mecanismos

9 LACERDA, Bruno Torquato Zampier. Bens Digitais. 2. ed. São Paulo: Foco, 2021

10 BRASIL, Tribunal de Justiça do Estado de São Paulo, Apelação Cível nº 1006313-68.2018.8.26.0344 Comarca de Marília / 2ª Vara Cível Juiz(a): Ernani Desco Filho Apelante(s): Companhia Paulista de Força e Luz Apelado(a)(s): Bradesco Auto/Re Cía de Seguros.Relator(a): Sandra Galhardo Esteves. Data do julgamento: 11/02/2019).

certificatórios do ICP Brasil”¹¹

Nos últimos anos, advogados passaram a utilizar evidências digitais em tribunais e cortes de muitos países. Entretanto, para que sejam consideradas provas válidas o perito deve realizar o processo de investigação cuidadosa e sistematicamente, desse modo preservando as evidências e as documentando detalhadamente, com a finalidade de autenticá-las.¹²

Neste sentido, a difusão do conhecimento digital à população e o aprimoramentos dos peritos são ferramentas que nos ajudarão a compreender esse cenário, e conseqüentemente, resultarão em reflexos positivos no âmbito processual. As palavras de Donizetti compreendem o nosso raciocínio:

“Além da assinatura digital, outros conceitos relacionados à informática jurídica precisam ser compreendidos pelos operadores do direito a fim de que a automação processual não se torne um entrave ao acesso à justiça, mas, sim, uma forma mais célere de alcançá-la”¹³

Portanto, podemos compreender através dos apontamentos trazidos neste artigo que a legislação vigente, tanto brasileira como portuguesa não necessitam de qualquer alteração para que o documento eletrônico, para que seja alçado ao mesmo o status de meio de prova.”, limitando a sua discussão a respeito em como trazer mais segurança através das tecnologias e não apenas estabelecer normas.

V - Considerações finais

No ordenamento processual civil brasileiro temos alguns tipos de provas elencados, nas quais é coeso refletirmos a extensão de

11 THEODORO JÚNIOR, Humberto. Curso de Direito Processual Civil, 59.^a ed, v. I. Rio de Janeiro: Forense, 2018, p. 1019

12 PEREIRA, E; FAGUNDES, L; NEUKAMP, P et al. Forense Computacional: fundamentos, tecnologias e desafios atuais. Em VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, p. 3-53, Rio de Janeiro, RJ, 2007

13 DONIZETTI, Elpidio. Atos praticados por meio eletrônico. PORTAL IED – INSTITUTO ELPIDIO DONIZETTI, 2016. Disponível em: <https://portalied.jusbrasil.com.br/noticias/379242852/atos-praticados-por-meio-eletronico>, acessado em 16/09/2021.

algumas destas provas para o nosso âmbito atual, onde o custo e o tempo para efetivação do registro tornar a prova eletrônica mais interessante, tendo em vista que uma publicação na internet pode ser deletada em fração de segundos.

Com isso, nós avançamos neste aspecto seja através do advogado que traz uma comprovação via blockchain, e que, caso eventualmente apresente documento falso será devidamente penalizado, bem como seu representado, ou da empresa que detém de sistemas de seguranças de suas informações, e com isso, evitam o cometimento de ilícito.

Por fim, os dilemas da volatilidade dos arquivos digitais estão interligados com a ciência tecnológica com a nossa legislação atual. A medida que tivermos mais meios tecnológicos para identificar alterações nessas provas debruçadas, a arguição de falsidade, tanto material quanto ideológica, não será difícil ser ventilada no processo judicial.

Referencias Bibliográficas

ALVARINO, Priscila. Assinatura Digital: Validade Jurídica, aplicações e benefícios, Revista Consultor Jurídico, 11 de agosto de 2021, Disponível em <https://www.conjur.com.br/2021-ago-11/alvarino-assinatura-digital-validade-aplicacoes-beneficios>, acessado em 19/09/2021

BRASIL, Tribunal de Justiça do Estado de São Paulo, Apelação Cível nº 1006313-68.2018.8.26.0344 Comarca de Marília / 2ª Vara Cível Juiz(a): Ernani Desco Filho Apelante(s): Companhia Paulista de Força e Luz Apelado(a)(s): Bradesco Auto/Re Cia de Seguros.Relator(a): Sandra Galhardo Esteves. Data do julgamento: 11/02/2019).

DONIZETTI, Elpidio. Atos praticados por meio eletrônico. PORTAL IED – INSTITUTO ELPIDIO DONIZETTI, 2016. Disponível em: <https://portalied.jusbrasil.com.br/noticias/379242852/atos-praticados-por-meio-eletronico>, acessado em 16/09/2021.

FURNO, Carlo. Contributo Alla Teoria Della Prova Legale.. Padova: Cedam, 1940, p. 16-17.)

MANUS, P. P. T. O livre convencimento do juiz e a prova produzida nos autos, Revista Consultor Jurídico, 12 de abril de 2019, Disponível em <https://www.conjur.com.br/2019-abr-12/reflexoes-trabalhistas-livre-convencimento-juiz-prova-produzida-autos>, acessado em 16/09/2021

MARQUES, Antônio Terêncio G. L. A prova documental na internet. 1. ed. 6ª reimpr. Curitiba: Juruá, 2011, p. 127

SANTOS, Vanderlei Batista dos. A prática arquivística em tempos de gestão do conhecimento. In: SANTOS, Vanderlei Batista dos. Arquivística: temas contemporâneos. Brasília: Senac, 2007. p. 175-223

SANTOS, N.M., As contribuições para o mundo do Direito da tecnologia blockchain, Revista Consultor Jurídico, Disponível em <https://www.conjur.com.br/2020-mai-12/natalia-santos-tecnologia-blockchain-direito>, acessado em 16/09/2021.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. São Paulo: Revista dos Tribunais, 2012, p. 656

SILVA, A.R., SUCESSÃO DE BENS DIGITAIS: a imprescindibilidade da adequação do ordenamento jurídico às necessidades demandadas pelo novo cenário social, Revista Consultor Jurídico, Disponível em <https://jus.com.br/artigos/90702/sucessao-de-bens-digitais-a-imprescindibilidade-da-adequacao-do-ordenamento-juridico-as-necessidades-demandadas-pelo-novo-cenario-social>, acessado em 20/09/2021.

PEREIRA, E; FAGUNDES, L; NEUKAMP, P et al. Forense Computacional: fundamentos, tecnologias e desafios atuais. Em VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, p. 3-53, Rio de Janeiro, RJ, 2007

THEODORO JÚNIOR, Humberto. Curso de Direito Processual Civil, 59.ª ed, v. I. Rio de Janeiro: Forense, 2018, p. 1019

O digital como prioridade da Comissão Europeia: breve análise sobre a transformação digital no âmbito da União Europeia

Digital as a priority of the European Commission: a brief analysis on digital transformation in the European Union

Dora Resende Alves¹

Ana Carolina Assumpção Stoffel²

Sumário: 1. Introdução; 2. O digital como prioridade da Comissão Europeia: o Regulamento (UE) 2021/694 e breves reflexões sobre seus reflexos no atual cenário eurocomunitário; 3. A Inteligência Artificial (IA) no direito da União Europeia; 4. Plano para transformação digital da Europa; 5. Considerações finais; Referências bibliográficas.

Resumo: O presente artigo resulta de estudo realizado na área do direito da União Europeia quanto ao uso e inserção das tecnologias facilitadoras no âmbito da UE. Tal questão é de grande importância no atual contexto, considerando que em 2021 a União Europeia estabeleceu um plano de transformação digital da Europa, o qual deve ser totalmente efetivado até 2030. Em que pese a inegável importância que a tecnologia tem adquirido no dia a dia não só das empresas, mas também dos cidadãos e da Administração Pública, é igualmente importante a preocupação com riscos advindos do uso do digital, como, mas não se restringindo, a proteção de dados, ambiente digital seguro, não exclusão dos grupos com potencial menor acesso a tais tecnologias digitais. Diante disso, é que se propôs a análise do digital como prioridade da Comissão Europeia, buscando-se demonstrar os principais pilares em que a União se está a alicerçar para a transformação digital, bem como os principais pontos de atenção que estão sendo observados. Para a elaboração do trabalho proposto, foram utilizadas doutrina europeia, sobretudo portuguesa, bem como documentação do direito da União Europeia.

1 Docente na Universidade Portucalense Infante D. Henrique. Investigadora do Instituto Jurídico Portucalense. Mestre e Doutora em Direito da Integração Europeia. E-mail: dra@upt.pt

2 Pós-graduada em Direito Internacional, pós-graduada em Direito Tributário, mestranda em Ciências Jurídico-Políticas, pela Universidade Portucalense (UPT, Portugal), Email: ac.astoffel@gmail.com

Palavras-chave: Tecnologia. União Europeia. Transformação digital.

Abstract: This article is the result of a study carried out in European Union law regarding the use and insertion of new technologies in the EU. This issue has great importance in the nowadays, considering that in 2021 the European Union established a plan for the digital transformation of Europe, which must be fully implemented by 2030. Despite the undeniable importance that technology has acquired in the daily lives not only of companies, but also of citizens and the Public Administration, the concern with risks arising from the use of digital is also important, such as, but not restricted to, data protection, secure digital environment, non-exclusion of groups with less potential access to such technologies. In this context is that it is analyzed the digital as a priority for the European Commission, seeking to demonstrate the main pillars on which the Union is building its foundation for digital transformation, as well as the main points of attention that are being observed. For the preparation of the proposed work, European doctrine was used, mainly Portuguese, as well as documentation of European Union law.

Keywords:. Technology. European Union. Digital transformation.

1. Introdução

Vivemos tempos de extrema digitalização, contexto este em que as tecnologias deixaram de ser um privilégio intramuros das empresas e indústrias e passaram a ser parte do cotidiano das pessoas singulares, empresas de pequeno porte e da Administração Pública.

É neste contexto que, rumo ao futuro e aproveitando os benefícios do desenvolvimento tecnológico, notadamente pela Revolução 4.0³, a União Europeia (UE) vem imprimindo esforços para utilizar tais meios de comunicação e informação (TIC) com maior rapidez, bem como seus benefícios, no dia-a-dia dos Estados-membros: uso de inteligência artificial para agilizar os serviços públicos prestados pelos Estados; algoritmos para descartar informações irrelevantes e selecionar dados sensíveis e que merecem atenção do Administrador; acesso amplo e irrestrito

3 Caso o leitor queira se aprofundar sobre a mencionada Resolução, recomenda-se: SCHWAB, Klaus (2016). A quarta Revolução Industrial. São Paulo: Edipro.

à internet 5G para toda sociedade⁴, inclusive aqueles em áreas remotas e idosos; aceleração de crescimento das pequenas empresas; benefícios da interoperabilidade⁵, entre outros, no âmbito da justiça eletrónica⁶.

Por outro lado, para cada avanço planejado, há outras preocupações, sendo uma que merece grande destaque, a segurança no âmbito cibernético. Isso porque de nada adianta criar-se um plano e levar-se a cabo estratégias de transformação digital do Bloco se os cidadãos não sentirem confiança em usar os meios tecnológicos para isso. É necessário que se garanta segurança e confiabilidade, para que a busca pela digitalização em ritmo acelerado não encontre óbices pelos próprios destinatários: os cidadãos.

Em razão do cenário acima explicitado, procurou-se primeiramente verificar como está sendo tratada a inserção das tecnologias digitais no âmbito legal, pela União Europeia, e, posteriormente, quais são as principais características, estratégias e cautelas que a UE tem tomado diante de tal contexto.

Faz-se, de acordo com o assunto focado, uso de variados endereços eletrónicos ao longo do texto, para acesso e como fonte, visto que a utilização das plataformas informáticas é parte do tema. Apesar de discutível valor académico, recorre-se aqui à disponibilização de endereços que serão a forma de acesso eficaz e que demonstram algumas das ideias desenvolvidas pelas autoras.

4 Ver COMITÉ ECONÓMICO E SOCIAL EUROPEU (2021). Parecer 2021/C 374/03.

5 ABREU, Joana Rita de Sousa Covelo de (2019). A justiça eletrónica europeia e a modernização do espaço de liberdade, segurança e justiça.... In: CARVALHO, Maria Miguel et al (Coord.). Democracia económica e responsabilidade social nas sociedades tecnológicas. Braga: UMINHO, p. 104.

6 ABREU, Joana Covelo de (2020). O sentido amplo de Contencioso da União Europeia e a justiça eletrónica europeia.... In: ABREU, Joana Covelo de et al (Coords.). O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia (e-Justice).

2. O digital como prioridade da Comissão Europeia: o Regulamento (UE) 2021/694 e breves reflexões sobre seus reflexos no atual cenário eurocomunitário

A Comissão Europeia, na sua formação 2019-2024, apresentou como uma das suas prioridades o desenvolvimento digital, concretizado no ano de 2021 através do Regulamento (UE) 2021/694 exarado conjuntamente pelo Parlamento Europeu e Conselho. O documento normativo reflete o anseio do Direito da União em estabelecer princípios e diretrizes estratégicas para o “Programa Europa Digital”.

Tal normatização não é uma surpresa, posto que reflete a necessidade de se regulamentar o uso das tecnologias digitais⁷, como, mas não apenas, o uso da inteligência artificial. Como explicitado no preâmbulo do Regulamento,

(...) a União deverá dar uma resposta urgente às tendências emergentes, incluindo, analisar questões como a inteligência artificial (IA) e as tecnologias de livro-razão distribuído (por exemplo, cadeias de blocos) e, ao mesmo tempo, assegurar um nível elevado de proteção de dados, em plena conformidade com o Regulamento (UE) 2016/679, com os direitos digitais, os direitos fundamentais e com os padrões éticos.⁸

Ainda que apenas em 2021 o Regulamento tenha surgido, regista-se que já se encontravam anteriores documentos

7 “Según la Comisión Europea, una tecnología facilitadora es aquella que proporciona elementos tecnológicos que permiten el desarrollo de nuevos productos, procesos y servicios con mayor valor añadido. Es decir, son tecnologías de ámbito general aplicables, por tanto, a múltiples sectores industriales que sirven de base para otras actividades de desarrollo e innovación. Tomemos, por ejemplo, la robótica, una tecnología considerada facilitadora. Se puede emplear para automatizar procesos en otros sectores, sin necesidad de conocer su funcionamiento interno ni sus detalles básicos. Los desarrolladores de la tecnología se han preocupado de facilitar el acceso a la misma a otros desarrolladores, para que estos, a su vez, la empleen como elemento para integrar en sus procesos de fabricación” (BLANCO SILVA, Fernando, CASTRO PÉREZ, José Manuel, GAYOSO TABOADA, Rubén A., SANTANA ALONSO, Wilfredo (2019). Las claves de la cuarta revolución industrial. Libros de Cabecera: Barcelona, p. 17).

8 PARLAMENTO EUROPEU e CONSELHO (2021). Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de abril de 2021 que cria o Programa Europa Digital.

institucionais sobre o uso da inteligência artificial na União Europeia em discussão e debate nos órgãos de representação normativa da União Europeia. Ou seja: verifica-se que a busca por regulamentar as novas tecnologias já é alvo de debates no direito eurocomunitário, dada a sua grande e inegável presença na sociedade contemporânea.

A busca pela regulamentação, desde o esboço e discussões entabuladas nos anos anteriores (desde 2007 mas mais organizada a partir de 2015) em busca de esforços conjuntos dos Estados que compõem a UE, reflete per se uma realidade não difícil de se verificar: a inteligência artificial e demais tecnologias digitais como prioridade para a Comissão Europeia. Assim não fosse, não teria a Comissão encetado esforços em debates e deliberações durante anos para promover e viabilizar a redação que resultou no Regulamento (UE) 2021/694.

É notório que as ciências jurídicas, como parte integrante das ciências sociais aplicadas, busca regulamentar situações importantes nas relações humanas. Como colocado de modo brilhante pelo jurista austríaco, Hans Kelsen, “o Direito é uma ordem normativa da conduta humana, ou seja, um sistema de normas que regulam o comportamento humano”⁹. Considerando o ascendente uso e desenvolvimento da inteligência artificial no dia a dia dos cidadãos europeus, justifica-se a necessidade e anseio do direito da União buscar respaldo jurídico para o novo cenário em que os Estados e seus povos se encontram.

Feitas tais considerações, propõe-se uma breve análise sobre como a tecnologia e o Plano de transformação digital têm sido tratados no âmbito europeu e suas principais implicações.

3. A Inteligência Artificial (IA) no Direito da União Europeia

9 KELSEN, Hans (2009). Teoria pura do direito. São Paulo: Martins Fontes, p. 4). Nesse mesmo sentido, disserta: SILVA, José Afonso da (2011). Curso de Direito Constitucional Positivo. São Paulo: Malheiros Editores, p. 121.

Conforme visto, uma das tecnologias de grande ênfase para a União Europeia é a inteligência artificial, sendo explicitamente considerada uma das cinco áreas de atenção no Regulamento (UE) 2021/694.

Para o direito da União Europeia,

[o] conceito de inteligência artificial (IA) aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas — com um determinado nível de autonomia — para atingir objetivos específicos. Os sistemas baseados em inteligência artificial podem ser puramente confinados ao software, atuando no mundo virtual (por exemplo, assistentes de voz, programas de análise de imagens, motores de busca, sistemas de reconhecimento facial e de discurso), ou podem ser integrados em dispositivos físicos (por exemplo, robôs avançados, automóveis autónomos, veículos aéreos não tripulados ou aplicações da Internet das coisas).¹⁰

Da conceituação supra transcrita, verifica-se que a inteligência artificial se relaciona com outras tecnologias facilitadoras, como a Internet of Things (IoT), embora sem se limitar a ela, podendo esta ser compreendida, de forma breve, como o cenário em que coisas que são parte do quotidiano das pessoas possuem tecnologia suficiente (ou seja, inteligência artificial) para se conectarem à rede mundial de computadores e promoverem a interação do mundo físico com o virtual de forma instantânea e por si próprias¹¹.

Como bem colocado por Blanco Silva et al, a inteligência artificial busca, dentre outros, assimilar e informatizar o raciocínio humano, de forma de, indo ao encontro da definição da Comissão Europeia transcrita no começo desta secção, tomar decisões de forma autónoma ou a mais autónoma e apurada possível¹².

O uso da inteligência artificial levanta inúmeros problemas dos quais se destacam as preocupações com os direitos humanos e

10 COMISSÃO EUROPEIA (2018). Documento COM(2018) 237 final, p. 1.

11 PUYOL, Javier. Del Internet de las cosas al Internet de los cuerpos. [em linha] [consult. 20 Abr 2020]. Disponível em <https://confilegal.com/20190317-del-internet-de-las-cosas-al-internet-de-los-cuerpos/>

12 BLANCO SILVA, Fernando, CASTRO PÉREZ, José Manuel, GAYOSO TABOADA, Rubén A., SANTANA ALONSO, Wilfredo (2019). Las claves de la cuarta revolución industrial. Libros de Cabecera: Barcelona, pp. 39-43.

com a segurança. Em ambos o caso a União Europeia está atenta, como resulta do relatório sobre a Inteligência Artificial e Direitos Fundamentais (Getting the future right – Artificial intelligence and fundamental rights)¹³ publicado 14 de Dezembro de 2020 pela FRA – Agência dos Direitos Fundamentais da União Europeia (fra.europa.eu)¹⁴.

Tal preocupação encontra-se igualmente externada na Comunicação citada acima, posto que a União Europeia visa regulamentar o uso da inteligência artificial para fins de garantir a segurança e a defesa dos direitos fundamentais das pessoas e das empresas, reforçando o investimento, a inovação e a utilização da dita tecnologia em toda a União Europeia¹⁵.

Neste contexto, a União Europeia sublinha a importância da educação sobre si própria, isto é, preocupa-se em manter uma política de transparência e confiança dos cidadãos: busca-se dar informação e tornar acessível o seu próprio funcionamento, deliberações, normativas e existência para que o cidadão europeu possa ser participante consciente do processo de integração europeu¹⁶. Não é inequívoco o acesso ao conhecimento sobre a União Europeia fora dos meios académicos relacionados com esta ordem jurídica ainda relativamente nova, com 70 anos celebrados.

As solicitações de participação cívica surgem cada vez mais pela via digital, na forma de consulta pública em variados temas¹⁷, por vezes, de forma prévia a um processo decisório, como forma de participação democrática em processos de intervenção rumo

13 Em: Getting the future right – Artificial intelligence and fundamental rights (europa.eu)

14 Em Acerca da FRA | European Union Agency for Fundamental Rights (europa.eu)

15 COMISSÃO EUROPEIA (2021). Documento COM(2021) 206 final.

16 SILVA, M. M. M., & ALVES, D. R. (2021). Education for access to European Union Law through the use of digital technologies.

17 Neste mesmo propósito digital, ver em EUSurvey - Survey (europa.eu)

a uma iniciativa legislativa¹⁸ ou simples convite a participação em eventos como é já a Conferência sobre o Futuro da Europa¹⁹ lançada em maio de 2021²⁰. Para que estas participações sejam possíveis em consciência e conhecimento, há um processo educativo e de inclusividade²¹ a desenvolver no sentido de tornar os cidadãos mais capacitados a intervir e exercer os seus direitos.

Todos as instituições, órgãos e organismos da União Europeia²² surgem envolvidos nesta construção, como se constata com o Comité Económico e Social Europeu que

saúda o lançamento da iniciativa [da Comissão Europeia «Orientações para a Digitalização até 2030»] e o objetivo de utilizar as tecnologias digitais para melhorar as vidas dos cidadãos, criar mais postos de trabalho, facilitar o progresso e reforçar a competitividade europeia. A pandemia realçou a importância e as possibilidades decorrentes do desenvolvimento digital, vincou a necessidade de efetuar ajustamentos e mudou o modo como socializamos e trabalhamos. A UE tem de dar uma resposta adequada a estes desafios. Para transformar as intenções em resultados, é essencial dispor de uma estratégia, um plano com objetivos específicos e uma forma de avaliar os progressos.²³

4. Plano para Transformação Digital da Europa

Além do Regulamento (UE) 2021/694, outro aspeto que merece atenção quanto a prioridade da Comissão Europeia face à era digital teve lugar em 9 de março de 2021: a Comissão apresentou um plano para que a transformação digital da Europa seja efetivada

18 Vejam-se os processos de iniciativa de cidadania europeia em Início | Iniciativa de cidadania europeia (europa.eu). Conforme ALVES, D. R., & SILVA, M. M. M. (2021). A iniciativa legislativa de cidadãos como instrumento de democracia: destaque para a União Europeia, e comunicação de Dora Resende Alves e Mário Simões Barata no I Congresso Internacional sobre os Novos Desafios dos Direitos Humanos (I CINDHU), Universidade Federal de Uberlândia (UFU), Brasil, 23 de julho de 2021 no tema “A iniciativa de cidadania europeia na jurisprudência do Tribunal de Justiça da União Europeia” (ainda não publicado).

19 Também em Conference on the Future of Europe (europa.eu)

20 Ver em Conferência sobre o Futuro da Europa (mne.gov.pt)

21 Ver COMITÉ ECONÓMICO E SOCIAL EUROPEU (2021). Parecer 2021/C 374/03.

22 Ver ABREU, Joana Rita de Sousa Covelo de, & REIS, Liliana (2020). Instituições, Órgãos e Organismos da União Europeia. Almedina.

23 COMITÉ ECONÓMICO E SOCIAL EUROPEU (2021). Parecer 2021/C 374/05.

até 2030²⁴. Esta visão para a década digital da UE fundamenta-se em quatro principais pilares, refletindo, assim, atenção especial do Parlamento Europeu em quatro áreas prioritárias, quais sejam: competências, governo, empresas e infraestruturas²⁵.

Por competências pode-se considerar a priorização da UE em desenvolver a capacidade relativa às tecnologias no âmbito da informação e comunicação em pelo menos 20 milhões de cidadãos europeus, bem como promover a inclusão em competências digitais básicas de, no mínimo, 80% dos cidadãos europeus. Tal necessidade vai de encontro ao Parecer do Comité Económico e Social Europeu (CESE), segundo o qual é importante manter e estimular o progresso do uso das tecnologias facilitadoras, inclusive no âmbito da prestação de serviços públicos, porém, sem deixar de capacitar os cidadãos para fazer o uso das mesmas, sob pena de se institucionalizar uma exclusão das pessoas, notadamente de grupos vulneráveis, como idosos, pessoas com pouco poder aquisitivo, moradores de áreas remotas ou rurais ou com deficiência cognitiva²⁶.

No que diz respeito ao âmbito governamental, a preocupação primária da UE respalda-se na prestação de serviço público de forma contínua, de qualidade e amplamente acessível a todos. Contudo, não basta tal amplitude, é necessário, como ponderado pelo CESE, que haja confiança dos cidadãos tanto em matéria de

24 COMISSÃO EUROPEIA (2021). Orientações para a Digitalização até 2030. Documento COM(2021) 118 final.

25 Disponível em *Década Digital da Europa: objetivos digitais para 2030* | Comissão Europeia

26 “A acessibilidade em linha de todos os serviços públicos europeus e nacionais é um objetivo legítimo. Contudo, o CESE chama a atenção para a necessidade de ninguém ficar para trás e para o facto de que é indispensável apoiar as pessoas que não podem beneficiar imediatamente do processo de digitalização. Há ainda um grupo significativo de cidadãos que carecem de conhecimentos e competências e até mesmo do equipamento informático e dos suportes lógicos necessários para beneficiar destes recursos. O CESE insta a Comissão a apoiar as pessoas que se encontram num processo de transição”. (COMITÉ ECONÓMICO E SOCIAL EUROPEU. Parecer n.º 2021/C 374/05. [em linha] [consult. 20 Set 2021]. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52021AE1530&from=PT>).

cibersegurança²⁷, proteção de dados quanto em transparência e transmissão de fideducia ao usuário. Essa preocupação de segurança demonstra-se de grande importância, posto que de nada valeria a UE investir em digitalizar a administração pública sem que a busca pela segurança no âmbito digital seja plena a ponto do cidadão sentir-se protegido para desfrutar de toda facilidade que o serviço público sob a modalidade digital pode oferecer-lhe²⁸.

Da noção acima, pode-se compreender a preocupação com a infraestrutura: para que seja possível oferecer serviços em linha de qualidade e com a estimativa de que 80% optem pela utilização dos meios digitais e que estes meios estejam disponíveis para a totalidade dos mesmos, é necessário garantir o apoio estrutural para sua efetivação. Assim, busca-se que a conectividade seja ampla e irrestrita a todos os cidadãos por meio do 5G, além de computadores ultra potentes com aceleração quântica. Busca-se ainda, em consonância com o princípio da inclusão, disponibilizar 10.000 nós periféricos de alta segurança com impacto neutro no clima, para as áreas remotas onde o 5G não seja viável de se alcançar.

Por fim, quanto às empresas, a UE preocupa-se em possibilitar que as mesmas vivenciem a transformação digital da forma mais ampla e irrestrita possível. Estima-se que atualmente 75% das empresas europeias utilizam de alguma forma de tecnologia, notadamente, mas não se restringindo, armazenamento de dados em nuvem e inteligência artificial. No âmbito do plano

27 Por cibersegurança compreende-se o conjunto de medidas e cuidados para evitar-se ataques cibernéticos e vazamento de informações. Nos dizeres de Blanco Silva et al., “en general, la seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, disponibilidad e integridad de los datos” (BLANCO SILVA, Fernando, CASTRO PÉREZ, José Manuel, GAYOSO TABOADA, Rubén A., SANTANA ALONSO, Wilfredo (2019). Las claves de la cuarta revolución industrial. Libros de Cabecera: Barcelona, p. 60).

28 ABREU, Joana Rita de Sousa Covelo de (2019). A justiça eletrônica europeia e a modernização do espaço de liberdade, segurança e justiça... In: CARVALHO, Maria Miguel et al (Coord.). Democracia econômica e responsabilidade social nas sociedades tecnológicas. Braga: UMINHO, p. 104.

de transformação digital da Europa para a área corporativa é proporcionar a duplicação de empresas “unicórnios”²⁹ no espaço comunitário e que a transformação digital tardia, seja banida, considerando que no atual cenário mais de 90% das pequenas empresas estão apenas no nível básico da era digital.

5. Considerações Finais

O uso das chamadas novas tecnologias, a nível de comunicação, informação e na faceta promissora da inteligência artificial constitui um inegável avanço no desenvolvimento mundial e, especificamente, uma nova prioridade para o futuro da União Europeia. Contudo, surgem também novas preocupações também elas desafiadoras em que a Comissão Europeia assume uma liderança atenta e impulsionadora mas também cautelosa.

O direito da União Europeia tem caminhado no sentido de acompanhar a necessária regulamentação, preocupado com facetas como seja a segurança e respeito pelos direitos fundamentais.

Contudo, apesar das vias digitais ficarem gradualmente acessíveis aos cidadãos europeus para formas inovadoras de exercício dos seus direitos e participação democrática, há ainda um esforço educativo a desenvolver pela e para a União Europeia para que possam ser utilizadas de modo igualitário e consciente.

Referências Bibliográficas

ABREU, Joana Rita de Sousa Covelo de (2019). A justiça eletrônica europeia e a modernização do espaço de liberdade, segurança

29 “São chamadas de unicórnios as startups tecnológicas que são avaliadas em mais de mil milhões de dólares. Alguns exemplos deste tipo de empresas são a Farfetch, a Dropbox ou a SpaceX. Estas empresas são avaliadas com base nas suas oportunidades de mercado e no seu potencial de mercado, a longo prazo. O caso mais conhecido de uma startup unicórnio é o Facebook. As startups unicórnio que marcaram as décadas passadas, nasceram integradas em ondas de inovação tecnológicas: a Apple, com a criação do computador pessoal; a Google, com a generalização do acesso à Internet e o Facebook, com o boom das redes sociais”. (Economias)

e justiça: a videoconferência no Regulamento nº 1206/2001 ao serviço de uma integração judiciária. In: CARVALHO, Maria Miguel et al (Coord.). Democracia econômica e responsabilidade social nas sociedades tecnológicas. Braga: UMINHO. pp. 93-116. ISBN 978-989-54194-3-2.

ABREU, Joana Covelo de (2020). O sentido amplo de Contencioso da União Europeia e a justiça eletrónica europeia - a tutela jurisdicional efetiva como pressuposto e finalidade: breves apontamentos. In: ABREU, Joana Covelo de et al (Coords.). O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia (e-Justice). [em linha] [consult. 29 Set 2021]. Disponível em http://repositorio.uportu.pt/jspui/bitstream/11328/3322/1/Ebook_Contencioso%20da%20Uniao%20Europeia_eUjust.pdf

ABREU, Joana Covelo de (2019). O desígnio da justiça eletrónica europeia de 2019 a 2023 à luz do contencioso da União – reflexões antecipatórias. In Direito e Pessoa no Mundo Digital - Algumas Questões. Universidade do Minho, pp. 27-45. ISBN 978-989-54194-9-4. [consult. 19 Set 2021]. Disponível em: https://issuu.com/comunicadireito/docs/jornadas_25_anos_edum

ABREU, Joana Rita de Sousa Covelo de, & REIS, Liliana (2020). Instituições, Órgãos e Organismos da União Europeia. Almedina. ISBN: 9789724086453

ALVES, D. R., & SILVA, M. M. M. (2021). A iniciativa legislativa de cidadãos como instrumento de democracia: destaque para a União Europeia. In L. Bujosa Vadell & F. S. Veiga, Derecho transnacional iberoamericano, vol. 2, pp. 455-467. Valencia, Espanha: Tirant Lo Blanch. ISBN: 978-84-1378-112-9. Disponível no Repositório UPT, <http://hdl.handle.net/11328/3609>

BLANCO SILVA, Fernando, CASTRO PÉREZ, José Manuel, GAYOSO TABOADA, Rubén A., SANTANA ALONSO, Wilfredo (2019). Las claves de la cuarta revolución industrial. Libros de Cabecera: Barcelona. ISBN 978-94-949079-8-2.

Blog UNIO EU Law Journal. Em Universal basic income and artificial

intelligence – Official Blog of UNIO

COMISSÃO EUROPEIA (2021). Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União. Documento COM(2021) 206 final de 21.04.2021. [consult. 19 Set 2021]. Disponível em: resource.html (europa.eu)

COMISSÃO EUROPEIA (2021). Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões Orientações para a Digitalização até 2030: a via europeia para a Década Digital. Documento COM(2021) 118 final de 09.03.2021. [consult. 19 Set 2021]. Disponível em: EUR-Lex - 52021DC0118 - PT - EUR-Lex (europa.eu)

COMISSÃO EUROPEIA (2018). Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões Inteligência artificial para a Europa. Documento COM(2018) 237 final de 25.04.2018.

COMISSÃO EUROPEIA (2021). Comunicação conjunta ao Parlamento Europeu e ao Conselho - Relatório sobre a aplicação da Estratégia de Cibersegurança da UE para a Década Digital. Documento JOIN(2021) 14 final/2 de 06.08.2021. [consult. 19 Set 2021]. Disponível em: EUR-Lex - JOIN:2021:14:REV1 - EN - EUR-Lex (europa.eu)

COMITÉ ECONÓMICO E SOCIAL EUROPEU (2021). Parecer 2021/C 374/03 - Reforço da digitalização integradora, segura e de confiança para todos (Parecer exploratório). JOUE C 374 de 16.9.2021, pp. 11-15. [consult. 19 Set 2021]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52021AE2647&from=PT>

COMITÉ ECONÓMICO E SOCIAL EUROPEU (2021). Parecer 2021/C 374/05 - Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Orientações para a Digitalização até 2030: a via europeia para a Década Digital [COM(2021) 118

final] JOUE C 374 de 16.9.2021, pp. 22-27. [consult. 19 Set 2021]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52021AE1530&from=PT>

Economias [em linha] [consult. 19 Set 2021]. Disponível em: <https://www.economias.pt/startup-unicornio/>

KELSEN, Hans (2009). Teoria Pura do Direito. São Paulo: Martins Fontes. ISBN 9788578272050.

PARLAMENTO EUROPEU e CONSELHO (2021). Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho de 29 de abril de 2021 que cria o Programa Europa Digital. [em linha] [consult. 19 Set 2021]. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32021R0694&from=EN>

PUYOL, Javier. Del Internet de las cosas al Internet de los cuerpos. [em linha] [consult. 20 Abr 2020]. Disponível em: <https://confi legal.com/20190317-del-internet-de-las-cosas-al-internet-de-los-cuerpos/>

SCHWAB, Klaus (2016). A quarta Revolução Industrial. São Paulo: Edipro. ISBN 978-85-7283-978-5.

SILVA, José Afonso da (2011). Curso de Direito Constitucional Positivo. São Paulo: Malheiros Editores.

SILVA, M. M. M., & ALVES, D. R. (2021). Education for access to European Union Law through the use of digital technologies. In Proceedings of EDULEARN21 Conference, 13th International Conference on Education and New Learning Technologies, 5th-6th July 2021 (online conference), pp. 12289-12294. DOI: 10.21125/edulearn.2021.2582. Disponível no Repositório UPT, <http://hdl.handle.net/11328/3624>

O uso da inteligência artificial e a possibilidade de eliminação dos vieses cognitivos na decisão jurídica

The use of artificial intelligence and the possibility of elimination of cognitive bias in legal decisions

Thiago Henrique Reis de Araújo Costa¹

Marcelo Leandro Pereira Lopes²

Sumário: Introdução: como funciona o uso da inteligência artificial no Direito?; 2 A inteligência artificial e a reprodução de vieses cognitivos; 3 A inteligência artificial é o futuro da decisão jurídica?; Considerações Finais.

Resumo: O uso da Inteligência Artificial na tomada de decisões jurídicas é um movimento em expansão no Poder Judiciário. Assim, surge o questionamento quanto a possibilidade de os algoritmos eliminarem vieses cognitivos inerentes a tomada de decisão humana. A presente pesquisa tem como objetivo analisar a capacidade do atual estado de desenvolvimento dos Sistemas Especialistas do direito alcançarem esse avanço próprio da teoria da decisão jurídica. Para isso, recorreu-se a pesquisa bibliográfica e análise de resoluções e legislação pertinentes ao tema, no intuito de apresentar conceitos fundamentais para o entendimento da aplicação da Inteligência Artificial no direito, e discorrer sobre a existência de vieses e suas respectivas distorções dos resultados. Como resultado, constatou-se a relação entre a opacidade desses softwares em conjunto com a lógica operante dos algoritmos — que recorrem a casos análogos para as soluções dos problemas apresentados — na reprodução de vieses discriminatórios. Assim, apesar de, em tese, ter potencial para superar as limitações cognitivas do ser humano por não padecer de influências de fatores emocionais, ideológicos, políticos e sociais, na realidade, em razão dos dados (input) que compõem a data base se formarem de padrões enviesados dos julgados anteriores, a máquina — até mesmo quando livre do erro na inserção

1 Graduando em Direito pela UniFacid Wyden de Teresina — E-mail: thiagohenriquerac@gmail.com

2 Mestre em Direito pela Universidade Católica de Brasília – UCB. Especialista em Direito Constitucional UFPI. Bacharel em Direito pela UNIVERSIDADE FEDERAL DO PIAUÍ- UFPI. Professor pesquisador e Coordenador do Núcleo de Estudo e Pesquisa em Política, Estado e Direito Constitucional – NEPEEDIC. E-mail: marcelolp1@hotmail.com

desses dados — apenas reproduz os mesmos vieses.

Palavras-Chave: Inteligência Artificial; Vieses cognitivos; Decisão jurídica.

Abstract: The use of Artificial Intelligence in legal decision-making is an expanding movement in the Judiciary. Thus, the question arises as to the possibility of algorithms eliminating cognitive biases inherent to human decision making. This research aims to analyze the capacity of the current state of development of Specialist Systems of law to achieve this advance in the theory of legal decision. For this, bibliographical research and analysis of resolutions and legislation pertinent to the theme were used, in order to present fundamental concepts for the understanding of the application of Artificial Intelligence in law, and to discuss the existence of biases and their respective distortions of the results. As a result, it was found the relationship between the opacity of these softwares together with the operating logic of the algorithms — which resort to analogous cases to solve the problems presented — in the reproduction of discriminatory biases. Thus, although, in theory it has the potential to overcome the cognitive limitations of the human being because it does not suffer from the influence of emotional, ideological, political and social factors, in reality, because the data (input) that make up the base date are formed of the biased patterns of previous judgments, the machine — even when free from the error in entering these data — just reproduces the same biases.

Key words: Artificial Intelligence; Cognitive biases; Legal decision.

1. Introdução: como funciona o uso da inteligência artificial no direito?

Com o objetivo de melhor explorar o problema proposto na presente pesquisa, antes, é preciso apresentar os conceitos básicos e explorar os mecanismos de funcionamento da Inteligência Artificial aplicada no direito.

A começar pela própria definição do que seja Inteligência Artificial, que apesar de ser um debate complexo e ainda em andamento, para os fins aqui propostos, pode ser colocada como ferramenta da informática que emula a inteligência humana nas suas capacidades, como raciocínio, aprendizagem e interação. (LAZZARETTI; HOHENDORFF, 2021).

Para a tomada de uma decisão, a função de aprendizado é primordial para a Inteligência artificial, pois a depender de como isso se dá, a configuração do resultado pode variar em razão da forma como as informações são apreendidas e modificadas:

[...] o aprendizado supervisionado, quando é utilizado um agente externo que indica à rede a resposta desejada para o padrão de entrada; o aprendizado não supervisionado (auto-organizado), quando não existe um agente externo indicando a resposta desejada para os padrões de entrada, e o chamado procedimento de reforço, que ocorre quando uma autoridade externa avalia a resposta fornecida. De todo modo, para que ocorra uma aprendizagem automática efetiva, é necessário estabelecer parâmetros de treinamento para que o algoritmo possa avaliar qual método de ordenação das informações é mais efetivo para se alcançar o resultado desejado [...] (VALENTINI, 2017, p. 59).

Uma das técnicas para construir uma Inteligência Artificial é a machine learning, ou aprendizado de máquina, é por meio dela que o sistema pode aprender tal qual um ser humano. Ela funciona a partir de dados previamente fornecidos — em geral, decisões judiciais em processos similares — que permitem, por meio de associações entre todas as informações, a máquina apresentar conclusões e previsões na forma de novos dados gerados. (LAZZARETTI; HOHENDORFF, 2021). Conforme explicado por Boeing (2019):

Importa salientar que há várias abordagens de machine learning, sendo que uma das mais populares na atualidade é o aprendizado profundo (deep learning), que está intimamente relacionada às redes neurais artificiais (artificial neural networks - ANN). O que caracteriza o aprendizado profundo é que o próprio algoritmo detecta seus erros e realiza os ajustes necessários para aprimorar seus resultados. Sua grande vantagem, portanto, é não precisar da intervenção de um especialista para realizar tarefas de grande complexidade, ou melhor, justamente por não depender de um humano para orientá-lo na execução das atividades é que ele está apto a resolver problemas que nem mesmo os seres humanos são capazes de explicar com exatidão. (BOEING, 2019, p. 20).

Em relação ao raciocínio e processamento das informações aprendidas pela máquina juiz numa tomada de decisão no direito, a que se mostra mais concreta e realizável é o modelo de raciocínio

baseado em casos (RBC), um software que busca um caso semelhante ao que se quer analisar, extrai os seus padrões e suas razões de decidir, e o adapta para servir de resolução ao problema proposto. (VALENTINI, 2017).

Um modelo de RBC se orienta por meio da realização das seguintes tarefas: recuperação, reutilização, revisão e fixação. A tarefa de recuperação consiste em, dado um problema-alvo, fazer o algoritmo recuperar da memória os casos análogos que são relevantes para resolvê-lo. Um caso análogo consiste em informações referentes a um determinado problema, sua correspondente solução e, normalmente, anotações sobre como chegar na solução. A tarefa de reutilização consiste em mapear a solução do caso anterior para o problema-alvo. Isto pode exigir adaptação da solução para que sirva para a nova situação. A revisão consiste em, a partir do mapeamento da solução anterior para a situação-alvo, testar a solução no mundo real (ou numa simulação) e, se necessário, revisá-la. Por fim, a fixação consiste em, depois que a solução foi adaptada com êxito para o problema-alvo, guardar a experiência resultante na memória como um novo caso. (VALENTINI, 2017, p. 64 – 65).

O procedimento heurístico ou forma de obtenção das informações que comporão os casos dessa base de dados (big data) que mais corresponde a complexidade da decisão jurídica são as chamadas redes neurais, que na lição de Valentini (2017):

Desse modo, nas redes neurais os sinais são recebidos na entrada (input), sendo que cada um desses dados é multiplicado por um número, ou peso, que indica a sua importância na saída (output). Após, é realizada uma soma ponderada dos sinais que produz um determinado nível de atividade o qual, se exceder certo limite (threshold), resultará em uma resposta de saída. (VALENTINI, 2017, p. 66).

A partir da formação dessa base de dados (input), dá-se início a leitura por meio da ação dos algoritmos, que são sistemas de dados programados para dar respostas (output), ou seja, a parte responsável pela interpretação das decisões jurídicas anteriores e formação da sentença. (NUNES; MARQUES, 2018).

Destaque-se, o objetivo é analisar em que estágio de desenvolvimento já se encontra o sistema especialista do direito (MEDEIROS, 2019) — projetado para emular o método de resolução

de problemas de um juiz —, especificamente quanto a superação ou não do juiz humano no que diz respeito a decisões proferidas que não sejam maculadas por vieses cognitivos e suas respectivas distorções da realidade. Essa será a métrica para aferir seu sucesso e do qual se apresentará uma abordagem crítica.

Afinal, entende-se aqui que o papel de julgador dado a Inteligência Artificial só valerá como uma evolução se puder ser superada uma das limitações humanas na produção de decisões a qual ainda hoje nem a doutrina nem a jurisprudência encontraram solução, que é a reprodução de preconceitos, seja de forma consciente ou não. Assim, o sucesso da Inteligência Artificial na decisão jurídica depende de sua capacidade de resolver os vícios inerentes à decisão humana.

2. A inteligência artificial e a reprodução de vieses cognitivos

A capacidade cognitiva do ser humano é limitada e sujeito a erros, muitas vezes por influência de fatores como preferências pessoais, ideologia política, preconceitos de raça, gênero, classe social ou opção religiosa, dentre tantos outros que podem atuar no íntimo do julgador. Seja de maneira sistemática ou inconsciente, como classifica Streck (2017), trata-se de preconceitos inautênticos que não podem ser a razão de uma decisão legítima dentro do direito, pois, na verdade, houve um desvirtuamento da resposta por vieses cognitivos que levaram o resultado à erro.

Com isso em vista, a alternativa de julgamento pela Inteligência Artificial, livre desses vieses cognitivos, pois, em tese, não sofre influência de uma pré-compreensão de mundo inautêntica, permitirá uma revolução do direito quanto à um julgamento justo e a obtenção de uma resposta constitucionalmente correta.

Contudo, o que se visualiza é um transplante — intencionalmente ou não — dos vieses cognitivos humanos para

o julgamento realizado por Inteligência artificial. Porém, destaque-se, muito desses erros não são inerentes a automação da decisão jurídica, mas tem origem nas informações (input) que compõe a data base, ou seja, são provenientes de julgados por humanos carregados de vieses.

Após a elaboração do modelo, são fornecidos dados para o sistema, de modo a possibilitar o machine learning (aprendizado de máquina), pelo qual a máquina analisará as informações fornecidas, seguindo as instruções estabelecidas pelo algoritmo, para encontrar padrões e, então, conseguir prever resultados. A qualidade dos dados fornecidos aos sistemas de inteligência artificial também impactará os resultados, pois os dados são coletados da sociedade que é permeada por desigualdades, exclusões e discriminações. Conforme estudo realizado por pesquisadores da Universidade de Oxford: [...] o aprendizado de máquina pode confirmar padrões discriminatórios – se eles forem encontrados no banco de dados, então, por conseguinte, um sistema de classificação exato irá reproduzi-los. Deste modo, decisões enviesadas são apresentadas como resultado de um “algoritmo objetivo”. (NUNES; MARQUES, 2018, p. 5).

Aqui vale se ater a crítica de teor hermenêutico, por se valer o algoritmo de um banco de dados com decisões pretéritas que servirão como a resposta para o caso em análise, estaria, então, a teoria da decisão reduzida a mero pragmatismo, no qual a resposta correta é aquilo que o tribunal ou juiz — neste caso, uma máquina — diz que é. (LAZZARETTI; HOHENDORFF, 2021). Seria a instalação do realismo jurídico no Poder Judiciário ou absolutismo do Poder Judiciário, com abertura de margem para arbitrariedades e redução de espaço para o exercício do efetivo contraditório e do direito de defesa.

Muitos também apontam o receio quanto a restrição da Inteligência Artificial de apenas poder aplicar a lógica matemática, incompatível com casos complexos permeado de incertezas que discutem direitos fundamentais. (ARAÚJO, 2020).

Quanto a crítica da reprodução de vieses pela Inteligência Artificial, o caso mais alarmante diz respeito ao sistema COMPAS (Correctional Offender Management Profiling for Alternative)

software usado por diversos tribunais dos EUA para calcular o risco de periculosidade de determinado réu que está sob julgamento, inclusive, quanto as chances de reincidência. (ARAÚJO, 2020).

O COMPAS, para o cálculo da classificação de periculosidade de um réu, utiliza critérios como o grau de instrução do réu, histórico de infratores na família ou em círculo de amizades do réu, a predisposição para crimes de acordo com a idade, os eventos criminais do réu nos últimos doze meses, dentre outros. A fórmula adotada pelo COMPAS para cálculo da periculosidade dos réus é, sinteticamente dizendo, bem simples: (1) o réu deverá responder a um questionário e as informações deste questionário são os dados de input para o processamento do sistema COMPAS; (2) o COMPAS, a partir das informações fornecidas pelo questionário, vai gerar uma determinada pontuação para classificação da periculosidade do respectivo réu em análise; (3) quanto maior for a pontuação gerada pelo COMPAS, maior será considerado o índice de periculosidade do réu e maior será considerada uma possível reincidência de crime para o réu que está sendo julgado; (4) por fim, quanto maior for o índice de periculosidade e de possibilidade de reincidência de crime calculado pelo COMPAS, maior será a pena aplicada na sentença para este réu. Dentro desse contexto, o COMPAS trabalha com dois status de periculosidade de reincidência: “Risco de Reincidência” e “Risco de Rescendência Violenta”. (ARAÚJO, 2020, p. 61 – 62).

Acontece que a análise dos casos julgados pelo sistema COMPAS demonstraram a presença de viés cognitivo em razão de preconceito racial:

Quanto à classificação para o status do “risco de reincidência”, os réus negros eram muitas vezes classificados com maior pontuação de risco do que realmente acontecia na realidade. A pesquisa constatou que os réus negros que não reincidiram ao longo do período de dois anos tinham quase o dobro de chances de serem erroneamente classificados com o status de “risco de reincidência” em comparação com seus colegas brancos (45% contra 23%). Em sentido oposto, os réus brancos costumavam ser classificados com menor risco de reincidência do que realmente acontecia na realidade. A pesquisa constatou que réus brancos que reincidiram ao longo do período de dois anos foram erroneamente rotulados como de baixo risco em quase duas vezes mais do que os negros (48% contra 28%). Mesmo quando a análise era controlada por crimes anteriores, reincidências futuras, idade e sexo, os acusados negros tinham 45% mais probabilidade de receber maior pontuação de risco do que os réus brancos. Quanto à classificação do status de “reincidência violenta”, os acusados negros tinham o dobro de probabilidade de

serem erroneamente classificados como de reincidência violenta em relação aos réus brancos. Os reincidentes brancos foram classificados erroneamente como de baixo risco em 63,2% em relação aos réus negros. No mesmo sentido do status anterior, o status de reincidência violenta também demonstrou que, mesmo quando a análise era controlada por crimes anteriores, reincidência futura, idade e sexo, os acusados negros tinham 77% mais probabilidade de receber maiores pontuações de risco do que os réus brancos. (ARAÚJO, 2020, p. 62 – 63).

A empresa Northpointe Inc., desenvolvedora do sistema COMPAS, não divulga publicamente os cálculos feitos para chegar às pontuações de risco dos réus (SALOMÃO, 2020), algo comum, visto esses softwares serem desenvolvidos em sua grande maioria por empresas privadas, interessadas em guardar segredo em razão de fins comerciais, o que traz prejuízos a transparência e inviabiliza o dever de prestação de contas por parte do Poder Judiciário.

Diante de uma sociedade que tem como principal alvo do poder punitivo estatal as minorias marginalizadas, tais como os negros, comunidade LGBTQIA+, mulheres e pobres, a probabilidade de reprodução de vieses preconceituosos pelo algoritmo em seu atual estágio de desenvolvimento é muito alta. Tais vieses algorítmicos são denominados machine bias, algorithm bias, ou simplesmente bias. (MARQUES; BOCCHINO, 2020). Assim, por mais que os dados não estejam corrompidos, se os padrões da sociedade são preconceituosos, haverá a presença do viés da confirmação para reproduzir a discriminação encontrada nos julgados anteriores. (SILVA; SALES; SILVA, 2020).

Aqui, identifica-se o problema na própria alimentação da base de dados. O que consequentemente impossibilita o distinguishing e o overruling do caso, ou seja, não há superação da jurisprudência, já que a lógica dos algoritmos dispensa a efetiva atuação das partes no processo, pois o julgamento se dá não em razão dos argumentos apresentados, mas, sim, por casos similares e precedentes consolidados, o que torna o direito estático (SILVA; SALES; SILVA, 2020) e propício a perpetuação de erros, é a reprodução do viés da ancoragem (MEDEIROS, 2019). Cabe lembrar que os

vieses preconceituosos também podem ser inseridos de maneira deliberada pelo programador, fenômeno chamado de human bias. (PÁDUA, 2020).

Outro problema identificado como origem da reprodução de vieses na tomada de decisões por Inteligência Artificial diz respeito a opacidade dos algoritmos, pois as razões de decidir são ininteligíveis até mesmo para os seus programadores:

[...] os algoritmos fundados em machine learning têm autonomia tamanha a ponto de criar a sua própria programação, alterando a sua própria estrutura, e é por essa razão que não se consegue chegar a uma conclusão quanto aos processos internos das máquinas, porque que o iter de aprendizagem é completamente obscurecido [...] (SILVA; SALES; SILVA, 2020, p. 22).

Ou seja, o modo como as técnicas avançadas de machine learning (deep learning) e redes neurais artificiais profundas (deep neural networks) funcionam hoje — complexidade do código de programação e variabilidade da lógica de decisão — somados no cenário brasileiro, em que não há padronização na estrutura de dados ao mesmo tempo em que se desenvolvem diversos softwares com programações distintas, impossibilitam a sua compreensão. (MEDEIROS, 2019).

O que transforma a Inteligência Artificial numa espécie de caixa preta tal como é o cérebro humano, onde não há como explicitar a motivação das decisões de forma totalmente clara. Assim, conclui-se que o estado da arte atual dos algoritmos ainda não apresenta vantagem em relação aos juízes humanos, pois, ainda, suas razões de decidir se encontram tão indecifráveis quanto.

Isso também é apontado como empecilho ao exercício dos direitos fundamentais do duplo grau de jurisdição e da fundamentação das decisões, já que não há como identificar os elementos que compõem a fundamentação, requisito essencial para a impugnação de qualquer decisão. (NUNES; MARQUES, 2018).

Alerte-se, o problema da opacidade da Inteligência Artificial

no Brasil já é uma realidade para o Poder Judiciário, como aponta Medeiros (2019) sobre o sistema Victor do STF:

Também no caso do Victor, utilizado pelo STF – cujo processo de criação foi guardado em sigilo sem a possibilidade de participação (fiscalidade) da sociedade e dos jurisdicionados –, uma análise equivocada do conjunto de dados ou um erro na pesquisa, pode acarretar que o algoritmo realize correlações defeituosas da repercussão geral inadmitindo recursos sem que seja possível compreender a lógica (regra de decisão) que embasou essa decisão específica. E mesmo que seja realizada a abertura do código fonte, é possível que não seja possível entender o funcionamento do algoritmo quando ele estiver em efetiva operação, posto que, a depender de sua complexidade, as operações interlineares não ficarão demonstradas. (MEDEIROS, 2019, p. 73 – 74).

Neste sentido, faz-se necessário criar instrumentos seguros para a preservação da fundamentação legal e do próprio Estado Democrático de Direito que se consubstancia na segurança jurídica e na previsibilidade das decisões judiciais por meio motivação clara de suas decisões.

3. A inteligência artificial é o futuro da decisão jurídica?

A possibilidade de a Inteligência Artificial produzir decisões judiciais de modo completamente automatizado e constitucionalmente adequado, passa por eliminar a influência de vieses e aumentar a transparência do caminho percorrido pelo algoritmo para se chegar à determinada conclusão.

Nesse sentido, encontra-se a Resolução 332 de 2020, do CNJ, que dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário. Em seu capítulo VII, em que trata do controle do usuário, determina no art. 17, inciso II, que seja possível a revisão da decisão tomada e dos dados utilizados para sua elaboração, sem que haja vinculação à solução apresentada pela Inteligência Artificial, o que possibilita a correção de vieses encontrados por magistrados humanos treinados para essa nova funcionalidade. (PÁDUA, 2020).

Garante o art. 18 o direito dos jurisdicionados de serem informados de forma clara quando submetidos a decisões por algoritmos, essencial para o exercício do contraditório, previsão igualmente encontrada no art. 20, caput, da Lei Geral de Proteção de Dados Pessoais (Lei nº. 13.709/2018). E o art. 19 da citada Resolução do CNJ exige que, para a elaboração de decisão judicial com auxílio da Inteligência Artificial, seja possível explicar os passos que conduziram até o resultado apresentado, de modo a impedir o uso de sistemas opacos. (Resolução 332/2020, CNJ).

Exigência também presente no art. 20, §1º, da Lei nº. 13.709/2018, que, num avanço no combate aos vieses nas decisões tomadas por algoritmos, estabeleceu no §2º, do mesmo dispositivo, a possibilidade de auditoria pela autoridade nacional responsável em caso de verificação de aspectos discriminatórios. (BRASIL, 2018).

Por fim, destaque-se positivamente a determinação da Resolução 332/2020 do CNJ no capítulo III, voltado especificamente ao combate dos vieses preconceituosos e a retirada dos softwares que os reproduzam:

Art. 7º As decisões judiciais apoiadas em ferramentas de Inteligência Artificial devem preservar a igualdade, a não discriminação, a pluralidade e a solidariedade, auxiliando no julgamento justo, com criação de condições que visem eliminar ou minimizar a opressão, a marginalização do ser humano e os erros de julgamento decorrentes de preconceitos. §1º Antes de ser colocado em produção, o modelo de Inteligência Artificial deverá ser homologado de forma a identificar se preconceitos ou generalizações influenciaram seu desenvolvimento, acarretando tendências discriminatórias no seu funcionamento. §2º Verificado viés discriminatório de qualquer natureza ou incompatibilidade do modelo de Inteligência Artificial com os princípios previstos nesta Resolução, deverão ser adotadas medidas corretivas. §3º A impossibilidade de eliminação do viés discriminatório do modelo de Inteligência Artificial implicará na descontinuidade de sua utilização, com o consequente registro de seu projeto e as razões que levaram a tal decisão. (RESOLUÇÃO 332/2020, CNJ, art. 7º).

Em tese, o potencial de evolução tecnológica no desenvolvimento da Inteligência Artificial aplicada a decisão jurídica

é infinito, e, por isso mesmo, um dia pode alcançar a programação do algoritmo julgador ideal. Mas, pela análise feita nessa pesquisa, entende-se que é um objetivo ainda muito distante da realidade.

Isso se dá por conta que a possibilidade de eliminação da reprodução de vieses cognitivos atualmente se manter remota, vide a ausência de transparência e compreensão dos fundamentos das decisões produzidas pelos Sistemas Especialistas programados para auxiliar o Poder Judiciário, e o modus operandi do raciocínio algorítmico restrito a leitura de casos passados, o que dá ensejo a reprodução de vieses já conhecidos pelos julgadores humanos, e impede a concretização do efetivo contraditório de do direito de defesa.

Assim, apesar de não padecer de vieses de cunho emocional ou de limitação de memória, já que sua análise parte de uma base de dados inúmeras vezes maior que o intelecto humano, o que representa uma vantagem, o estágio atual desenvolvido pelos programadores ainda não permitiu superar os vieses da confirmação e da ancoragem, que conseqüentemente carregam vieses de cunho discriminatórios originados de decisões humanas que servem de informações (input) para compor a base de dados (data base), o que alimenta o ciclo de decisões deturpadas. (LORDELO, 2020).

Considerações Finais

Chega-se a conclusão que a possibilidade de eliminação — ou ao menos, de um maior controle — dos vieses cognitivos presente nas decisões jurídicas proferidas por Inteligência Artificial, se concretizará quando o avanço da tecnologia permitir uma leitura legível e transparente das razões que levam o algoritmo a determinado resultado, em conjunto com a capacidade considerar, efetivamente, os argumentos trazidos a debate pelas partes, o que tornaria possível a superação da jurisprudência em razão da distinção de casos novos.

Neste quadro, a Inteligência Artificial poderá ser um importante instrumento de auxílio nas decisões humanas, em especial, no tocante a celeridade processual e a economicidade. Um Poder Judiciário que atenda prontamente as demandas sociais, mas que, ao mesmo tempo, não perde seu fundamento democrático deve ser o foco da utilização da Inteligência Artificial como mecanismo facilitador nas tomadas de decisões pelos órgãos jurisdicionais.

Referências

ARAÚJO, Érik da Silva e. A INTELIGÊNCIA ARTIFICIAL E A CRIATIVIDADE NA INTERPRETAÇÃO, ARGUMENTAÇÃO E DECISÃO JURÍDICA COMO UM PROCESSO DE CONSTRUÇÃO DO DIREITO. Pouso Alegre, 2020. 126 p Dissertação (Pós-Graduação, Mestrado em Direito) - Faculdade de Direito do Sul de Minas.

BOEING, Daniel Henrique Arruda. ENSINANDO UM ROBÔ A JULGAR: PRAGMÁTICA, DISCRICIONARIEDADE E VIESES NO USO DE APRENDIZADO DE MÁQUINA NO JUDICIÁRIO. FLORIANÓPOLIS, 2019. 84 p Trabalho de Conclusão de Curso (Direito) - Universidade Federal de Santa Catarina.

BRASIL. CNJ. Resolução n. 332. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Diário Oficial da União, 21 de agosto de 2020.

BRASIL. Lei n. 13.709. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, 14 de agosto de 2018.

LAZZARETTI , Bianca Kaini; HOHENDORFF, Raquel von. O USO DE INTELIGÊNCIA ARTIFICIAL NA TOMADA DE DECISÕES JUDICIAIS: UMA ANÁLISE SOB A PERSPECTIVA DA CRÍTICA HERMENÊUTICA DO DIREITO. Revista RD Uno, Chapecó, 19 04 2021.

MARQUES, Meire Aparecida Furbino; BOCCHINO, Lavinia

Assis. TECNOLOGIA E JURISDIÇÃO: OS VIESES COGNITIVOS ALGORÍTMICOS E O RISCO PARA OS DIREITOS FUNDAMENTAIS. In: XI CONGRESSO RECAJ-UFMG DIREITOS HUMANOS, GÊNERO E TECNOLOGIAS DA CONTEMPORANEIDADE. 2020, Belo Horizonte, 2020, p. 136-146.

MEDEIROS, Nathália Roberta Fett Viana de. USO DA INTELIGÊNCIA ARTIFICIAL NO PROCESSO DE TOMADA DE DECISÕES JURISDICIONAIS: Uma análise sob a perspectiva da teoria normativa da participação. Belo Horizonte, 2019. 162 p Dissertação (Programa de Pós-Graduação stricto sensu em Direito) - Pontifícia Universidade Católica de Minas Gerais.

NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. INTELIGÊNCIA ARTIFICIAL E DIREITO PROCESSUAL: VIESES ALGORÍTMICOS E OS RISCOS DE ATRIBUIÇÃO DE FUNÇÃO DECISÓRIA ÀS MÁQUINAS. REVISTA DOS TRIBUNAIS ONLINE, v. 285, 2018.

PÁDUA, Sérgio Rodrigo de. O JUIZ CIBORGUE: INTELIGÊNCIA ARTIFICIAL E DECISÃO JUDICIAL. In: ENCONTRO VIRTUAL DO CONPEDI DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III, n. II. 2020, Florianópolis: CONPEDI, 2020, p. 315-335.

SALOMÃO, Luis Felipe (Coord.). Inteligência Artificial: Tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário brasileiro. Relatório do Centro do de Inovação, Administração e Pesquisa do Judiciário da FGV. 74 p, 2020.

SILVA, RAPHAEL CAETANO RODRIGUES; SALES, ANA FLÁVIA; SILVA, CRISTIAN KIEFER DA. OS RISCOS DA IMPLEMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO PROCESSO DECISÓRIO. Belo Horizonte, 2020. 29 p Trabalho de Conclusão de Curso (Direito) - Centro Universitário Una.

STRECK, Lenio Luiz. DICIONÁRIO DE HERMENÊUTICA: Quarenta temas fundamentais da Teoria do Direito à luz da Crítica Hermenêutica do Direito. Belo Horizonte: Letramento: Casa do Direito, 2017. 320 p.

VALENTINI, Rômulo Soares. JULGAMENTO POR

COMPUTADORES? AS NOVAS POSSIBILIDADES DA JUSCIBERNÉTICA NO SÉCULO XXI E SUAS IMPLICAÇÕES PARA O FUTURO DO DIREITO E DO TRABALHO DOS JURISTAS. Belo Horizonte, 2017. 150 p Tese (PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO) - Universidade Federal de Minas Gerais.

Inteligência artificial, economia comportamental e publicidade: uma união perigosa para o consumidor virtual

Artificial intelligence, behavioral economics and marketing: a dangerous union to the virtual consumer

João Pedro Leite Barros¹

Débora Fernandes Maranhão²

Sumário: 1. Economia comportamental e a publicidade; 2. Inteligência artificial associada à publicidade; 2.1 Caso da indústria farmacêutica; 3. Perigo para o consumidor; Considerações Finais.

Resumo: O presente trabalho visa contribuir para um debate necessário à proteção do consumidor. Há muito, práticas de economia comportamental já eram empregadas para manipular o comportamento do indivíduo e induzir a compra de um bem. Já neste momento, havia certa preocupação com as tentativas de enganar o consumidor. Atualmente, o perigo foi elevado, uma vez que são associados sistemas de inteligência artificial aos anteriores conhecimentos de economia comportamental. Assim, com o advento desta tecnologia, cada vez mais aperfeiçoada, as vulnerabilidades do consumidor podem estar sendo exploradas economicamente por meio da publicidade comportamental. Sendo que ainda há dificuldade em identificar e investigar estas práticas, por isso é necessária maior atenção e estudos para coibir abusos. As normas recentes de proteção de dados são, de fato, um progresso, mas podem não ser suficientes para proteção do consumidor neste cenário. Tendo em vista que poucos dados – que não precisam ser pessoais – são usados para chegar às conclusões obtidas pelo algoritmo. O perigo destas práticas comerciais reside em forçar excessivamente o consumo, ao explorar as fraquezas e incompreensões do consumidor. Então, essa união entre a economia comportamental e a inteligência

1 Doutor em Direito Civil pela Universidade de Brasília e pela Universidade de Lisboa. Mestre em Ciências Jurídicas (Direito Civil) pela Universidade de Lisboa. Professor em Direito do Consumidor na Universidade de Brasília (UnB). Advogado. E-mail: barroseleite@gmail.com

2 Pós-graduanda em Direito Digital e Proteção de Dados pelo Instituto brasileiro de ensino, Desenvolvimento e Pesquisa (IDP). Bacharela em Direito pela Universidade de Brasília (UnB). Advogada do Núcleo de Prática Jurídica da UnB. E-mail: debora.fmaranhao@gmail.com

artificial pode transformar a publicidade convencional, que apresenta o produto ao consumidor, em uma publicidade que objetiva forçar excessivamente o consumo de bens.

Palavras-chave: Inteligência Artificial; Economia Comportamental; Publicidade; Consumidor.

Abstract: This paper aims to contribute to a debate for consumer protection. Behavioral economics practices have long been used to manipulate individual's behavior and induce the purchase of a good. Already at this time, there was some concern about attempts to deceive the consumer. Currently, the danger has been increased since artificial intelligence systems are associated with this previous knowledge of behavioral economics. Therefore, with the advent of this technology, consumer's vulnerabilities maybe are being economically exploited through behavioral advertising. Since there is still difficulty in identifying and investigating these practices, more attention and studies are needed to curb abuse. Recent data protection regulations are indeed a progress, but they may not be sufficient for consumer's protection in this scenario. Considering that few data – which do not need to be personal – are used to reach the conclusions obtained by the algorithm. The danger of these commercial practices lies in excessively forcing consumption by exploiting the consumer's weaknesses and lack of understanding. Thereby, this union between behavioral economics and artificial intelligence could transform conventional advertising, which presents the product to the consumer, into an advertising that aims to force the consumption of goods.

Keywords: Artificial Intelligence; Behavioral Economics; Marketing; Consumer.

1. Economia comportamental e a publicidade

Já em 1978, o economista Richard H. Thaler, responsável por grandes obras na área de economia comportamental, trazia a público o seu primeiro artigo sobre o tema, no qual mencionou-se às «economic mental illusions³», que se referem ao comportamento do consumidor contrário ao que ele próprio pensa de si mesmo. Esta ciência comportamental foi, então, ilustrada por meio de

3 O autor explica estas ilusões como momentos em que o consumidor desvia das previsões do modelo normativo – teoria largamente usada por economistas para descrever o que consumidores racionais fariam em determinada situação. Cfr. THALER, Richard. Toward a Positive Theory of Consumer Choice. *Journal of Economic Behavior and Organization*, v. 1, n. 1, 1980, p. 39–40.

práticas comerciais utilizadas para persuadir o consumidor a agir de determinada forma, como a criação de uma ilusão pela manipulação do preço de referência para que os consumidores pensassem fazer um bom negócio em uma promoção⁴.

Neste contexto, há também o conceito das âncoras, presente na obra Nudge⁵, em que os autores dizem expressamente que «podemos influenciar sua escolha numa situação específica, sugerindo sutilmente um ponto de partida para seu processo de pensamento». A própria expressão Nudge⁶ é reportada como uma parte do processo de decisão que pode ser usada para alterar o comportamento humano.

Esse campo de estudo da economia demonstra como esse comportamento humano pode ser previsto e alterado em determinados casos, em especial no que se refere à decisão de compra, já que se observou que os modelos econômicos tradicionais não explicavam além da racionalidade humana. Em 1999⁷, surgiu o conceito de «market manipulation» exatamente se reportando à economia comportamental como uma forma de explorar a tendência de comportamento irracional dos consumidores.

De fato, algumas práticas comerciais que fazem uso da ciência comportamental podem ser observadas no mercado há anos e com sucesso, como a Unilever⁸ – empresa de produtos para lavanderia – que modifica sua atuação em cada país a depender da cultura local. No Brasil, a empresa tem uma preocupação com a região nordeste em que está mais presente a lavagem manual de roupas, por exemplo. Contudo, o estudo do comportamento pode promover práticas comerciais que intentem ludibriar o consumidor.

4 THALER, Richard. Misbehaving. Tradução: George Schlesinger. 1 ed. Rio de Janeiro: Intrínseca, 2019. p. 75

5 THALER, Richard; SUSTEIN, Cass. Nudge. Tradução: Ângelo Lessa. Rio de Janeiro: Objetiva, 2019. p. 38

6 THALER, Richard; SUSTEIN, Cass. Nudge. Tradução: Ângelo Lessa. Rio de Janeiro: Objetiva, 2019. p. 12

7 CALO, Ryan. Digital market manipulation. George Washington Law Review, v. 82, n. 4, p. 995–1051, 2014. p.7-8

8 MOTHERSBAUGH, David L.; HAWKINS, Del I. Consumer behavior: building marketing strategy. 13. ed. Eugene: McGraw-Hill Education, 2016. p. 67

É o caso da Apple⁹ que mudou o tamanho da barra de sinal para gerar a impressão de maior cobertura da rede, após ser questionada sobre esse quesito em versões anteriores do iPhone.

Assim, além de incentivar o consumo de bens, a economia comportamental também tem sua faceta obscura quando faz com o que o consumidor compre pensando estar adquirindo um produto melhor ou um preço melhor. Essas práticas podem ser vistas no mercado desde o século passado, como foi mencionado. Porém, com a era digital e o advento de sistemas avançados de inteligência artificial, a atenção deve ser ainda maior, porque o consumidor é reconhecidamente vulnerável e agora ainda pode ser submetido à exploração econômica de suas vulnerabilidades humanas.

2. Inteligência artificial associada à publicidade

A exploração das tecnologias de inteligência artificial (IA) no mercado são um divisor de águas¹⁰. Explica-se: o mercado, em especial o digital, ao agregar os sistemas de IA, tem possibilitado diversas inovações, como o uso de algoritmos, ferramentas de rastreamento e filtros de conteúdo. A IA é constantemente utilizada para organizar e selecionar informações relevantes¹¹ em plataformas e pode aprimorar a experiência do consumidor virtual.

Reporta-se, inclusive, que o processo de tomada de decisão pode ser modificado pela possibilidade que esses sistemas tecnológicos conferem aos consumidores de terceirizar a decisão de compra, fala-se aqui na existência do «algorithmic consumer¹²». Nesse caso, o consumidor é auxiliado a tomar decisões racionais

9 CALO, Ryan. Digital market manipulation. *George Washington Law Review*, v. 82, n. 4, p. 995–1051, 2014. p.13

10 ABRARDI, Laura; CAMBINI, Carlo; RONDI, Laura. Artificial intelligence, firms and consumer behavior: A survey. *Journal of Economic Surveys*, n. July, p. 1–23, 2021. p. 12

11 ABRARDI, Laura; CAMBINI, Carlo; RONDI, Laura. Artificial intelligence, firms and consumer behavior: A survey. *Journal of Economic Surveys*, n. July, p. 1–23, 2021.

12 ABRARDI, Laura; CAMBINI, Carlo; RONDI, Laura. Artificial intelligence, firms and consumer behavior: A survey. *Journal of Economic Surveys*, n. July, p. 1–23, 2021. p. 8

baseadas no suporte de um algoritmo, que pode ajudá-lo a decidir a melhor hora de comprar algo cujo preço muito volátil.

E não se nega que a inteligência artificial pode trazer benefícios ao consumidor. Todavia, alerta-se por ora para os perigos que podem estar contidos em sistemas de IA associados ao marketing digital. Isso porque há estudos¹³ que apontam que o algoritmo associado ao machine learning e à publicidade direcionada podem fazer com que o consumidor pague até duas vezes o valor original do bem de consumo. A base disso está em um estudo que verificou os preços que poderiam ser cobrados pela plataforma Netflix, modificando de acordo com o histórico de pesquisa e variáveis demográficas¹⁴.

Eli Pariser¹⁵, além de tratar sobre os filtros algorítmicos que condenam o indivíduo à bolha, denuncia a criação de perfis em redes sociais por softwares, destinados à publicidade, com o fim de se aproximarem ainda mais do usuário para compreender seu comportamento.

Ligando essas práticas comerciais mais invasivas ao fato de que o processo de aprendizagem e mudança de cada algoritmo é mencionado na doutrina como uma «caixa preta», tamanha sua obscuridade¹⁶, impende atentar-se a este tema para não permitir a expansão da vulnerabilidade do consumidor.

A economia comportamental já trazia práticas comerciais que incentivavam o consumo a um ponto que merecia maior ponderação. Atualmente, as empresas têm disponíveis softwares avançados e podem obter mais dados sobre o comportamento do consumidor e, por conseguinte, ter mais ingerência na manipulação

13 ABRARDI, Laura; CAMBINI, Carlo; RONDI, Laura. Artificial intelligence, firms and consumer behavior: A survey. *Journal of Economic Surveys*, n. July, p. 1–23, 2021. p. 14

14 ABRARDI, Laura; CAMBINI, Carlo; RONDI, Laura. Artificial intelligence, firms and consumer behavior: A survey. *Journal of Economic Surveys*, n. July, p. 1–23, 2021. p. 14

15 PARISER, Eli. *The Filter Bubble: What the Internet Is Hiding from You*. London: Viking/Penguin Press, 2011. p.104

16 ABRARDI, Laura; CAMBINI, Carlo; RONDI, Laura. Artificial intelligence, firms and consumer behavior: A survey. *Journal of Economic Surveys*, n. July, p. 1–23, 2021. p. 8

de suas decisões de compra.

O Brasil não está isolado neste cenário. A própria Associação Brasileira de Comércio Eletrônico informa que, com o uso de análise preditiva, as empresas compreendem o comportamento do consumidor e têm a previsão de seus passos futuros. Isto permite que eles estimulem a venda cruzada¹⁷, com base nas compras pretéritas.

Essa problemática pode ser ilustrada. Há o já muito conhecido exemplo da loja Target e sua sapiência de gestações. No caso, foi utilizado um software para compreender quando uma mulher está grávida e oferecer-lhe itens de consumo para bebês, de acordo com o período da gestação em que se encontrava. Isso foi possível apenas observando o histórico de compra desta mulher; a compra de cálcio, magnésio e zinco¹⁸ eram um indício da gravidez.

Não apenas o consumidor não tem mais privacidade, como também é incentivado a consumir, o que já era uma dificuldade antes da IA. O direito ao arrependimento¹⁹ no Brasil também objetiva evitar compras feitas por impulso, sob forte influência da publicidade, demonstrando que práticas comerciais já eram preocupantes no impulsionamento excessivo do consumo. Com a associação à IA, aumentou-se ainda mais a exposição do consumidor virtual às práticas que induzem a mudança comportamental para forçar o consumo.

2.1. Caso da indústria farmacêutica

Neste momento, exemplifica-se o perigo da associação entre a publicidade, a inteligência artificial e a economia comportamental.

17 ABDCOMM. Disponível em: <<https://abcomm.org/noticias/com-uso-de-inteligencia-artificial-infracommerce-expande-same-day-delivery-para-outras-capitais-do-brasil/>>. Acesso em: 29 set. 2021.

18 PASQUALE, Frank. *The Black Box Society: the secret algorithms that control money and information*. Cambridge: Harvard University Press, 2015. p. 37

19 BARROS, J. P. L. O direito de arrependimento nos contratos eletrônicos de consumo como forma de extinção das obrigações. In: *Estudos de direito do consumidor*. Coimbra: Centro de direito do consumo, 2018. p. 155.

Ressalta-se de início que houve dificuldade em encontrar casos práticos em fontes cientificamente confiáveis e recentes. Acredita-se que possivelmente a explicação para tanto não é a inexistência, muito pior, é a falta de conhecimento desses casos. Muito porque não são investigados – aqui se fala em particular do Brasil – e também porque são de difícil aceção por quem observa de fora das empresas e sem cognição de como é a construção dos algoritmos, as black boxes.

Um caso²⁰ interessante foi objeto de deliberação pela Federal Trade Commission (FTC) nos Estados Unidos. Pesquisas identificaram que os norte-americanos cada vez mais confiavam em informações médicas na internet e que a indústria farmacêutica se beneficiava disso. É tanto que os gastos com remédios nos Estados Unidos dobraram, em dígitos bilionários, em menos de 11 anos. A FTC apontou em seu relatório para o perigo que representa o mercado manipulando as emoções das pessoas no âmbito médico e incentivando a compra de medicações. A indústria farmacêutica online estava trabalhando para promover a adoção massiva de medicações para o mercado pediátrico e adolescente, após lucrar \$14,6 bilhões seguidamente a anúncios televisivos sobre antidepressivos²¹.

Então, nesse caso, o recurso à automedicação passou a ser incentivado por plataformas digitais, enquanto é contraindicado por profissionais da área. Acontece que o lucro bilionário retira os filtros éticos, campo aberto para o lucro indiscriminado das empresas farmacêuticas. O exemplo demonstra que a IA na publicidade requer atenção para que não transponha barreiras éticas e de

20 FTC. Complaint, Request for Investigation, Public Disclosure, Injunction, and Other Relief: Google, Microsoft, QualityHealth, WebMD, Yahoo, AOL, HealthCentral, Healthline, Everyday Health, and Others Named Below. Disponível em: <<https://www.ftc.gov/sites/default/files/attachments/other-applications-petitions-and-requests/101123publiccmptdigitaldemocracy.pdf>>.

21 FTC. Complaint, Request for Investigation, Public Disclosure, Injunction, and Other Relief: Google, Microsoft, QualityHealth, WebMD, Yahoo, AOL, HealthCentral, Healthline, Everyday Health, and Others Named Below. Disponível em: <<https://www.ftc.gov/sites/default/files/attachments/other-applications-petitions-and-requests/101123publiccmptdigitaldemocracy.pdf>>. p.7

privacidade, ao interferir nas decisões que o consumidor faz em sua consciência.

3. Perigo para o consumidor

A inteligência artificial, aliada às ciências comportamentais, pode potencializar ainda mais a manipulação da decisão do consumidor. A publicidade se torna a modificação de comportamento em grande escala²². Ryan Calo²³ dá exemplos como o de um estudo de marketing que demonstrou que mulheres se sentiam menos atraentes na segunda-feira e recomendou que o mercado focasse nesse momento de vulnerabilidade para vender produtos de beleza. Contudo, o perigo é que conclusões como esta – que utilizam da fragilidade humana para induzir a aquisição de bens – já podiam ser tomadas no século passado, quando começou a se falar da economia comportamental. Agora práticas perigosas podem ser potencializadas com a IA.

Observa-se que o meio principal de ganhar dinheiro das mídias sociais atualmente é pela mudança de comportamento do usuário, em que eles detêm o poder de criar vícios²⁴ que podem ser usados para favorecer a compra de bens que satisfaçam o vício criado pelo próprio mercado, aprisionando abusivamente o consumidor e suas fragilidades e vontades.

Ademais, o algoritmo utilizado pelas redes sociais é capaz de entender como cada pessoa reage quando está triste ou feliz. Inclusive, pode aumentar a pressão social em cima de um usuário se entender que ele está mais suscetível a consumir quando está triste – e o faz por meio de comentários negativos em postagens e exibição de conteúdo de usuários que o próprio algoritmo tenha

22 LANIER, Jaron. Ten arguments for deleting your social media accounts right now. New York: Henry Holt and company, 2018.

23 CALO, Ryan. Digital market manipulation. *George Washington Law Review*, v. 82, n. 4, p. 995–1051, 2014. p.3

24 LANIER, Jaron. Ten arguments for deleting your social media accounts right now. New York: Henry Holt and company, 2018. p. 12

reportado que fazem aquela pessoa se sentir triste, por exemplo²⁵.

Além disso, a tecnologia consegue identificar sentimentos pelo uso de palavras positivas²⁶, um pequeno detalhe que, unido às demais práticas, pode gerar resultados fidedignos. O algoritmo pode colocar no feed um anúncio logo após um vídeo que potencialmente fez o usuário rir, se entender que feliz ele tende a consumir mais²⁷. E há outras maneiras de a inteligência artificial compreender as emoções de um usuário, como pelos emoticons utilizados em um texto, pela sequência de faixas de músicas solicitadas, por sensores que captam o movimento para detectar o estado emocional e por sistemas de percepção de sorrisos quando o usuário assiste um vídeo²⁸, tendo sido, até mesmo, patenteada a tecnologia de direcionamento de anúncios com base em emoções²⁹.

Pode-se se dizer que o Regulamento 2016/679 da União Europeia (RGPD) e a Lei 13.709/2018 (LGPD) no Brasil, ao protegerem mais os dados³⁰, inibiram as práticas reportadas neste trabalho. Contudo, em que pese a maior proteção, não se pode olvidar que poucos dados são requeridos para tecer as práticas supramencionadas. Na verdade, o consumidor pode não ter fornecido dado algum e ainda assim ser alvo dessa forma publicitária, em razão da permissão de outros usuários.

25 LANIER, Jaron. Ten arguments for deleting your social media accounts right now. New York: Henry Holt and company, 2018. p. 27

26 PARISER, Eli. The Filter Bubble: What the Internet Is Hiding from You. London: Viking/Penguin Press, 2011. p. 68

27 LANIER, Jaron. Ten arguments for deleting your social media accounts right now. New York: Henry Holt and company, 2018. p. 14

28 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 46

29 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 46

30 Importante mencionar que desde 1999, a Comissão Europeia tem se atentado para as inúmeras transações e possibilidades de o consumidor ter seus dados coletados indevidamente pela internet. Cfr.: Procedure 1999/0153/COD, COM (1999) 337: Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos da Comunidade e à livre circulação desses dados.

Aliás, o Professor Miguel Asensio³¹ já refletia que as tecnologias da sociedade da informação propiciaram obter e processar inúmeros dados e informações sobre interesses e comportamentos dos cidadãos, seja através do próprio tráfego de dados de provedores e serviços pela internet, seja pela captação indevida e sorrateira. Se, sob uma ótica, esses dados segmentados representam grande importância comercial para os fornecedores, sob outra, se obtidos de forma ilícita ou temerária, representará riscos substanciais ao consumidor.

É dizer: não é necessário que muitos consentam com o uso de seus dados, uma amostra menor permite que os agentes que capturam dados cheguem aos mesmos resultados³². Então, ainda que se acredite estar isolado dessas práticas, a permissão de outrem pode viabilizar as mesmas consequências. Para além, alguns dados pessoais, como o nome, podem se tornar irrelevantes, os softwares são tão avançados que não interessa identificar o usuário como pessoa, ele se torna o conjunto de números que corresponde à determinada publicidade que se encaixa melhor com aquelas informações³³.

A atenção requerida agora é porque esta forma de análise comportamental em massa pode afetar a capacidade do ser humano de decidir. Ao adentrar nesse perfilhamento, as grandes empresas passam a apresentar as opções e induzir a tomada de decisão³⁴. Assim, por mais que a captura de dados não tenha invadido a privacidade, a forma de manipulação destes dados quando se destina a adentrar no comportamento do consumidor

31 ASENSIO, Pedro Alberto de Miguel. *Derecho Privado de Internet*. 5ª ed. Madrid: Civitas Ediciones, 2015, p. 390 e ss..

32 VENTURINI, T.; ROGERS, R. "API-Based Research" or How can Digital Sociology and Journalism Studies Learn from the Facebook and Cambridge Analytica Data Breach. *Digital Journalism*, v. 7, n. 4, p. 532-540, 2019. p. 6

33 BAROCAS, Solon; NISSENBAUM, Helen. *Big Data's End Run around Anonymity and Consent. Privacy, Big Data, and the Public Good*. Cambridge: Cambridge University Press, 2014. p. 44-75. Disponível em: <<https://nissenbaum.tech.cornell.edu/papers/BigDatasEndRun.pdf>>.

34 PARISER, Eli. *The Filter Bubble: What the Internet Is Hiding from You*. London: Viking/Penguin Press, 2011. p.67

e modificá-lo afeta a privacidade porque interfere na tomada de decisão individual.

Sobre o tema, em pesquisa científica, a professora Sibony³⁵ concluiu, através de estudos de casos, que o fornecedor pode distorcer o comportamento do consumidor através de determinadas práticas, mesmo que inconscientes, levando-o a contratar instantaneamente e de forma impensada³⁶. Ou seja, não são cumpridos os requisitos da suitability³⁷ (adequabilidade) da informação, cujos parâmetros fundamentais são especialmente a exatidão, dimensão sucinta, compreensibilidade, clareza e fácil acesso.

Com efeito, a questão central é que a IA pode ser vantajosa para o consumidor, mas também pode ser preocupante, pois pode transformar a publicidade convencional que apresenta o bem ao consumidor em uma publicidade que busca aperfeiçoar-se na missão de forçar o consumo.

Considerações finais

Em se tratando de publicidade que se aproveita de condição de saúde e da fraqueza de conhecimento, a norma consumerista brasileira já tem disposição que poderia afastar ou punir práticas como a da indústria farmacêutica americana. Trata-se do art. 39, VI,

35 A conduta persuasiva psicológica do fornecedor deve ser melhor estudada, em que pese não existirem conclusões imediatas de como a psicologia pode influenciar diretamente o direito, seja como matéria de prova ou de outra forma. Cfr.: SIBONY, Anne-Lise. Can EU Consumer Law Benefit from Behavioural Insights? An analysis of the unfair practices directive. *European Review of Private Law*, Alphen aan den Rijn, v. 22, n. 6, p. 901-941, 2014.

36 Confira noção desenvolvida por: MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor: um estudo dos negócios jurídicos de consumo no comércio eletrônico*. São Paulo: Revista dos Tribunais, 2004, p. 273.

37 Para mais, Cfr.: LIZ, Jorge Pegado. *Algumas reflexões a propósito dos direitos dos consumidores à informação*. Liber Amicorum Mário Frota: A Causa dos Direitos dos Consumidores. Coimbra: Almedina, 2012, p. 344.

do Código de Defesa do Consumidor³⁸, segundo o qual a publicidade não pode aproveitar-se de certas fraquezas do consumidor.

Embora seja consoladora a previsão da lei brasileira, lembre-se que muitas dessas práticas simplesmente não são vistas. Neste estudo, houve, em verdade, uma considerável dificuldade em encontrar casos recentes em que a inteligência artificial foi usada de forma perigosa em publicidades comportamentais. Não à toa Frank Pasquale³⁹ falava sobre o segredo dos algoritmos que controlam dinheiro e informação. Exatamente por essa falta de informação que é ainda mais necessário fomentar a discussão sobre este assunto e estimular a transparência por parte das empresas.

Não há problema, de plano, na utilização de sistemas de IA em publicidade comportamental. O problema é quando as empresas utilizam a tecnologia para buscar e lucrar em cima das vulnerabilidades do consumidor⁴⁰. Esse é o verdadeiro perigo: ter suas decisões alteradas fora de sua consciência e ser induzido agressivamente a consumir. A ética precisa encontrar espaço e preservar a integridade do que há de mais privado no indivíduo, suas decisões particulares.

Deve-se retomar a publicidade como a forma de oferecer o bem de consumo, sem forçar o consumo. Também há benefício na própria publicidade comportamental, que é receber os anúncios mais interessantes, mas resiste a face perigosa, ser forçosamente compelido a comprar por fatores desconhecidos pelo indivíduo.

Referências Bibliográficas

38 Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas:

IV - prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços;

39 PASQUALE, Frank. *The Black Box Society: the secret algorithms that control money and information*. Cambridge: Harvard University Press, 2015.

40 CALO, Ryan. Digital market manipulation. *George Washington Law Review*, v. 82, n. 4, p. 995–1051, 2014. p.3

ABDCOMM. Disponível em: <<https://abcomm.org/noticias/com-uso-de-inteligencia-artificial-infracommerce-expande-same-day-delivery-para-outras-capitais-do-brasil/>>. Acesso em: 29 set. 2021.

ABRARDI, Laura; CAMBINI, Carlo; RONDI, Laura. Artificial intelligence, firms and consumer behavior: A survey. *Journal of Economic Surveys*, n. July, p. 1–23, 2021.

ASENSIO, Pedro Alberto de Miguel. *Derecho Privado de Internet*. 5ª ed. Madri: Civitas Ediciones, 2015.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. *Privacy, Big Data, and the Public Good*. Cambridge: Cambridge University Press, 2014. p. 44–75. Disponível em: <<https://nissenbaum.tech.cornell.edu/papers/BigDatasEndRun.pdf>>.

BARROS, J. P. L. O direito de arrependimento nos contratos eletrônicos de consumo como forma de extinção das obrigações. In: *Estudos de direito do consumidor*. Coimbra: Centro de direito do consumo, 2018.

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

CALO, Ryan. Digital market manipulation. *George Washington Law Review*, v. 82, n. 4, p. 995–1051, 2014.

FRAZÃO, Ana. Capitalismo de vigilância e black box society. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/capitalismo-de-vigilancia-e-black-box-society-28022019>>. Acesso em: 23 mar. 2021.

FTC. Complaint, Request for Investigation, Public Disclosure, Injunction, and Other Relief: Google, Microsoft, QualityHealth, WebMD, Yahoo, AOL, HealthCentral, Healthline, Everyday Health, and Others Named Below. Disponível em: <<https://www.ftc.gov/sites/default/files/attachments/other-applications-petitions-and-requests/101123publiccmptdigitaldemocracy.pdf>>.

LANIER, Jaron. Ten arguments for deleting your social media

accounts right now. New York: Henry Holt and company, 2018.

LIZ, Jorge Pegado. Algumas reflexões a propósito dos direitos dos consumidores à informação. Liber Amicorum Mário Frota: A Causa dos Direitos dos Consumidores. Coimbra: Almedina, 2012.

MARQUES, Cláudia Lima. Confiança no comércio eletrônico e a proteção do consumidor: um estudo dos negócios jurídicos de consumo no comércio eletrônico. São Paulo: Revista dos Tribunais, 2004, p. 273.

MOTHERSBAUGH, David L.; HAWKINS, Del I. Consumer behavior: building marketing strategy. 13. ed. Eugene: McGraw-Hill Education, 2016. p. 67

PARISER, Eli. The Filter Bubble: What the Internet Is Hiding from You. London: Viking/Penguin Press, 2011. p.104

PASQUALE, Frank. The Black Box Society: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

SIBONY, Anne-Lise. Can EU Consumer Law Benefit from Behavioural Insights? An analysis of the unfair practices directive. European Review of Private Law, Alphen aan den Rijn, v. 22, n. 6, p. 901-941, 2014.

THALER, Richard; SUSTEIN, Cass. Nudge. Tradução: Ângelo Lessa. Rio de Janeiro: Objetiva, 2019.

THALER, Richard. Misbehaving. Tradução: George Schlesinger. 1 ed. Rio de Janeiro: Intrínseca, 2019.

THALER, Richard. Toward a Positive Theory of Consumer Choice. Journal of Economic Behavior and Organization, v. 1, n. 1, 1980, p. 39-40.

VENTURINI, T.; ROGERS, R. “API-Based Research” or How can Digital Sociology and Journalism Studies Learn from the Facebook and Cambridge Analytica Data Breach. Digital Journalism, v. 7, n. 4, p. 532-540, 2019.

O uso de tecnologia de reconhecimento facial pelo poder público: necessidade de regulação específica em defesa da privacidade

Governmental use of Facial Recognition Technology: specific regulations is needed to protect privacy

Christiane Bedini Santorsula¹

Marcos Vinícius Sales dos Santos²

Sumário: Introdução. 1. Algoritmos de reconhecimento facial: aplicações e vulnerabilidades quanto ao uso pelo Poder Público; 2. Panorama global sobre o uso de reconhecimento facial e casos de banimento de uso em locais públicos; 3. Considerações Finais; Referências.

Resumo: O presente estudo aborda os riscos gerados à privacidade dos indivíduos e à proteção de dados como efeitos do uso indiscriminado e não regulado de tecnologias de reconhecimento facial pelo Estado para segurança e monitoramento de locais públicos. Por meio de revisão bibliográfica e exploração do cenário normativo, o trabalho analisa o crescimento de aplicações de tecnologia para reconhecimento facial e identifica as problemáticas advindas da falta de acurácia de tal tecnologia, bem como da inexistência de planos de tratamento dos dados armazenados. O trabalho apresenta os movimentos mundiais relacionados à limitação de uso da ferramenta sob análise e as preocupações associadas. Identificou-se que, em alguns locais, há normas proibitivas da utilização da mencionada ferramenta, enquanto em outros há um completo vácuo regulatório. Aborda-se o panorama no Brasil diante das normas existentes sobre privacidade e proteção de dados. Concluiu-se que há a necessidade de uma regulação específica que veicule parâmetros concernentes à auditabilidade, à proporcionalidade, à transparência e à segurança de dados com a finalidade de assegurar adequado equilíbrio entre a privacidade do indivíduo e atuação do Estado para efetivação de segurança pública.

1 . Doutoranda e mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Advogada. Professora. Membro efetivo da Comissão de Compliance da Ordem dos Advogados do Brasil - São Paulo. E-mail: christiane.bedini@gmail.com.

2 . Doutorando e mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Procurador do Município de São Paulo. Advogado. E-mail: mvsales.adv@gmail.com.

Palavras-chave: Reconhecimento Facial; Inteligência Artificial; Proteção de Dados; Privacidade; Segurança Pública.

Abstract: This study addresses the risks to privacy and data protection derived from indiscriminate and unregulated use of facial recognition technologies by the State aiming security and monitoring of public places. The work is grounded on literature and regulatory scenario reviews and analyzes the growth of technology applications for facial recognition and identification as problems arising from the lack of accuracy, as well as the lack of incident plans. The work presents the global initiatives related to facial recognition bans and restrictions of use and related concerns. Key findings were presented to show that rules banned the use of the tool in some places, while in others there is a complete regulatory vacuum. The study also broadly addresses, the Brazilian regulatory overview on privacy and data protection. It was concluded that there is a need for a specific regulation to embed standards on auditability, proportionality, transparency and data security to provide proper balance between the individual's privacy and the State's duty on public security effectiveness.

Keywords: Facial Recognition; Artificial Intelligence; Data Protection; Privacy; Public Security.

Introdução

O presente estudo analisa os problemas emergentes do uso de tecnologia de reconhecimento facial (TRF) pelo Estado em locais públicos como estratégia direcionada à tutela da segurança pública. O cenário digital sempre representou um desafio ao Direito como modulador de condutas sociais, já que a expansão tecnológica abre novas possibilidades sem que o legislador seja capaz de acompanhá-las e determinar seus limites³.

Iniciativas globais abordando o uso de TRF confirmam a necessidade de soluções que produzam equilíbrio entre a garantia das liberdades e privacidade dos indivíduos e as vantagens provenientes de uso de tecnologia de reconhecimento facial pelo Poder Público no incremento de segurança pública e prevenção de

3 INDUSTRY, I. In the Face of Danger: Facial Recognition and the Limits of Privacy Law. *Harvard Law Review* v. 120, 2007, pp 1870-1891. p.1872

ilícitos⁴.

Para desempenhar essa complexa tarefa, o Estado deve agir de modo eficiente, porquanto a segurança pública é, ao mesmo tempo, um direito dos cidadãos e um dever do Estado⁵. Contudo, as ações devem ser moldadas pelos direitos e garantias fundamentais⁶, dentre os quais destacamos, para os fins do presente estudo, os direitos à privacidade e à proteção de dados. Esse raciocínio deriva da escorreita compreensão do princípio da proporcionalidade que, ao mesmo tempo, veda tanto a tutela deficiente quanto interdita excessos⁷. Dessa constatação advém a necessidade de encontrar um ponto de equilíbrio entre o poder-dever estatal de adotar maneiras para garantir tanto a segurança pública quanto a tutela do direito à intimidade.

1. Algoritmos de reconhecimento facial: aplicações e vulnerabilidades quanto ao uso pelo Poder Público

Ubiquidade e perenidade são adjetivos associados à sensação de insegurança que permeia as relações sociais⁸. Hassemer, com razão, anotou que “os riscos de lesões são, ao mesmo tempo, abrangentes, devastadores e difusos. Conseguimos preparar-nos apenas precariamente para as lesões esperadas, e não conseguimos

4 Cf. DE LA FUENTE, Elvira. Las herramientas de investigación tecnológica en la Convención de Budapest y su incorporación a la legislación española. In: FRANCISCO, José Carlos; LORENCINI, Bruno Cesar; GRAU RUIZ, María Amparo; SÁNCHEZ-URÁN, María Yolanda. (Org.). Nuevas Tecnologías y Derecho: retos y oportunidades planteados por la Inteligencia Artificial y la Robótica. 1ed.Porto (Portugal): Juruá Editorial, 2019, p. 170-174.

5 Como já reconhecido, no Brasil, pelo Supremo Tribunal Federal: RE 559646 AgR, Relatora Ministra Ellen Gracie, Segunda Turma, publicado no DJe de 24-06-2011.

6 HASSEMER, Winfried. Direito Penal: fundamentos, estrutura, política. Trad. Adriana Beckman Meirelles et al. Porto Alegre: Sérgio Antonio Fabris Ed, 2008, p. 277-278.

7 SARLET, Ingo Wolfgang. Constituição, proporcionalidade e Direitos Fundamentais: o Direito Penal entre proibição de excesso e de insuficiência. Revista Opinião Jurídica (Fortaleza), Fortaleza, v. 4, n. 7, p. 160-209, jun. 2006, p. 178-180.

8 BECK, Ulrich. Sociedade de Risco: rumo a uma outra modernidade. 2 ed. trad. Sebastião Nascimento. São Paulo: Editora 34. 2011, p. 23.

remediar os danos inesperados”⁹. Dada a impossibilidade fática de se alocar um agente público fisicamente em cada local para a vigilância, novas tecnologias como a de reconhecimento facial (TRF) se apresentam como alternativas para o controle estatal.

Para dimensionar a problemática abordada, importa referir que o mercado de aplicação de TRF encontra-se em franca expansão com projeção de faturamento próxima da marca de 10 bilhões de dólares em 2027, com parcela significativa proveniente de aquisições dos sistemas pelo Poder Público¹⁰. As referidas contratações estão notadamente associadas ao escaneamento biométrico para monitoramento e ao rastreamento de indivíduos sem o seu conhecimento, intensificando o receio de monitoramento em massa de forma totalmente indiscriminada¹¹.

A biometria é a mensuração e análise de características físicas e comportamentais com o propósito de verificação da identidade do indivíduo, sendo certo que um dos seus usos mais comuns é o reconhecimento facial¹² por meio de tecnologia que escaneia o rosto de uma pessoa¹³. Diferentemente das formas tradicionais de verificação de dados biométricos, o reconhecimento facial

9 HASSEMER, Winfried, Op. cit, p. 275.

10 WESTBROOK, Myranda. Global Privacy concerns of facial recognition big data. Honors Theses. University of Tennessee, 2020. Disponível em . <https://scholar.utc.edu/honors-theses/292> p.5

11 Ibidem, p. 10. E mais adiante: “there is a deep concern on the part of the public in the use of the biometric information that is being collected and how it can be used to personally identify an unsuspecting person in the future. This information can be misused and should be monitored The security measures put in place to regulate the use of facial recognition technology should be strongly inclusive as to include future uses of this technology” (p. 16).

12 PITTMAN, Jeffrey. Privacy in the age of doxxing. Southern Journal of Business and Ethics; Vol. 10, 2018, p. 53-58, p. 53

13 “A face pode ser capturada a alguns metros de distância. É uma técnica não invasiva, não oferecendo nenhum tipo de risco à saúde do usuário. A desvantagem é que o sistema não é capaz de reconhecer gêmeos idênticos. O reconhecimento se dá através da imagem adquirida da face, que basicamente pode ser do tipo bidimensional ou tridimensional. Medidas geométricas da face como distâncias entre olhos e nariz, curvatura da boca e outras ou como o uso de imagens da face como um todo são algumas das técnicas usadas na classificação de faces”. (ZIMMERMAN, Antonio Carlos. Reconhecimento de faces humanas através de técnicas de inteligência artificial aplicadas a formas 3D. Tese (Doutorado em Engenharia Elétrica), Universidade Federal de Santa Catarina, Florianópolis, 2003, p.37).

viabiliza formas ampliadas de identificação e vigilância remotas de grande número de pessoas sem o conhecimento destas¹⁴. Esse monitoramento em massa representa problema associado ao uso secundário ou manipulado dos dados sem qualquer tipo de controle, transparência ou prestação de contas¹⁵. Vale dizer, há o risco real de que os dados coletados por tais ferramentas com a finalidade de assegurar a segurança pública seja utilizada indevidamente para outros propósitos, o que tem aptidão para atingir direitos fundamentais¹⁶ como as liberdades de expressão e de associação, bem como à privacidade.

A revolução tecnológica e as novas formas e interação social, política e econômica não podem se desenvolver em detrimento da privacidade¹⁷. Tanto é assim que as legislações, majoritariamente, têm se esforçado em valorizar a privacidade e a proteção de dados como forma de garantir a própria dignidade da pessoa humana e o exercício da democracia¹⁸. A tarefa encerra complexidades sobre os limites de regulação das tecnologias de um lado e, de outro, as restrições de uso em prol de liberdades individuais. Essa malha complexa de elementos se verifica em razão da transformação digital como elemento de ascensão dos dados à condição de ativo valioso numa era do capitalismo em que os indivíduos têm seus dados coletados, armazenados e utilizados para outros objetivos,

14 GARVIE, Clare et. al. The perpetual line-up: Unregulated police face recognition in America. Georgetown Law, Center on Privacy & Technology, 2016, p.10

15 Cf. SOLOVE, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, p. 745, 2007, GWU Law School Public Law Research Paper No. 289, p. 767

16 GARVIE, Clare et. al. Op. Cit. p.16

17 INDUSTRY, I. Op. Cit p. 1881. "When lives of ordinary citizens are suddenly searchable, moments of naivete or indiscretion become lasting reminders open to entire world. This phenomenon creates the risk that individuals will be judged solely on the basis of their moments of weakness, thus erasing a lifetime of good".

18 FRAZÃO, Ana. Fundamentos da proteção de dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo, FRAZÃO, Ana, OLIVA, Milena (Coord.) Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. Thomson Reuters São Paulo, 2019. P. 49

extrapolando as finalidades originais¹⁹.

A despeito da multiplicação de normas de proteção de dados pessoais, privacidade e inteligência artificial, questões sobre TRF não são adequadamente tratadas pela legislação existente, que se mostra insuficiente para regular a matéria diante das lacunas verificadas, particularmente quanto ao seu uso pelo Poder Público.²⁰ No Brasil, apesar da utilização das TRF em algumas cidades, como o Rio de Janeiro, existe um preocupante vácuo normativo tanto quanto aos limites e padrões a serem observados por tais sistemas²¹. A Lei Geral de Proteção de Dados – LGPD²² (Lei nº 13.709/2018) expressamente optou (artigo 4º) por excluir do âmbito de sua disciplina o tratamento de dados pessoais realizado para fins exclusivamente segurança pública, defesa nacional, segurança do estado ou atividades de investigação e repressão de infrações penais. O parágrafo primeiro do mesmo artigo 4º delegou à legislação específica a tarefa de disciplinar o uso e condições específicas relacionadas. No parágrafo quarto, determina que a Autoridade Nacional de Proteção de Dados (ANPD) publicará diretivas sobre o tema. Recentemente criada no Brasil, a atuação da ANPD é, ainda, incipiente e não há diretiva nesse sentido. Importante notar que a lei brasileira seguiu as excecionalidades de aplicação da lei de proteção de dados europeia (General Data Protection Regulation

19 ZUBOFF, Shoshana. The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019. Profile books, 2019. A autora aborda o capitalismo de vigilância e chama a coleta excessiva e despropositada de dados para múltiplos fins de “behavioral surplus”.

20 Nesse sentido, Frank Pasquale quanto ao Estado e entidades privadas como extratores de dados em grande escala, fazendo com que os indivíduos e seus comportamentos fiquem sob escrutínio constante, enquanto os indivíduos sabem nada, ou muito pouco, sobre a atuação do Estado e qual a destinação dos dados coletados e armazenados. O autor define esse fluxo unilateral de informações como “one way mirror”. In PASQUALE, Frank. The black box society. Harvard University Press, 2015.

21 ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. Revista Digital de Direito Administrativo, [S. l.], v. 8, n. 1, p. 171-204, 2021, p. 178-179.

22 Depois de intensos debates até sua sanção, a lei teve o início de sua vigência foi prorrogado 2020. Porém, para aplicação de sanções administrativas o prazo foi prorrogado para agosto de 2021.

– GDPR) que também enfrenta questões de vácuos legislativos, como será abordado adiante²³. No cenário brasileiro, atualmente está em discussão na Câmara dos Deputados uma anteprojeto²⁴ sobre o tratamento de dados pessoais na esfera criminal.

Não bastassem a ausência de transparência sobre o uso secundário dos dados biométricos coletados com o reconhecimento facial e a ausência de normas regulatórias específicas, outro problema chama a atenção: a baixa acurácia do reconhecimento facial. Dentre as biometrias existentes, a TRF apresenta os maiores índices de erros (falsos positivos ou negativos), impactando diretamente grupos vulneráveis como mulheres e pessoas negras²⁵. Assim, é possível dizer que o uso de tais tecnologias é “especialmente arriscado em contextos nos quais determinados grupos já são historicamente objeto de tratamento discriminatório”²⁶. Esses dados revelam o potencial das TRF como reprodutora em massa de preconceitos, o que chama a atenção para a governança adequada dos projetos e reforça a necessidade de regulação específica dos limites e possibilidades de sua utilização.

Por fim, outro aspecto relaciona-se ao controle e à fiscalização de quem desenvolve e opera os sistemas de reconhecimento facial e outras tecnologias de acordo com contratação realizada pelo Estado. A adequada due diligence nas relações das empresas desenvolvedoras para o fornecimento das tecnologias também merece destaque. As questões são relevantes na medida se

23 A União Europeia, publicou a Diretiva (UE) 2016/680, buscou preencher questões sobre investigação e persecução penal, mas não se mostra como adequada para dirigir pontos relacionados ao uso e tecnologias como a de reconhecimento facial e os riscos envolvidos. AO ESPECIFICA. AAR AS LINHAS DE COMPOSICAMENTO interessante. as tambolvidos. ento e de gerenciamento de crises. of their mome

24 Conhecido como “LGPD Penal”, o anteprojeto foi entregue no dia 05 de novembro de 2020 à Câmara dos Deputados pelo presidente da Comissão de Juristas, o Ministro Néfi Cordeiro, do Superior Tribunal de Justiça.

25 Com referências a vários estudos sobre o tema da baixa acurácia do reconhecimento facial por algoritmos, ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A. Op. cit, p. 174-175.

26 ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A., op. cit, p. 175.

tais atividades estão excepcionadas da LGPD cria-se um limbo normativo²⁷ com alto grau de risco que confirma a necessidade de normas especiais.

2. Panorama sobre o uso de reconhecimento facial e casos de banimento de uso em locais públicos

As aproximações conceituais e as reflexões sobre as problemáticas atuais, tal como expostas no tópico anterior, demonstraram que a contemporaneidade não é apenas marcada pela sociedade da informação que se movimenta no cenário de economias digitais. Essa economia dirigida por dados (“data driven economy”) também se caracteriza pela inserção continuada de novas tecnologias com poucas informações sobre o seu funcionamento e riscos potenciais, além de insuficiente regulação.

Recentemente, a União Europeia publicou diretrizes para a regulação de inteligência artificial. O documento define biometria e aponta que reconhecimento por sistemas que operam de maneira remota e amplificada (vigilância em massa) mostram-se aplicações com alto grau de risco, demandando normas restritivas ou mesmo proibitivas.²⁸ Reconhecendo a importância da proposta regulatória, os órgãos reguladores de proteção de dados no âmbito da UE, quais sejam, European Data Protection Supervisor (EDPS) e o European Data Protection Board (EDPB), publicaram em Junho de 2021 parecer sobre o tema, abordando explicitamente os riscos de tecnologias para reconhecimento facial, sugerindo a cessação de uso até que haja normas específicas que preencham lacunas de segurança jurídica e social.²⁹ O parecer conjunto das citadas autoridades de dados justifica sua diretriz ao indicar que não há

27 MENEZES, Joyceane B.; COLAÇO, Hian S.. Quando a Lei Geral de Proteção de Dados não se aplica? In: TEPEDINO, Gustavo, FRAZÃO, Ana, OLIVA, Milena (Coord.) Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. Thomson Reuters São Paulo, 2019. p. 187

28

29 Disponível em https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

meios de discernir se a implementação TFR e seu uso continuado respeitará os requisitos de proporcionalidade e necessidade, de modo a assegurar a captura biométrica por reconhecimento facial em nível aceitável de interferência em direitos fundamentais. Casos noticiados nos EUA e relacionados a uso tendencioso, com viés discriminatório e verificação de acurácia precária³⁰, serviram como propulsores para diversas iniciativas de amplitude federais, bem como no âmbito dos Estados federados para estabelecer, restrições ou cessação de uso. Em resposta a diversos movimentos sociais. Em 2020, IBM, Microsoft e Amazon cessaram comercialização de TRF para órgãos públicos e, em 2021, reiteraram seu comprometimento, com a moratória em razão dos vieses tendenciosos ³¹.

Vários projetos de lei para regular a matéria encontram-se em tramitação no Congresso norte-americano. Para ilustração importante para o estudo, cita-se dois projetos apresentados em 2020 a saber, (i) o Projeto de Lei Ethical Use of Facial Recognition Act que menciona o caráter de desproporcionalidade de uso e falta de acurácia bem como a preocupação com o alto potencial da tecnologia violar direitos fundamentais como a privacidade.³² A ementa do projeto deixa clara a preocupação ao sintetizar a proibição de não haverá investimento em TFR sem devido processo interno de autorização para o engajamento da conduta de uso

30 Estudo do Massachusetts Institute of Technology sobre acurácia em TRF determinou quantidade significativa de vieses tendenciosos especialmente em mulheres e negros. Ver <https://www.media.mit.edu/articles/facial-recognition-software-is-biased-towards-white-men-researcher-finds/>. Esse estudo foi seguido de ampla pesquisa pelo National Institute of Standards and Technology, que trouxe dados sobre o desenvolvimento e bons grau de acurácia dos algoritmos de alguns desenvolvedores, mas demarcaram a insegurança em relação a diversos outros, explorando vieses discriminatórios e desvios de análise de gênero e raça. Conferir íntegra em https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf#page=49.

31 Em comunicado oficial dirigido ao Congresso norte-americano, está Disponível em <https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/>

32 <https://www.congress.gov/116/bills/s3284/BILLS-116s3284is.pdf>

da tecnologia³³ e o Facial Recognition and Biometric Technology Moratorium Act³⁴

Ainda nos EUA, o Estado de Illinois, foi o pioneiro em normatizar questões de identificação biométrica e diante dos avanços da TRF, manteve tendência de restrições e proibição de uso por entidades do setor privado. Em Utah, lei aguarda sanção traz condições de aplicação de TRF, estabelecendo a capacitação obrigatória para os agentes públicos que façam uso da tecnologia, bem como autorização prévia para utilização e necessidade de dupla validação humana dos resultados apontados pelo sistema, além de obrigar as autoridades a informar os espaços em que a identificação poderá ocorrer.³⁵ A cidade São Francisco, na Califórnia, foi uma das primeiras a determinar o banimento do uso; Los Angeles, Portland, Boston e Nova Iorque também exararam normas banindo ou limitando TRF até existência de regulação específica.³⁶

Em vigor a partir de Julho de 2021, o Estado de Washington sancionou lei com para regular o uso de tecnologia de reconhecimento facial pelo Poder Público. A nova lei traz um vetor importante de regulação: accountability. De acordo com a norma, nenhuma autoridade pública poderá desenvolver, adquirir ou usar tecnologia de reconhecimento facial sem antes submeter um relatório de prestação de contas (accountability report). Estabelece a necessária revisão humana por profissional capacitado e que tenha autonomia para modificar a decisão sobre a identificação com TRF, inclusive nas situações em que se verifique ameaça à privacidade. Destaca-se ponto da lei sobre a revisão pública,

33 “This bill prohibits any officer, employee, or contractor of a federal agency from engaging in specified activities with respect to facial recognition technology without a warrant until a congressional commission established by this bill recommends rules governing the use and limitations on both government and commercial use of such technology.(...) <https://www.congress.gov/bill/116th-congress/senate-bill/3284>

34 <https://www.congress.gov/116/bills/s4084/BILLS-116s4084is.pdf>

35 Texto na íntegra disponível em <https://legiscan.com/UT/text/SB0034/id/2336227/Utah-2021-SB0034-Enrolled.pdf>

36 Até a data de finalização deste trabalho, a cidade de Los Angeles estava debatendo sobre afrouxamento das restrições e esse tipo de debate também tomou novo corpo no Reino Unido.

demonstrando a necessidade de participação da sociedade civil.³⁷ Na Austrália³⁸ e no Canadá³⁹ foram publicadas diretrizes que exploram a matéria e convidam os reguladores a sopesar os riscos e estabelecer vetores normativos efetivos. O uso de TRF na China teve aumento exponencial durante a pandemia de COVID-19 e seu uso difundido e confrontado na mesma proporção, levou o supremo tribunal popular do país (China's Supreme People's Court) a estabelecer novas regras de reconhecimento facial em locais públicos.⁴⁰ Todas essas iniciativas mostram os desafios inerentes ao tema e as convergências institucionais ao perceber o assunto deve ser enfrentado com cautela.

3. Considerações finais

O estudo identificou o amplo uso de tecnologias de reconhecimento facial por vários Estados com a finalidade declarada de aumentar a segurança pública. Não obstante seu aspecto positivo, a ferramenta sob análise vem sendo usada de forma indiscriminada, sem regulação específica quanto aos limites e possibilidades de sua aplicação, sem auditabilidade e sem transparência, a qual não se limita à informação de que os dados serão coletados; diz respeito notadamente a como são coletados e como são utilizados e auditados⁴¹. Notou-se também que há o risco

37 SAVAGE, C. W. Washington Enacts First-in-Nation State Law Regulating Governmental Use of Facial Recognition Technology. *Intellectual Property & Technology Law Journal*, [s. l.], v. 32, n. 7, p. 21–23, 2020. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=144723573&lang=pt-br&site=ehost-live>.

38 Australia Human Rights Commission moratorium on facial recognition tech Maio de 2021, https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf

39 Cf. RICHARDSON, Rashida. Facial Recognition in the Public Sector: The Policy Landscape. German Marshall Fund of the United States, 2021. <http://www.jstor.org/stable/resrep28529>.

40 Casos de vazamento Clearview AI e Verkada, empresas que fornecem TRF para órgãos de governo reforçam as preocupações sobre regulação específica e restrições necessárias diante do risco à privacidade.

41 HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital, desafios para o Direito. Rio de Janeiro: Forense 2021. P.87

de utilização dos dados para finalidades distintas da segurança pública (usos secundários não declarados), assim como o fato de que a baixa acurácia das TRF afetam mais intensamente grupos sociais historicamente prejudicados (impacto desproporcional).

As discussões sobre os parâmetros regulatórios demandam ampla discussão social e pressão externa para accountability. Dentre as balizas indispensáveis para a normatização do uso de tais ferramentas, destacam-se a proporcionalidade⁴², a transparência, a capacitação dos agentes utentes do sistema, revisão humana, relatórios de impacto e de tratamento de incidentes e certificação adequada de desenvolvedores⁴³, testes externos de acurácia. Outros pontos importantes se relacionam a realização de testes prévios de interesse para o uso⁴⁴, regras de auditabilidade e colocação de sinais de informação ao público sobre uso nos espaços em que for empregada a TRF⁴⁵. O elenco de fatores expostos acima demonstra que o percurso para atingir soluções é promissor, mesmo com todos os tumultos, o que é natural em momentos históricos que marcarão mudanças importantes para a sociedade.

Referências

ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, [S. l.], v. 8, n. 1, p. 171-204, 2021.

42 SOLOVE, Daniel. Op.cit. p. 753

43 KINDT, Els J. Transparency and Accountability Mechanisms for Facial Recognition. German Marshall Fund of the United States, 2021, <http://www.jstor.org/stable/resrep28527.p.6>acialhecimento Fácioslopment of . asileira de protepeu de proteno viment des negativas quando uma conduta se encontra carente de acialhecimento Fácioslopment of . asileira de protepeu de proteno viment des negativas quando uma conduta se encontra carente de

44 Testes de interesse são necessários de modo a garantir proporcionalidade. Criando os limites das relações. Manter a privacidade e habilidade de nos sentirmos únicos, sem a erosão de identidade e soberania sobre si mesmo. Cf. INDUSTRY, I. Op. cit, pp. 1887-1888.

45 Cf. RICHARDSON, Rashida. Op. cit.

AUSTRALIA HUMAN RIGHTS COMMISSION. Moratorium on facial recognition technology Maio de 2021. https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf

BECK, Ulrich. Sociedade de Risco: rumo a uma outra modernidade. 2 ed. trad. Sebastião Nascimento. São Paulo: Editora 34. 2011.

DE LA FUENTE, Elvira. Las herramientas de investigación tecnológica en la Convención de Budapest y su incorporación a la legislación española. In: FRANCISCO, José Carlos; LORENCINI, Bruno Cesar; GRAU RUIZ, María Amparo; SÁNCHEZ-URÁN, María Yolanda. (Org.). Nuevas Tecnologías y Derecho: retos y oportunidades planteados por la Inteligencia Artificial y la Robótica. 1ed.Porto (Portugal): Juruá Editorial, 2019

EUROPEAN DATA PROTECTION BOARD. Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)Disponível em https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo, FRAZÃO, Ana, OLIVA, Milena (Coord.) Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. Thomson Reuters São Paulo, 2019.p49

GARVIE, Clare et. al. The perpetual line-up: Unregulated police face recognition in America. Georgetown Law, Center on Privacy & Technology, 2016.Disponível em <https://www.perpetuallineup.org/p.10>

HASSEMER, Winfried. Direito Penal: fundamentos, estrutura, política. Trad. Adriana Beckman Meirelles et al. Porto Alegre: Sérgio Antonio Fabris Ed, 2008.

HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital:

transformação digital, desafios para o Direito. Rio de Janeiro: Forense 2021. P.87

INDUSTRY, I. In the Face of Danger: Facial Recognition and the Limits of Privacy Law. *Harvard Law Review* v. 120, 2007, pp 1870-1891

KINDT, Els J. Transparency and Accountability Mechanisms for Facial Recognition. German Marshall Fund of the United States, 2021, <http://www.jstor.org/stable/resrep28527>

MASSACHUSETTS INSTITUTE OF TECHNOLOGY <https://www.media.mit.edu/articles/facial-recognition-software-is-biased-towards-white-men-researcher-finds/>.

MENEZES, Joyceane B.; COLAÇO, Hian S.. Quando a Lei Geral de Proteção de Dados não se aplica? In: TEPEDINO, Gustavo, FRAZÃO, Ana, OLIVA, Milena (Coord.) Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. Thomson Reuters São Paulo, 2019

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf#page=49.

PASQUALE, Frank. The black box society. Harvard University Press, 2015.

PITTMAN, Jeffrey. Privacy in the age of doxxing. *Southern Journal of Business and Ethics*; Vol.10 2018 pp. 53-58. Disponível em : <https://www.proquest.com/openview/d6dfff44fc44ce4fe82727034d59d478/1?pq-origsite=gscholar&cbl=316220>

RICHARDSON, Rashida. Facial Recognition in the Public Sector: The Policy Landscape. German Marshall Fund of the United States, 2021. <http://www.jstor.org/stable/resrep28529>.

SARLET, Ingo Wolfgang. Constituição, proporcionalidade e Direitos Fundamentais: o Direito Penal entre proibição de excesso e de insuficiência. *Revista Opinião Jurídica (Fortaleza)*, Fortaleza, v. 4, n. 7, p. 160-209, jun. 2006.

SAVAGE, C. W. Washington Enacts First-in-Nation State Law Regulating Governmental Use of Facial Recognition Technology. *Intellectual Property & Technology Law Journal*, [s. l.], v. 32, n. 7, p. 21–23, 2020. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=144723573&lang=pt-br&site=ehost-live>.

SILVA SÁNCHEZ, Jesús-María. *A expansão do Direito Penal. Aspectos da política criminal nas sociedades pós-industriais*. Tradução de Luiz Otávio de Oliveira Rocha. 3ª ed. São Paulo: Editora Revista dos Tribunais, 2013.

SOLOVE, Daniel J., ‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy. *San Diego Law Review*, Vol. 44, p. 745, 2007, GWU Law School Public Law Research Paper No. 289, Disponível em <https://ssrn.com/abstract=998565> .

WESTBROOK, Myranda. *Global Privacy concerns of facial recognition big data*. Honors Theses. University of Tennessee, 2020. Disponível em. <https://scholar.utc.edu/honors-theses/292>

ZIMMERMAN, Antonio Carlos. *Reconhecimento de faces humanas através de técnicas de inteligência artificial aplicadas a formas 3D*. Tese (Doutorado em Engenharia Elétrica), Universidade Federal de Santa Catarina, Florianópolis, 2003.

ZUBOFF, Shoshana. *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama’s books of 2019*. Profile books, 2019.

UNITED STATES OF AMERICA Senate. Projeto de Lei 3284. <https://www.congress.gov/116/bills/s3284/BILLS-116s3284is.pdf>

UNITED STATES OF AMERICA Senate. Projeto de Lei 4084. <https://www.congress.gov/116/bills/s4084/BILLS-116s4084is.pdf>

UNITED STATES OF AMERICA. State Of Utah. Projeto de Lei 0034. <https://legiscan.com/UT/text/SB0034/id/2336227/Utah-2021-SB0034-Enrolled.pdf>

Inteligência artificial como ferramenta auxiliar no processamento de execuções fiscais no Brasil: panorama e perspectivas

Artificial Intelligence applied to tax collection suits as a tool to enhance litigation process in Brazil: overview and perspectives

Marcos Vinicius Sales dos Santos¹

Vivian Leinz²

Sumário: Introdução. 1. Inteligência artificial no Poder Judiciário brasileiro; 2. Potencialidades da inteligência artificial para melhoria do processamento da execução fiscal; 3. Considerações finais. Referências.

Resumo: Tendo como problema a necessidade de incremento da qualidade da prestação jurisdicional, o presente estudo analisou se a inteligência artificial pode contribuir para a melhoria do processamento das execuções fiscais no Brasil, favorecendo a mitigação dos índices de congestionamento processual e da quantidade de tarefas repetitivas a serem desempenhadas pelos juízes e seus auxiliares, liberando-os para a prática de atos mais complexos que exigem a cognição humana. Identificaram-se vários projetos envolvendo inteligência artificial em andamento no Judiciário brasileiro, dentre eles alguns que dizem respeito ao processamento de executivos fiscais. Buscou-se descrever brevemente esses últimos, bem como os resultados obtidos por meio desses projetos para o aprimoramento da prestação jurisdicional. Concluiu-se que a utilização da inteligência artificial contribui efetivamente para a celeridade e a eficiência do processamento dos executivos fiscais, diminuindo o tempo de tramitação do processo e a necessidade de intervenção humana em etapas que não demandam grande grau de cognição, permitindo a localização mais rápida do devedor e de bens passíveis de penhora, e alavancando a arrecadação, devendo ser ampliado seu espectro para outras jurisdições e funcionalidades.

Palavras-chave: Inteligência Artificial; Execução Fiscal; Efetividade da Tutela

1 Marcos Vinicius Sales dos Santos. Doutorando e mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Procurador do Município de São Paulo. Advogado. Endereço eletrônico: mvsales.adv@gmail.com.

2 Vivian Leinz. Doutoranda e mestra em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Procuradora da Fazenda Nacional. Endereço eletrônico: vileinz@hotmail.com

Judicial.

Abstract: Having as a problem the need to increase the quality of the justice delivery system, this study analyzed whether artificial intelligence could contribute to improving the process of lawsuits that aim to collect unpaid taxes in Brazil, favoring the mitigation of procedural congestion rates and the number of repetitive tasks to be performed by judges and their assistants, freeing them to practice more complex acts that require human cognition. Several projects involving artificial intelligence in progress in the Brazilian Judicial System were identified, among them some related to lawsuits issued to collect unpaid taxes. We sought to briefly describe the latter, as well as the results obtained through these projects for the improvement of the justice delivery system. The conclusion was that the use of artificial intelligence effectively contributes to the speed and efficiency of lawsuits that aim to collect unpaid taxes, reducing the processing time and the need for human intervention in stages that do not require a great degree of cognition. Besides that, artificial intelligence allows an increase in the speed to locate a debtor and his assets, thereby improving tax collection. Therefore, artificial intelligence should be expanded to other jurisdictions and functionalities.

Keywords: Artificial Intelligence; Tax collection lawsuit; Effectiveness of the Judicial System.

Introdução

O Brasil tem adotado uma série de iniciativas voltadas à progressiva melhoria da qualidade da prestação jurisdicional. A legislação processual tem passado por sucessivas reformas para enfrentar o fenômeno da litigância repetitiva e propiciar melhor gestão do grande acervo processual.

Ainda dentre essas providências, é digna de nota a criação do processo judicial eletrônico, regulamentado pela Lei nº 11.419/2006, que possibilitou a utilização de tecnologias da informação em grande escala para automatizar trâmites processuais, o que trouxe

maior celeridade à atuação do Poder Judiciário³ e deu início à “virada tecnológica”⁴ no contexto das políticas públicas de gestão de conflitos.

Mesmo com tantos esforços para dar vazão à enorme quantidade de casos que chegam ao Estado-juiz todos os dias, é conhecido o atual estágio de congestionamento dos tribunais brasileiros no que diz respeito ao número de processos judiciais. De acordo com o relatório Justiça em Números, no final do ano de 2020 o Judiciário contava com 75,4 milhões de processos em andamento, com taxa de congestionamento líquida de 69,1% (excluídos processos suspensos, sobrestados em arquivo provisório) e bruta de 73%⁵. A “razoável duração do processo”, erigida à condição de direito fundamental (art. 5º, LXXVIII, da CRFB), ainda é uma promessa não cumprida.

Importa destacar que mais da metade dos processos judiciais em curso no ano de 2020 se referiam a execuções. Por sua vez, as execuções fiscais consistiam em 68% do estoque desse tipo de processo, sendo as principais “responsáveis pela alta taxa de congestionamento do Poder Judiciário, representando aproximadamente 36% do total de casos pendentes e

3 Sobre o tema, vide BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Caderno PJe: Processo Judicial Eletrônico. Brasília: CNJ, 2016; FUNDAÇÃO GETULIO VARGAS (Brasil). Políticas Públicas do Poder Judiciário: uma análise quantitativa e qualitativa do impacto da implantação do Processo Judicial Eletrônico (PJe) na produtividade dos Tribunais. Brasília: CNJ, 2017; PORTO, Fábio Ribeiro. O impacto da utilização da inteligência artificial no executivo fiscal: estudo de caso do Tribunal de Justiça do Rio de Janeiro. Direito em Movimento, v. 17, p. 142-199, 2019, p. 159-161.

4 NUNES, Dierle José Coelho. Virada tecnológica no Direito Processual (da automação à transformação): seria possível adaptar o procedimento pela tecnologia?. In: NUNES Dierle, LUCON, Paulo Henrique dos Santos, WOLKART Erik Navarro. (Org.). Inteligência Artificial e Direito Processual: Os Impactos da Virada Tecnológica no Direito Processual. 2ed.Salvador: Juspodivm, 2021, v. 1, p. 17-54.

5 BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Justiça em Números 2021. Brasília, CNJ, 2021. p. 102 e 126.

congestionamento de 87% em 2020”⁶.

Para debelar a crise acima delineada, cogitam-se inúmeras possibilidades⁷. Dentre elas, merece destaque a crescente utilização de tecnologias da informação no âmbito do Judiciário para além da digitalização e da automação já propiciadas pelo processo judicial eletrônico (PJE). Em atenção a essa realidade, a presente pesquisa, valendo-se do método hipotético-dedutivo, volta-se a investigar se inteligência artificial (IA) pode contribuir para a melhoria do processamento das execuções fiscais no Brasil, favorecendo a mitigação dos índices de congestionamento processual e a quantidade de tarefas repetitivas a serem desempenhadas pelos juízes e seus auxiliares, liberando-os para a prática de atos mais complexos que exigem a cognição humana.

1 Aplicações da inteligência artificial no Poder Judiciário brasileiro

Como registrado por Jordi Nieva Fenoll, são possíveis diversos usos da inteligência artificial na esfera judicial, dentre os quais podem ser destacados: a) em matéria de procedimento, viabilizando a automação da marcha processual⁸; b) no auxílio da valoração da prova de acordo com padrões determinados⁹; c) na argumentação, auxiliando na construção de alegações persuasivas¹⁰.

As aplicações da IA na atividade jurisdicional podem ser classificadas da seguinte forma: a) Robô-Classificador, que tem

6 Ibidem, p. 169. Para ampla análise dos impactos das execuções fiscais para o congestionamento dos tribunais brasileiros, vide PORTO, Fábio Ribeiro. O impacto da utilização da inteligência artificial no executivo fiscal: estudo de caso do Tribunal de Justiça do Rio de Janeiro. *Direito em Movimento*, v. 17, p. 142-199, 2019, com o reconhecimento de que, “no quadro geral das execuções, o maior problema é a execução fiscal” (p. 149).

7 Por exemplo, meios alternativos de resolução de disputas e desjudicialização da execução fiscal.

8 FENOLL, Jordi Nieva. *Inteligencia artificial y proceso judicial*. Marcial Pons. Madrid, 2018, p. 24-25.

9 Ibidem, p. 26-28.

10 Ibidem, p. 28-31.

como objetivo principal catalogar informações úteis para auxiliar movimentações processuais e o processo de tomada de decisão pelos humanos, tais como precedentes e dispositivos normativos possivelmente aplicáveis ao caso, além de sugerir ou gerar modelos de documentos; b) Robô-Relator, que extrai e condensa dados a partir da mineração de textos, identifica onde estão as peças processuais, sumariza os argumentos das partes, sugere minutas de atos judiciais etc.; c) Robô-Julgador, com características similares ao modelo anterior, mas com a capacidade adicional de julgar casos repetitivos¹¹.

A utilização da inteligência artificial pelo Poder Judiciário brasileiro já é uma realidade. Conforme informações disponibilizadas pelo Conselho Nacional de Justiça (CNJ), tais ferramentas já são utilizadas para triagem de casos de grande massa mediante a classificação de petições iniciais de acordo com temas estabelecidos para facilitar o trabalho dos julgadores no tratamento em bloco de casos similares, movimento processual inteligente com a sugestão do próximo ato a ser praticado, análise de prevenção, identificação de similaridade processual, leitura, identificação e extração de partes de julgados, geração de texto para o magistrado com base nos escritos anteriores, produção de resumos de textos (sumarizador)¹² e outros.

De acordo com dados reunidos pelo CNJ no “Painel de Projetos com Inteligência Artificial no Poder Judiciário”¹³, em 2019 havia quarenta e um projetos envolvendo inteligência artificial em andamento no Judiciário brasileiro, os quais foram desenvolvidos por trinta e dois tribunais.

11 A classificação é proposta por BOEING, Daniel Henrique Arruda; MORAIS DA ROSA, Alexandre. Ensinando um robô a julgar: pragmática, discricionariedade, heurísticas e vieses no uso de aprendizado de máquina no judiciário. 1. ed. Florianópolis: EMais, 2020, p. 234-235.

12 BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Inteligência artificial no Poder Judiciário brasileiro. Brasília, CNJ, 2019. p. 29-32.

13 BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Projetos com inteligência artificial no poder judiciário. Disponível em <<https://paineisanalytics.cnj.jus.br/single/?appid=29d710f7-8d8f-47be-8af8-a9152545b771&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&opt=ctxmenu,cursel>>. Acesso em: set. 2021.

A expansão dos usos da IA pelo Judiciário brasileiro é objeto de preocupação pelo CNJ que, em 21/08/2020, editou a Resolução nº 332 para dispor sobre a transparência e a governança na produção e no uso de tais ferramentas. Tal ato normativo, dentre outras coisas, prescreve: a necessidade de garantia da segurança jurídica e isonomia entre os jurisdicionados (art. 5º); o tratamento adequado de dados utilizados para o desenvolvimento e treinamento da IA, com a plena observância da Lei Geral de Proteção de Dados (arts. 6º e 9º); a preservação da igualdade, a não discriminação, a pluralidade e a solidariedade como diretrizes a serem observadas quando da tomada de decisões apoiadas em ferramentas de IA (art. 7º) e a realização de testes, previamente à colocação em produção, para verificar se o modelo de IA está afetado por algoritmos enviesados com tendências discriminatórias (art. 7º, §§1º, 2º e 4º).

2. Potencialidades da inteligência artificial para melhoria do processamento da execução fiscal

Uma importante premissa para o uso da IA como ferramenta auxiliar no processamento da execução fiscal é o baixo grau de cognição judicial nesses casos. O processo de conhecimento volta-se a certificar a existência de um direito (solucionar crise de incerteza), que pode demandar profunda análise do conjunto fático-probatório e altas indagações jurídicas durante a atividade de construção da norma aplicável ao caso concreto; o processo de execução, por sua vez, possui atividade voltada a satisfazer o direito do credor estampado no título executivo (crise de inadimplemento), motivo pelo qual a cognição em tais casos é eventual e limitada¹⁴. Em nosso entendimento, essa característica dos processos de execução tornam estes feitos bons candidatos à intervenção com tecnologias da informação, porquanto restam mitigadas as justas preocupações com os vieses algorítmicos.

14 Não se desconhece o fenômeno do “sincretismo processual”, que mistura as atividades cognitivas e executivas na mesma relação processual.

A execução fiscal possui dois gargalos importantes, sendo o primeiro deles a própria citação do devedor.¹⁵ Em muitos casos os órgãos administrativos de cobrança, como a Receita Federal e as Secretarias de Fazenda, já esgotaram as possibilidades de localização do devedor, repetindo o Judiciário as mesmas diligências infrutíferas com vistas à sua citação. O segundo dos gargalos da execução fiscal é a localização de bens do devedor.¹⁶

Ultrapassar esses óbices é imperativo para diminuir o tempo de tramitação média da execução fiscal e, por consequência, dos processos como um todo, melhorando o grau de congestionamento do Judiciário, baixando o estoque de processos e contribuindo para uma resposta jurisdicional mais ágil e eficiente. As potencialidades da utilização da IA nos executivos fiscais revelam-se no enfrentamento desses entraves e na automação da própria marcha processual.

Do total de quarenta e um projetos identificados pelo Conselho Nacional de Justiça envolvendo inteligência artificial em andamento no Judiciário brasileiro, cinco visam ao aprimoramento do processamento das execuções fiscais.

O projeto “HÉRCULES”, iniciativa conjunta do TJAL e da Universidade Federal de Alagoas – UFAL, foi implementado em 2019 na 15ª Vara Cível – Fazenda Municipal de Maceió. A principal função do robô é classificar as petições intermediárias, separando-as em categorias específicas, para então serem trabalhadas. Antes

15 De acordo com relatório de pesquisa do Instituto de Pesquisa e Ensino Avançado - IPEA denominado “Custo Unitário do Processo de Execução Fiscal na Justiça Federal”, em mais de 40% dos casos o devedor não é localizado, não se aperfeiçoando a triangulação processual: “Apenas 3,5% dos executados apresentam-se voluntariamente ao juízo”. “Em 47,4% dos processos ocorre pelo menos uma tentativa inexitosa de citação, e em 36,9% dos casos não há qualquer citação válida. Como a citação ocorre por edital em 6,4% dos casos, pode-se afirmar que em 43,5% dos executivos fiscais o devedor não é encontrado pelo sistema de justiça”. (INSTITUTO DE PESQUISA ECONÔMICA APLICADA. Custo unitário do processo de execução fiscal na justiça federal. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/relatoriopesquisa/121009_relatorio_custounitario_justicafederal.pdf>. Acesso em: set. 2021. p. 19).

16 Em apenas 15% dos casos há penhora de bens. Desses, em somente 2,6% ocorre leilão judicial, exitoso ou não. Unicamente em 0,2% dos casos o resultado da hasta será suficiente à satisfação integral do débito e em 0,3% deles a adjudicação do bem enseja a extinção da dívida. (Ibidem, p. 20).

da criação desse sistema, todas as petições eram classificadas em intermediárias e encaminhadas a um escaninho único, cabendo aos servidores o processo repetitivo de triá-las e separá-las. Desde a criação desse projeto, já foram classificadas 11.330 petições (dados de abril de 2021), o que incrementou a eficiência da prestação jurisdicional. Com esse projeto o TJAL foi finalista do “Prêmio Inovação - Judiciário Exponencial” no ano de 2020, concorrendo com iniciativas do Conselho Nacional de Justiça e do Supremo Tribunal Federal.^{17 18}

O projeto “TIA” do TJAP, utilizado como piloto nos juizados cíveis e da fazenda pública, faz a leitura de processos e a identificação de demandas repetitivas, facilitando a atuação do Poder Judiciário em lote¹⁹. Assim que ocorre o protocolo de petição inicial, o robô faz uma busca no sistema e verifica se há ação semelhante em curso, realizando então o agrupamento dos processos.²⁰

O projeto “HÓRUS” do TJDFT surgiu no contexto de uma demanda de digitalização dos processos desse tribunal, que se encerraria em 2020, cujo procedimento se demonstrou moroso na etapa concernente à carga dos processos no Processo

17 BRASIL. PODER JUDICIÁRIO DE ALAGOAS. Robô Hércules classifica mais de 11 mil petições e agiliza trabalho da 15ª Vara Cível: Uso de inteligência artificial está ajudando uma das Varas mais demandadas do Judiciário alagoano. Disponível em: <<https://www.tjal.jus.br/noticias.php?pag=lerNoticia¬=18099>>. Acesso em: set. 2021.

18 Além de classificar as petições, o “HÉRCULES” valida o preenchimento de Certidões de Dívida Ativa, considerando os requisitos legais. (BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Projetos com inteligência artificial no poder judiciário. Disponível em: <<https://paineisanalytics.cnj.jus.br/single/?appid=29d710f7-8d8f-47be-8af8-a9152545b771&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&opt=ctxmenu,currsel>>. Acesso em: set. 2021.)

19 Ibidem.

20 BRASIL TRIBUNAL DE JUSTIÇA DO AMAPÁ. Robô de inteligência artificial é desenvolvido no TJAP para agilizar andamento de processos com demandas repetitivas. Disponível em: <<https://www.tjap.jus.br/portal/publicacoes/noticias/9768-%C2%B4rob%C3%B4-de-intelig%C3%Aancia-artificial-%C3%A9-criado-no-tjap-para-agilizar-andamento-de-processos-com-demandas-repetitivas.html>>. Acesso em: set. 2021.

Judicial Eletrônico – PJE e de seus respectivos metadados²¹, especialmente em relação aos processos da Vara de Execução Fiscal devido ao grande volume de processos por ela gerenciado.²² Foi descrito como “processamento inteligente para inserção de dados digitalizados para os casos da vara de Execução Fiscal”.²³ Com a utilização da ferramenta o tempo médio de cadastro de processos no PJE passou de 15 minutos para 14 segundos no caso de processos simples, já incluída a carga de dados básicos como classe, assunto, parte, advogado e endereço, e para 45 segundos na hipótese de processos mais complexos, garantindo-se maior rapidez no cadastro das demandas.²⁴

O projeto “ELIS” do TJPE foi concebido para auxiliar na triagem inicial de processos de execução fiscal, analisando inconsistências entre os dados da petição inicial, da Certidão de Dívida Ativa - CDA e aqueles cadastrados no PJE, verificando a competência e eventual prescrição. O resultado dessa iniciativa é “a redução de atividades manuais e repetitivas no âmbito da Execução Fiscal, possibilitando uma maior celeridade nos processos, redução de custos e da taxa de congestionamento.”²⁵ ELIS tem a capacidade de analisar por volta de 80 mil processos em 15 dias, ao passo que a triagem manual de 70 mil processos leva ao redor de um ano e meio para ser concluída. Por conta do reconhecimento da

21 BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Projetos com inteligência artificial no poder judiciário. Disponível em: <<https://paineisanalytics.cnj.jus.br/single/?appid=29d710f7-8d8f-47be-8af8-a9152545b771&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&opt=ctxmenu,currsel>>. Acesso em: set. 2021.

22 CAVALCANTE, Weiss Weber Araújo. MELO, Jairo Simão Santana. NEVES, Thiago Arruda. Hórus: processamento inteligente dos dados digitalizados da vara de execução fiscal do Distrito Federal. Revista CNJ, Brasília, DF, v. 3, n. 1, p. 51-64, jan./jun. 2019. p. 51

23 BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Inteligência artificial no Poder Judiciário brasileiro, p. 35.

24 BRASIL. TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS. TJDFt usa inteligência artificial para aprimorar sistemas. Disponível em: <<https://www.tjdft.jus.br/institucional/imprensa/noticias/2019/maio/tjdft-usa-inteligencia-artificial-para-aprimorar-sistemas>>. Acesso em: set. 2021.

25 BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Inteligência artificial no Poder Judiciário brasileiro. Coordenação: José Antônio Dias Toffoli; Bráulio Gabriel Gusmão. – Brasília: CNJ, 2019. p. 34.

eficiência dessa ferramenta, ela foi disponibilizada para utilização por outros tribunais brasileiros por meio da plataforma SINAPSES do Conselho Nacional de Justiça²⁶.

O projeto “Classificador de Petições de Execução Fiscal” do TJSC é uma ferramenta de apoio à triagem de processos de execução fiscal que classifica as petições em oito espécies distintas, permitindo seu posterior impulsionamento em bloco por intermédio de intervenção humana, mas sem apresentação de sugestão de minuta de atos a serem proferidos pelos juízes ou seus auxiliares.²⁷ Em relação a essa iniciativa não foram localizados dados acerca do incremento na atividade jurisdicional.

Além dos projetos catalogados pelo CNJ, há outros que merecem destaque.

Em 2018 o Tribunal de Justiça do Rio de Janeiro – TJRJ aplicou a inteligência artificial na execução de dívidas fiscais municipais, especificamente no bloqueio de bens do devedor. Por meio desse projeto reduziu-se o tempo de acesso aos sistemas utilizados para constrição de bens, passando-se de 35 minutos no modelo tradicional de cobrança realizado por um servidor público, para 25 segundos por meio da utilização de inteligência artificial, gerando um incremento em 1.400% na rapidez desse comando e permitindo o bloqueio de bens em 6.619 execuções fiscais. Em três dias esse sistema realizou a tarefa que levaria dois anos e meio se fosse feito pelos servidores da 12ª Vara da Fazenda Pública do Rio

26 BRASIL. TRIBUNAL DE JUSTIÇA DE PERNAMBUCO. TJPE disponibiliza ferramenta de IA para execução fiscal em Programa de formação do CNJ. Disponível em: <http://www.tjpe.jus.br/-/tjpe-disponibiliza-ferramenta-de-inteligencia-artificial-para-execucao-fiscal-em-programa-de-formacao-do-cnj?redirect=http%3A%2F%2Fwww.tjpe.jus.br%2Finicio%3Fp_p_id%3D3%26p_p_lifecycle%3D0%26p_p_state%3Dmaximized%26p_p_mode%3Dview%26_3_groupId%3D0%26_3_keywords%3Delis%26_3_struts_action%3D%252Fsearch%252Fsearch%26_3_redirect%3D%252F&inheritRedirect=true>. Acesso em: set. 2021.

27 BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Projetos com inteligência artificial no poder judiciário. Disponível em: <<https://paineisanalytics.cnj.jus.br/single/?appid=29d710f7-8d8f-47be-8af8-a9152545b771&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&opt=ctxmenu,currsel>>. Acesso em: set. 2021.

de Janeiro/RJ.²⁸

O Tribunal de Justiça do Rio Grande do Sul – TJRS adotou solução de inteligência artificial que sugere o despacho a ser proferido após a análise da petição inicial da execução fiscal e documentos anexos²⁹, enquanto o sistema “POTI” do Tribunal de Justiça do Rio Grande do Norte – TJRN realiza em segundos bloqueios de ativos financeiros.³⁰

Considerações finais

A inteligência artificial tem amplo campo de aplicação no Poder Judiciário brasileiro, especialmente na execução fiscal, dadas suas características de baixa carga cognitiva, procedimento repetitivo, enorme volume de processos em trâmite e grande base de dados para aprendizagem da máquina.

A utilização desse ferramental tecnológico auxilia na diminuição do “tempo morto” dos processos com a realização de atos automáticos (movimentação), permite a alocação de humanos para tarefas mais complexas que efetivamente demandam raciocínio, ajuda na celeridade e eficiência, identifica cobranças viáveis ou não a partir da análise de padrões e permite a localização mais rápida do devedor e de bens passíveis de penhora, auxiliando no incremento da arrecadação.

O sucesso no uso da inteligência artificial para aprimorar as execuções fiscais foi comprovado pelos resultados positivos obtidos com os projetos já existentes, podendo e devendo ser

28 BRASIL. TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. TJRJ adota modelo inovador nas cobranças de tributos municipais. Disponível em: <<http://www.tjrj.jus.br/noticias/noticia/-/visualizar-conteudo/5111210/5771753>>. Acesso em: set. 2021.

29 BRASIL. TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. Inteligência artificial nos processos de execução fiscal. Disponível em: <<https://www.tjrs.jus.br/novo/noticia/inteligencia-artificial-nos-processos-de-execucao-fiscal/>>. Acesso em: set. 2021.

30 BRASIL. CONSELHO NACIONAL DE JUSTIÇA. CNJ usará automação e inteligência artificial para destravar execução fiscal. Disponível em: <<https://www.cnj.jus.br/cnj-usara-automacao-e-inteligencia-artificial-para-destravar-execucao-fiscal/>>. Acesso em: set. 2021.

ampliado seu espectro para outras jurisdições e funcionalidades, contribuindo para o aprimoramento da eficiência jurisdicional em relação a essa espécie processual.

Referências bibliográficas

BOEING, Daniel Henrique Arruda; MORAIS DA ROSA, Alexandre. Ensinando um robô a julgar: pragmática, discricionariedade, heurísticas e vieses no uso de aprendizado de máquina no judiciário. 1. ed. Florianópolis: EMais, 2020, p. 234-235.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA. Caderno PJe: Processo Judicial Eletrônico. Brasília: CNJ, 2016. Disponível em: <https://www.cjf.jus.br/observatorio/arq/caderno_pje.pdf>. Acesso em set. 2021.

_____. Inteligência artificial no Poder Judiciário brasileiro. Brasília, CNJ, 2019. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2020/05/Inteligencia_artificial_no_poder_judiciario_brasileiro_2019-11-22.pdf>. Acesso em: set. 2021.

_____. Justiça em Números 2020. Brasília, CNJ, 2021, Disponível em: < <relatorio-justica-em-numeros2021-12.pdf> (cnj.jus.br)>. Acesso em: set. 2021.

_____. Projetos com inteligência artificial no poder judiciário. Disponível em: <<https://paineisanalytics.cnj.jus.br/single/?appid=29d710f7-8d8f-47be-8af8-a9152545b771&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&opt=ctxmenu,currsel>>. Acesso em: set. 2021.

BRASIL. TRIBUNAL DE JUSTIÇA DE ALAGOAS. Robô Hércules classifica mais de 11 mil petições e agiliza trabalho da 15ª Vara Cível: Uso de inteligência artificial está ajudando uma das Varas

mais demandadas do Judiciário alagoano. Disponível em: <<https://www.tjal.jus.br/noticias.php?pag=lerNoticia¬=18099>>. Acesso em: set. 2021.

BRASIL TRIBUNAL DE JUSTIÇA DO AMAPÁ. Robô de inteligência artificial é desenvolvido no TJAP para agilizar andamento de processos com demandas repetitivas. Disponível em: <<https://www.tjap.jus.br/portal/publicacoes/noticias/9768-%C2%B4rob%C3%B4-de-intelig%C3%Aancia-artificial-%C3%A9-criado-no-tjap-para-agilizar-andamento-de-processos-com-demandas-repetitivas.html>>. Acesso em: set. 2021.

BRASIL. TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS. TJDFt usa inteligência artificial para aprimorar sistemas. Disponível em: <<https://www.tjdft.jus.br/institucional/imprensa/noticias/2019/maio/tjdft-usa-inteligencia-artificial-para-aprimorar-sistemas>>. Acesso em: set. 2021.

BRASIL. TRIBUNAL DE JUSTIÇA DE PERNAMBUCO. TJPE disponibiliza ferramenta de IA para execução fiscal em Programa de formação do CNJ. Disponível em: <http://www.tjpe.jus.br/-/tjpe-disponibiliza-ferramenta-de-inteligencia-artificial-para-execucao-fiscal-em-programa-de-formacao-do-cnj?redirect=http%3A%2F%2Fwww.tjpe.jus.br%2Finicio%3Fp_p_id%3D3%26p_p_lifecycle%3D0%26p_p_state%3Dmaximized%26p_p_mode%3Dview%26_3_groupId%3D0%26_3_keywords%3Delis%26_3_struts_action%3D%252Fsearch%252Fsearch%26_3_redirect%3D%252F&inheritRedirect=true>. Acesso em: set. 2021.

BRASIL. TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. TJRJ adota modelo inovador nas cobranças de tributos municipais. Disponível em: <<http://www.tjrj.jus.br/noticias/noticia/-/visualizar-conteudo/5111210/5771753>>. Acesso em: set. 2021.

BRASIL. TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. Inteligência artificial nos processos de execução fiscal. Disponível em: <<https://www.tjrs.jus.br/novo/noticia/inteligencia-artificial-nos-processos-de-execucao-fiscal/>>. Acesso em: set. 2021.

CAVALCANTE, Weiss Weber Araújo. MELO, Jairo Simão Santana. NEVES, Thiago Arruda. Hórus: processamento inteligente dos dados digitalizados da vara de execução fiscal do Distrito Federal. Revista CNJ, Brasília, DF, v. 3, n. 1, p. 51-64, jan./jun. 2019.

FENOLL, Jordi Nieva. Inteligencia artificial y proceso judicial. Marcial Pons. Madrid, 2018, p. 24-25.

FUNDAÇÃO GETULIO VARGAS (Brasil). Políticas Públicas do Poder Judiciário: uma análise quantitativa e qualitativa do impacto da implantação do Processo Judicial Eletrônico (PJe) na produtividade dos Tribunais. Brasília: CNJ, 2017

INSTITUTO DE PESQUISA ECONÔMICA APLICADA. Custo unitário do processo de execução fiscal na justiça federal. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/relatoriopesquisa/121009_relatorio_custounitario_justicafederal.pdf>. Acesso em: set. 2021.

NUNES, Dierle José Coelho. Virada tecnológica no Direito Processual (da automação à transformação): seria possível adaptar o procedimento pela tecnologia?. In: NUNES Dierle, LUCON, Paulo Henrique dos Santos, WOLKART Erik Navarro. (Org.). Inteligência Artificial e Direito Processual: Os Impactos da Virada Tecnológica no Direito Processual. 2ed.Salvador: Juspodivm, 2021, v. 1, p. 17-54.

PORTO, Fábio Ribeiro. O impacto da utilização da inteligência artificial no executivo fiscal: estudo de caso do Tribunal de Justiça do Rio de Janeiro. Direito em Movimento, v. 17, 2019, p. 142-199.

Blockchain como mecanismo propulsor de conformidade tributária: panorama e perspectivas

Blockchain as a mechanism to foster tax compliance: overview and perspectives

Carlos Alexandre Dias Torres¹

Christiane Bedini Santorsula²

Sumário: Introdução 1. Evasão Fiscal e suas repercussões; 2. A tecnologia de blockchain: aplicações, tendências e benefícios para conformidade tributária (tax compliance) e ecossistema tributário de confiança e transparência; Considerações Finais.

Resumo: O presente trabalho tem como escopo abordar a tecnologia de blockchain e sua aplicação para otimização de conformidade tributária. Utilizando-se de revisão bibliográfica, o estudo aborda em sua primeira parte o cenário de evasão fiscal no Brasil e traça um panorama geral sobre tal problema no cenário mundial. Considerando malefícios sociais, políticos e econômicos advindos da evasão fiscal, a importância de maior compliance tributário fica destacado através de suas vantagens e contribuições para mitigação desse problema global. Em sua segunda parte, o trabalho explora o conceito de blockchain e suas aplicações atuais, destacando as aplicações potenciais para conformidade tributária efetiva, bem como expõe questões sobre tax morale e como o uso de blockchain poderia incrementar um ambiente de segurança, transparência e credibilidade tributários criando um movimento cíclico e virtuoso de tax compliance entre os setores público e privado.

Palavras-chave: blockchain; evasão fiscal; compliance tributário; big data; tax morale.

1 . Doutorando e mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Procurador da Fazenda Nacional no núcleo de fraudes fiscais estruturadas. Membro do Fórum de combate à corrupção e lavagem de dinheiro do Estado de São Paulo (FOCCOSP). Advogado. E-mail: calexandretorres@gmail.com

2 . Doutoranda e mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Advogada. Professora. Membro efetivo da Comissão de Compliance da ordem dos Advogados do Brasil - São Paulo. E-mail: christiane.bedini@gmail.com

Abstract: The present study approaches block chain technology and its application to enhance tax compliance. Using a literature review, the study firstly addresses, tax evasion and its repercussions in Brazil and worldwide. Taking into consideration social, political and economic harms arising from tax evasion, the importance of greater tax compliance is highlighted as a driver to mitigate this global problem. Secondly, the work analyses the concept of blockchain and its current applications, most notably potential applications for effective tax compliance, as well as poses debates related to tax morale and how the use of blockchain could foster an environment of tax security, transparency and credibility thus creating a cyclical and virtuous tax compliance environment between the public and private sectors.

Keywords: blockchain; tax evasion; tax compliance; big data; tax morale.

Introdução

A Era do Big Data³, no contexto da revolução digital, remodelou as formas de atuação de mercados, pautando novas relações econômicas e diferentes interações sociais. As economias globalizadas, responsáveis pela profusão de atividades empresariais com velocidade e impactos disruptivos, experimentam enfrentamento com novas tecnologias e movimento de inovação multiplicados com o agigantamento de dados em volume, velocidade e variedade, demandando reestruturações empresariais e institucionais.

Não obstante, novos problemas convivem ou asseveram problemas antigos, como a evasão fiscal, um tema de preocupação global. A abordagem de evasão fiscal convida inferência imediata sobre o prejuízo aos cofres públicos. Afinal, em decorrência dessa conduta ilícita, quantia bastante relevante deixa de ser arrecadada pelo Estado, frustrando a programação financeira e, por conseguinte, dificultando a satisfação de uma série de direitos

3 O termo Big Data refere-se a situações em que as tecnologias digitais são utilizadas para lidar com grandes e diversas quantidades de dados e às várias possibilidades provadas e públicas em diferentes contextos. Cf HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital, desafios para o Direito. Rio de Janeiro: Forense 2021. p.16 e 17

conferidos constitucionalmente aos cidadãos⁴. Logo, o prejuízo aos cofres públicos ressoa na falha institucional em proporcionar à sociedade contrapartidas básicas, dando azo a ameaças ao exercício dos direitos fundamentais dos indivíduos.⁵

As linhas acima traçaram contornos de um desafio inescapável: modulação de novas tecnologias para que gerem mais outputs positivos pelo combate a irregularidades crônicas do que outputs negativos pelo seu uso para finalidades escusas. Nesse sentido, nascem reflexões importantes sobre a necessidade de correto entendimento, capacitação e regulação de uso de tecnologias avançadas, para que haja maior espaço para benefícios e melhores ferramentas para banimento das aplicações abusivas. A tarefa é árdua e o instituto de compliance atua de forma indissociável sobre o sistema de governança das empresas, estimulando cumprimento de políticas e controles internos e atendimento a normas internas e externas, não apenas de caráter jurídico, mas também de caráter social.

Compliance e mitigação de riscos corporativos modifica a forma de tomada de decisões nas empresas, que se tornam mais responsivas a enforcement público e pressão da sociedade civil e outros grupos de interesse (stakeholders), passando a se reestruturar internamente para criação de valor. Compliance específico na seara tributária faz parte desse movimento de mudança de cultura, pois transcende a simples ideia de pagar tributos e cumprir obrigações acessórias (já que isso é mandatório por lei) e avança para análise de otimização das atividades e gerenciamento a adequado dos novos riscos mapeados.

Neste cenário de transformação digital, problemas tributários crônicos e necessidade de programas de compliance efetivos, este trabalho propôs a combinação entre blockchain e compliance como propulsora de melhor conformidade tributária e uma das

4 Cf. BUFFON, Marciano. Tributação e Dignidade Humana: Entre os Direitos e Deveres Fundamentais. Livraria do Advogado. Porto Alegre, 2009. p. 91.

5 HOLMES, Stephen; SUSTEIN, Cass R.. O custos dos direitos.: porque a liberdade depende dos impostos. Livro eletrônico. São Paulo : Martins Fontes, 2019.

formas de enfrentamento de desvios materiais, como a evasão fiscal.

1. A Evasão Fiscal e suas repercussões

Por definição, a evasão fiscal é uma estratégia elaborada pelo contribuinte voltada a obter uma economia indevida de tributos. Não se confunde com a denominada elisão, a qual é, majoritariamente⁶, conceituada como uma forma de planejamento lícito, idealizado por pessoa jurídicas e naturais e que lhes permita auferir um encargo fiscal menos oneroso⁷. A evasão fiscal é, assim, uma prática que atormenta diversos países, especialmente aqueles que adotam um modelo de Estado Fiscal, cujas receitas oriundas dos tributos constituem a principal fonte de custeio de suas atividades⁸. Uma pesquisa sobre o tema estima que as práticas tributárias ilícitas no mundo desviam, por ano, cerca de 3 trilhões de dólares do tesouro estatal⁹. Considerando apenas os países relacionados naquela pesquisa, o total de recursos que deixa de ser recolhido aos cofres públicos, a cada ano, equivale a mais de 5% da soma do Produto Interno Bruto (PIB) daquelas nações¹⁰. Os

6 “[...] o termo ‘elisão’ não poderia ser usado para significar a postura lícita do contribuinte na economia de tributos, devendo, por rigor linguístico, ser abandonado. Para evitar confusões no uso da linguagem e por melhor representar as condutas enfocadas, preferimos o termo ‘elusão’. ‘Elisão’, do latim *elisione*, significa ato ou efeito de elidir; eliminação, supressão”. TORRES, Heleno Taveira. *Direito Tributário e Direito Privado: Autonomia Privada: Simulação: Elusão Tributária*. São Paulo: Revista dos Tribunais. 2003. p. 188.

7 TORRES, Heleno Taveira. *Limites do Planejamento Tributário e a Norma Brasileira Antissimulação (LC 104/01)*. In: ROCHA, Valdir de Oliveira (coord.) *Grandes Questões Atuais do Direito Tributário*. vol. 5. São Paulo: Dialética. 2001. p. 103.

8 “Pois, sendo o estado fiscal o estado cujas necessidades financeiras são essencialmente cobertas por impostos, facilmente se compreende que ele tem sido (e é) a regra do estado moderno(...)”. NABAIS, José Casalta. *O Dever Fundamental de Pagar Impostos*. Livraria Almedina. Coimbra. 1998. p. 192.

9 SIQUEIRA, Marcelo Lettieri and RAMOS, Francisco de Souza. *A Economia da Sonegação: Teorias e Evidências Empíricas*. *Revista de Economia Contemporânea*, v.9, n.3. 2005. p. 577.

10 Tax Justice Network. *The cost of tax abuse: a briefing paper on the cost of tax evasion worldwide*. p. 2. Disponível em: <http://www.taxjustice.net/wp-content/uploads/2014/04/Cost-of-Tax-Abuse-TJN>

esquemas de elisão fiscal nem sempre ocorrem dentro os limites de legitimidade tributária. Muitos são os planejamentos abusivos que elegem conhecidos centros financeiros offshore como parte da estratégia ilícita, e isso representa mais um obstáculo ao exercício da atividade arrecadatória dos Estados¹¹.

O Brasil também sofre, sobremaneira com as consequências da evasão fiscal. As tipologias fraudulentas empregadas nesse desiderato são as mais diversas, como a utilização de “laranjas” ou “testas de ferro” na composição societária de empresas, a constituição das chamadas empresas “de fachada” para ocultar a operação e o patrimônio da verdadeira contribuinte, a simulação de operações empresariais etc. Em 2021, estima-se que os recursos que não foram devidamente recolhidos ao erário em decorrência de comportamentos ilícitos somam cerca de 500 bilhões de reais¹².

Em termos de enforcement, o Brasil também estabelece a aplicação de sanções rigorosas a quem é flagrado cometendo evasão fiscal. No âmbito federal, por exemplo, a multa prevista é de 150% (cento e cinquenta por cento) sobre a totalidade ou diferença de imposto ou contribuição nos casos de falta de pagamento ou recolhimento, de falta de declaração e nos de declaração inexata quando a conduta é dotada de elementos típicos de sonegação, fraude ou conluio. E se o contribuinte autuado se negar a prestar os esclarecimentos ou entregar a documentação requisitada pelo órgão fiscalizador, aquela penalidade pode chegar a 225%

11 Segundo estudo desenvolvido pela ONG Tax Justice Network (TJN), a partir de dados obtidos junto ao Fundo Monetário Internacional (FMI) e ao Bank of International Settlements (BIS), estima-se existirem cerca de US\$ 21 trilhões depositados em contas bancárias localizadas nos denominados paraísos fiscais, grande parte fruto de evasão fiscal. Cf. *The Price of Offshore Revisited*. Tax Justice Network. Londres. 2012. Disponível em: <<https://www.taxjustice.net/2014/01/17/price-offshorerevisited/#:~:text=MAIN%20REPORT%201%20%E2%80%93%20The%20Price,zero%20tax%20and%20substancial%20secrecy.>>. Acesso em 17 de março de 2020.

12 O que representa algo em torno de 20 mil reais por segundo evadidos no Brasil. Sonegômetro. Sindicato Nacional dos Procuradores da Fazenda Nacional – SINPROFAZ. Disponível em: <<http://www.quantocostaobrasil.com.br/>>. Acesso em 03 de fevereiro de 2021.

(duzentos e vinte e cinco por cento) sobre o tributo sonegado¹³. As medidas de enforcement, assim, sempre foram tidas como um verdadeiro incentivo negativo, tendo em vista que o receio quanto ao risco de fiscalização e punição é, sim, um elemento que estimula o cumprimento da norma tributária. Por outro lado, os meios coercitivos não são os únicos instrumentos existentes a convencer o contribuinte a recolher regularmente os seus tributos.

Nesse contexto, outras questões também podem ser apontadas como motivadoras da conformidade fiscal pelos contribuintes. Questões de ordem social, reputacional e outras relacionadas a tax morale¹⁴, por exemplo, surgem como grandes incentivadores da integridade fiscal, como estudado no tópico seguinte.

2. A tecnologia de blockchain: aplicações, tendências e viabilidade para compliance no ambiente tributário

Em apertada síntese, blockchain é um sistema tecnológico que opera mediante uma cadeia de informações em caráter descentralizado, permitindo aos participantes da cadeia de informações a distribuição com transparência, segurança e

13 Art. 44, §§ 1º e 2º. BRASIL. Lei n.º 9.430/96, de 27 de dezembro de 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9430.htm>. Acesso em 23 de abril de 2020.

14 “The term ‘tax morale’ is often used in reference to these types of influences on tax compliance. We will define tax morale broadly as an umbrella term capturing nonpecuniary motivations for tax compliance as well as factors that fall outside the standard, expected utility framework. For example, individuals may have some intrinsic motivation to pay taxes or feel guilt or shame for failure to comply. They may comply due to reciprocal motivations: the willingness to pay taxes in exchange for benefits that the state provides to them or to others even though their pecuniary payoff would be higher if they didn’t pay taxes.” Cf. LUTTMER, Erzo. F. P.; SINGHAL, Monica. Tax Morale. *Journal of Economic Perspectives*, [s. l.], v. 28, n. 4, p. 149–168, 2014. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=99368578&lang=pt-br&site=ehost-live> p. 150.

sigilo¹⁵, garantindo eficiência e imutabilidade dos dados.¹⁶ Com sua propagação iniciada na área financeira, notadamente com a emergência das criptomoedas¹⁷, a aplicação de blockchain em outros setores tem sido objeto de discussões relevantes que confirmam o seu benefício como ferramenta de prevenção dos riscos das operações, com precisão e confiabilidade. A implementação da tecnologia de blockchain na cadeia de fornecimento (supply chain) de setores como o agropecuário e o de saúde, bem como em soluções para desenvolvimento sustentável, tem tomado agendas de governos e órgãos internacionais.¹⁸ Nesse sentido, notável a iniciativa da União Europeia, através do Conselho Europeu de Inovação, em premiar soluções de alto impacto social através de aplicação de blockchain.¹⁹ Diante de tal expansão, este trabalho

15 LIANG, T.-P. et al. What Drives the Adoption of the Blockchain Technology? A Fit-Viability Perspective. *Journal of Management Information Systems*, [s. l.], v. 38, n. 2, p. 314–337, 2021. DOI 10.1080/07421222.2021.1912915. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=151799337&lang=pt-br&site=ehost-live>. p. 315 . Os autores ensinam que “Blockchain is an emerging technology that underlies a series of peer-to-peer transactions to protect the transaction records, called blocks. For protecting each block, blockchain technology utilizes time stamps, cryptographic hash, and data structures to prevent data or information from being tampered. With such design features, blockchain technology provides several advantages, such as decentralization (function without intermediary), immutability (unchangeable and indestructible), anonymity (hidden real-world identity), traceability (irrefutable record), and security (smart contract)”p. 316

16 TISCINI, R. et al. The blockchain as a sustainable business model innovation. *Management Decision*, London, v. 58, n. 8, p. 1621-1642, 2020. The strongest feature of BC, data security, is the reason why, even if it was firstly applied to financial markets (i.e. Bitcoin), now its uses are extended also to other markets, such as the agri-food industry, where data security and the validity of an entire history of transactions is of central importance. p. 1624

17 Sobre isso ler VASQUEZ, Geraldo. An Introduction to Blockchain. *CPA Journal*, [s. l.], p. 52–55, 2021. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=151374392&lang=pt-br&site=ehost-live>

18 Nesse sentido, vide GOMEZ-TRUJILLO Ana Maria, OCAMPO, Juan Velez-, GONZALEZ-PEREZ, Maria Alejandra, Trust, Transparency, and Technology: Blockchain and Its Relevance in the Context of the 2030 Agenda, *The Palgrave Handbook of Corporate Sustainability in the Digital Era*, 10.1007/978-3-030-42412-1, (561-580), (2021). s is of central importance. P.o de Sroblem. a; tax morale. I, Vicente (Org.). *Teoria JURidica ect privacye encontra carente de*

19 Mais sobre as soluções premiados no sitio oficial da Comissão Europeia <https://digital-strategy.ec.europa.eu/en/news/commissions-european-innovation-council-awards-eu5-million-blockchain-solutions-social-innovations>

sugere uma exploração introdutória sobre o uso de blockchain por empresas de maneira a impulsionar tax compliance, causando, inclusive, efeito positivo na dinâmica de atuação da administração tributária.

Temas de ordem tributária têm servido de alvo para diversas mudanças de conduta e criação de mecanismos de prevenção, detecção e remediação de irregularidades e atos ilícitos, engajando empresas na criação de programas de compliance mais robustos e que tenham pauta específica para tributos, concentrando esforços na construção de novos modelos comportamentais²⁰. Uma nova análise de estruturas voltadas à inserção de temas de ética e sustentabilidade às estratégias empresariais e a melhores controles internos, buscam otimizar soluções e gerenciamento de crises²¹. A aplicação de blockchain como ferramenta que limite falsificações e proporcione transparência quanto aos atos praticados numa cadeia obrigacional tributária, proporcionam melhor controle e monitoramento, um dos pilares de programas de compliance. Porém, para melhor apontar os demais benefícios dessa tecnologia para compliance tributário, é necessário abrir caminho de compreensão sobre os elementos que dirigem tax compliance para, na sequência, indicar como a blockchain atuaria sobre tais elementos de maneira a otimizar sua operacionalização.

Para essa contextualização, importante destacar que conformidade tributária não se funda apenas em melhor enforcement público, aumento de fiscalizações e imposição de

20 “All firms exist within a nexus of legal, regulatory, and social norms. The contemporary compliance function is the means by which firms adapt their behavior to these constraints. More concretely, compliance is the set of internal processes used by firms to adapt behavior to applicable norms”. GRIFFITH, Sean J. Corporate governance in a era of compliance. *William & Mary Law Review*, v. 57, n. 6, 2016, p. 2.081. Disponível em: <https://core.ac.uk/downloads/pdf/73973569.pdf>. Acesso em: 31 jan. 2020.

21 DINIZ, Eduardo Saad. Ética negocial e compliance entre a educação executiva e interpretação judicial. São Paulo: RT, 2019, p. 33.

multas mais altas²². Esses elementos ganham musculatura quando combinados com outros fatores de influência em tax compliance tais como:²³ (i) incentivos positivos a contribuintes que tenham bom nível de conformidade, tais como descontos e inclusão em programas de benefícios fiscais; (ii) a confiança nas autoridades cria um ambiente de conformidade no qual o contribuinte tem uma percepção de credibilidade²⁴ e movimento reflexo de segurança; (iii) aumento de base de dados e cruzamentos de dados pelas autoridades fiscais criam o entendimento de presença do Estado e monitoramento fiscal que impulsiona compliance; (iv) transparência sobre o funcionamento do sistema tributário e as iniciativas de governo criam um cenário de pertencimento do contribuinte, que fica mais inclinado à conformidade; (v) a simplificação do sistema fiscal também movimentam reforço para compliance²⁵ e (vi) questões de caráter moral e social também se mostram como impulsos importantes de compliance²⁶

Trata-se de um movimento de cultura ética durante o qual a utilização de tecnologia de blockchain pode auxiliar na efetividade de compliance ao fornecer uma cadeia segura de verificação de

22 Embora não consigam, sozinhos, resolver questões de tax noncompliance, são vetoriais no exercício do poder do Estado na melhor detecção de ilegalidades tributárias com uso efetivo de mecanismos de sanção, gerando compliance tributário. Cf., LIN MEI TAN; BRAITHWAITE, V. Motivations for tax compliance: the case of small business taxpayers in New Zealand. *Australian Tax Forum*, v. 33, n. 2, p. 221–247, 2018. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=130659943&lang=ptbr&site=ehost-live> p. 227

23 Cf. ALM, James et. Al., *New Technologies and the Evolution of Tax Compliance* (May 18, 2020). *Virginia Tax Review*, Vol. 39, No.3, Spring 2020, UC Irvine School of Law Research Paper No. 2020-42, Available at SSRN: <https://ssrn.com/abstract=3604507> pp. 294 e ss

24 Vide TORGLER, Benno.; SCHNEIDER, F. *What Shapes Attitudes Toward Paying Taxes? Evidence from Multicultural European Countries*. *Social Science Quarterly* (Wiley-Blackwell), v. 88, n. 2, p. 443–470, 2007. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=24814337&lang=pt-br&site=ehost-live> p. 448

25 ALM, J.; TORGLER, B. *Do Ethics Matter? Tax Compliance and Morality*. *Journal of Business Ethics*, v. 101, n. 4, p. 635–651, 2011. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=63166415&lang=pt-br&site=ehost-live> p. 657.

26 Cf. ALM, J.; TORGLER, B. Op.cit. “Another theory is broadly related to Kant’s definition of morality (Laffont,1975; Sugden,1984),and is based on the assumption that a “fair” tax is atax that a taxpayer believes to be fair for all other taxpayers to pay.”p.638

dados, documentos, informações²⁷. Um ecossistema de compliance tributário que esteja aderido à era digital poderá encontrar na blockchain uma ferramenta estratégica que também atua na rapidez de processamento de obrigações fiscais, dá transparência aos atos, permite prevenção majorada e melhor espaço para detecção de fraudes e irregularidades. Em razão de sua característica de imutabilidade, impossibilita manobras maliciosas e oportunistas por parte de agentes corporativos. Até mesmo indicadores de performance ganham potencial de otimização com blockchain.²⁸ Seu uso criaria um ambiente de confiança e um ecossistema de cooperação público-privada, pois o Estado fiscal²⁹ consegue receber informações com maior acurácia e precisão, gerando inovação, redução de custos³⁰ e menor exposição a desvios³¹.

Por conseguinte, todos os fatores de influência para conformidade tributária mencionados nas linhas anteriores deste tópico podem ser fomentados por um constructo tecnológico e propulsor de compliance, o que contribuiria para conferir transparência, simplificação, mitigação de riscos e reforço ético, refletindo na própria resposta do Estado, criando uma metarregulação que favorece uma relação mais salutar entre o Fisco e o contribuinte. Não obstante, questões de falta de escalabilidade, alto custo de aquisição e implementação, bem como os aspectos controversos da imutabilidade, são algumas das deficiências que necessitam ser supridas antes que a blockchain se confirme

27 PRICEWATERHOUSECOOPERS; MICROSOFT CORPORATION. Blockchain for Tax Compliance. 2019 . <https://www.pwc.nl/nl/tax/assets/documents/pwc-blockchain-for-tax-compliance.pdf> p21.

28 Ibidem. p. 33

29 (...) blockchain technology itself may offer a new enforcement instrument for tax authorities. Because a blockchain ledger is virtually impossible to manipulate, tax administrators can build blockchain-based applications to perform tax-enforcement functions. (...)In addition, blockchain can also be used to codify consideration for profit allocation between related companies, thus streamlining compliance with intercompany pricing rules ALM, James et. Al., Op. cit. P..345

30 NAIR, Malavika; SUTTER, Daniel. "The Blockchain and Increasing Cooperative Efficacy." The Independent Review, vol. 22, no. 4, Independent Institute, 2018, pp. 529–50, <http://www.jstor.org/stable/26591760>. p.532

31 Ibidem. p. 541

como ferramenta propulsora de compliance. Ademais, tal como verificado em relação a outras tecnologias inovadoras, o Direito deverá acelerar e acertar o passo normativo para garantir redução de abusos, usos inadequados e enviesados, dentre tantas outras possibilidades negativas quando uma conduta se encontra carente de regulação específica.³²

Considerações Finais

A difusão de atividades públicas e privadas com fronteiras diluídas pelo fenômeno da globalização, economia digital e falta de regulação específica sobre diversas matérias, dá azo a condutas oportunistas, justificando o papel do instituto de compliance como identificador de desvios comuns à pessoa humana como vantagens diretas ou indiretas, e aumento de poder e controle.³³ Com compliance efetivo, a cultura ética organizacional dirige educação, controle e monitoramento. Com isso, novas ferramentas como blockchain podem ajudar na criação de novos filtros decisórios nas empresas e que inibam condutas fraudulentas, engajando as empresas e tornando-as mais aderentes às demandas

32 En matière de politiques publiques, l'intérêt de ce sujet est de questionner la réglementation de l'utilisation de la blockchain. Dans un monde globalisé, les lois nationales se font concurrence et, dans un monde virtuel, l'absence de réglementation peut entraver le développement de la blockchain (cas du Libra/Diem de Facebook). La création de nouvelles normes internationales sur la blockchain apparaît donc comme une question cruciale.. ALFIERI, E.; BURLACU, R.; ENJOLRAS, G. La Blockchain, un outil innovant au service du financement des entreprises. *Recherches en Sciences de Gestion*, [s. l.], n. 143, p. 115–141, 2021. DOI 10.3917/resg.143.0115. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=151996949&lang=pt-br&site=ehost-live>. P. 137

33 TORRES, Carlos Alexandre Dias; SANTORSULA, Christiane Bedini. A evasão fiscal como abuso do poder econômico. Enquadramento, competência do CADE e perspectivas em competition policy. IN: BAGNOLI, Vicente (Org.). *Teoria Jurídica do Mercado: uma homenagem ao Prof. Fabiano Del Masso*. São Paulo: Scortecci, 2021 p. 82

contemporâneas.³⁴

O percurso é longo, mas os potenciais resultados mostram-se promissores. A despeito das limitações da blockchain, com o crescimento exponencial de desenvolvimento tecnológico vivenciando atualmente, estima-se que haverá melhorias importantes e catalizadoras de aplicação em futuro próximo. Justamente por isso, iniciativas legislativas ainda incipientes deverão preencher as lacunas necessárias a permitir que tecnologias como a blockchain operem em prol de mais conformidade tributária, integridade e desenvolvimento social e econômico.

Referências bibliográficas

ALFIERI, E.; BURLACU, R.; ENJOLRAS, G. La Blockchain, un outil innovant au service du financement des entreprises. *Recherches en Sciences de Gestion*, [s. l.], n. 143, p. 115–141, 2021. DOI 10.3917/resg.143.0115. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=151996949&lang=pt-br&site=ehost-live>. P. 137

ALM, J.; TORGLER, B. Do Ethics Matter? Tax Compliance and Morality. *Journal of Business Ethics*, v. 101, n. 4, p. 635–651, 2011. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=63166415&lang=pt-br&site=ehost-live>

ALM, James et. Al., New Technologies and the Evolution of Tax Compliance (May 18, 2020). *Virginia Tax Review*, Vol. 39, No.3, Spring 2020, UC Irvine School of Law Research Paper No. 2020-42, Available at SSRN: <https://ssrn.com/abstract=3604507> pp. 294 e ss

ALM, James et. Al., New Technologies and the Evolution of Tax Compliance (May 18, 2020). *Virginia Tax Review*, Vol. 39, No.3,

34 SAAVEDRA, Giovanni A.; SANTORSULA, Christiane Bedini; VALENTIM, Raphael M. Responsabilidade Social Corporativa (RSC) integrada ao sistema de gestão das empresas: mecanismo de proteção de valor corporativo. IN: SAAVEDRA, Giovanni A.(org). *Governança Corporativa, Compliance e Proteção de Dados*. São Paulo : Eseni, 2019p. 13

Spring 2020, UC Irvine School of Law Research Paper No. 2020-42, Available at SSRN: <https://ssrn.com/abstract=3604507p.345>

BRASIL. Lei n.º 9.430/96, de 27 de dezembro de 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/19430.htm>. Acesso em 23 de abril de 2020.

BUFFON, Marciano. Tributação e Dignidade Humana: Entre os Direitos e Deveres Fundamentais. Livraria do Advogado. Porto Alegre, 2009. p. 91.

COMISSÃO EUROPEIA. European Innovation Council awards 5 million to blockchain solution on social innovations. Disponível em : <https://digital-strategy.ec.europa.eu/en/news/commissions-european-innovation-council-awards-eu5-million-blockchain-solutions-social-innovations>

DINIZ, Eduardo Saad. Ética negocial e compliance entre a educação executiva e interpretação judicial. São Paulo: RT, 2019

GOMEZ-TRUJILLO Ana Maria, OCAMPO, Juan Velez-, GONZALEZ-PEREZ, Maria Alejandra, Trust, Transparency, and Technology: Blockchain and Its Relevance in the Context of the 2030 Agenda, The Palgrave Handbook of Corporate Sustainability in the Digital Era, 10.1007/978-3-030-42412-1, (561-580), (2021). s is of central importance. P.o de Sroblem. a; tax morale. I, Vicente (Org.). Teoria JUrídica ect privacye encontra carente de

GRIFFITH, Sean J. Corporate governance in a era of compliance. William & Mary Law Review, v. 57, n. 6, 2016, p. 2.081. Disponível em: <https://core.ac.uk/downloads/pdf/73973569.pdf>. Acesso em: 31 jan. 2020.

HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital, desafios para o Direito.Rio de Janeiro: Forense 2021. p.16 e 17

HOLMES, Stephen; SUSTEIN, Cass R.. O custos dos direitos.: porque a liberdade depende dos impostos. Livro eletrônico. São Paulo : Martins Fontes, 2019.

LIANG, T.-P. et al. What Drives the Adoption of the Blockchain Technology? A Fit-Viability Perspective. *Journal of Management Information Systems*, [s. l.], v. 38, n. 2, p. 314–337, 2021. DOI 10.1080/07421222.2021.1912915. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=151799337&lang=pt-br&site=ehost-live>.

LIN MEI TAN; BRAITHWAITE, V. Motivations for tax compliance: the case of small business taxpayers in New Zealand. *Australian Tax Forum*, v. 33, n. 2, p. 221–247, 2018. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=130659943&lang=ptbr&site=ehost-live> p. 227

LUTTMER, Erzo. F. P.; SINGHAL, Monica. Tax Morale. *Journal of Economic Perspectives*, [s. l.], v. 28, n. 4, p. 149–168, 2014. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=99368578&lang=pt-br&site=ehost-live> p. 150.

NABAIS, José Casalta. *O Dever Fundamental de Pagar Impostos*. Livraria Almedina. Coimbra. 1998

NAIR, Malavika; SUTTER, Daniel. “The Blockchain and Increasing Cooperative Efficacy.” *The Independent Review*, vol. 22, no. 4, Independent Institute, 2018, pp. 529–50, <http://www.jstor.org/stable/26591760>

OCDE Tax Compliance by design: achieving improved SME tax compliance by adopting a system perspective. OCDE Publishing, 2014. Disponível em : https://read.oecd-ilibrary.org/taxation/tax-compliance-by-design_9789264223219-en#page1

PRICEWATERHOUSECOOPERS; MICROSOFT CORPORATION. *Blockchain for Tax Compliance*. 2019 . <https://www.pwc.nl/nl/tax/assets/documents/pwc-blockchain-for-tax-compliance.pdf> p21.

RAMOS, Francisco de Souza. *A Economia da Sonegação: Teorias e Evidências Empíricas*. *Revista de Economia Contemporânea*, v.9, n.3. 2005. p. 577.

SAAVEDRA, Giovani A.; SANTORSULA, Christiane Bedini; VALENTIM, Raphael M. *Responsabilidade Social Corporativa*

(RSC) integrada ao sistema de gestão das empresas: mecanismo de proteção de valor corporativo. IN: SAAVEDRA, Giovani A.(org). Governança Corporativa, Compliance e Proteção de Dados. São Paulo : Eseni, 2019

SINPROFAZ. Disponível em: <<http://www.quantocustaobrasil.com.br/>>.

TAX JUSTICE NETWORK The Price of Offshore Revisited Tax Justice Network. Londres. 2012. Disponível em: <https://www.taxjustice.net/2014/01/17/price-offshorerevisited/#:~:text=MAIN%20REPORT%201%20%E2%80%93%20The%20Price,zero%20tax%20and%20subst,antial%20secrecy>.

TAX JUSTICE NETWORK. The cost of tax abuse: a briefing paper on the cost of tax evasion worldwide Disponível em: <http://www.taxjustice.net/wp-content/uploads/2014/04/Cost-of-Tax-Abuse-TJN>

TISCINI, R. et al. The blockchain as a sustainable business model innovation. Management Decision, London, v. 58, n. 8, p. 1621-1642, 2020

TORGLER, Benno.; SCHNEIDER, F. What Shapes Attitudes Toward Paying Taxes? Evidence from Multicultural European Countries. Social Science Quarterly (Wiley-Blackwell), v. 88, n. 2, p. 443–470, 2007. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=24814337&lang=pt-br&site=ehost-live> p. 448

TORRES, Carlos Alexandre Dias; SANTORSULA, Christiane Bedini. A evasão fiscal como abuso do poder econômico. Enquadramento, competência do CADE e perspectivas em competition policy. IN: BAGNOLI, Vicente (Org.). Teoria Jurídica do Mercado: uma homenagem ao Prof. Fabiano Del Masso. São Paulo: Scortecci, 2021 p. 82

TORRES, Heleno Taveira. Direito Tributário e Direito Privado: Autonomia Privada: Simulação: Elusão Tributária. São Paulo: Revista dos Tribunais. 2003. p. 188.

TORRES, Heleno Taveira. Limites do Planejamento Tributário e a Norma Brasileira Antissimulação (LC 104/01). In: ROCHA, Valdir de Oliveira (coord.) Grandes Questões Atuais do Direito Tributário. vol. 5. São Paulo: Dialética. 2001. p. 103.

VASQUEZ, Geraldo. An Introduction to Blockchain. CPA Journal, [s. l.], p. 52–55, 2021. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=151374392&lang=pt-br&site=ehost-live>

Os efeitos da pandemia de Covid-19 sobre a regulação do comércio internacional como estabelecida pela OMC

The effects of the covid-19 pandemic on the regulation of international trade as established by the WTO

Hérica Cristina Paes Nascimento¹

Maique Barbosa de Souza²

Sumário: 1. Diretrizes de trabalho da OMC. 1.1 Organização Mundial do Comércio. 1.2. Regulação do Comércio pela Organização Mundial do Comércio. 2. Pandemia de COVID-19 e regulação do Comércio Internacional. 2.1. Pandemia de COVID-19 e consequências econômicas. 2.2. Tratamento de produtos médicos no contexto do combate ao COVID-19. 3. Considerações Finais.

Resumo: O comércio internacional remonta aos primórdios em que as grandes civilizações se utilizavam de seu poderio bélico para garantir a manutenção de rotas de comércio a outros povos, de modo a se conectar e comercializar seus produtos, fazendo crescer essa modalidade de troca de que foi se fortalecendo ao longo dos séculos até se tornar o que presenciamos nos dias atuais. Com isso, os países passaram a perceber que negociar para estabelecer política externa de comércio era mais do que necessário para a subsistência de sua nação, uma vez que nenhum país sozinho é capaz de produzir tudo o que necessita e nem é capaz de consumir tudo o que produz. Arelada a uma política interna e externa a regulação do comércio mundial é uma crescente que tem se mostrado ainda

1 Mestranda em Direito da Empresa e dos Negócios na Universidade do Vale do Rio dos Sinos - UNISINOS. Possui Pós-graduação “Lato Sensu” em Direito e Justiça do Trabalho pela Faculdade Sul-Americana - FASAM (2016). Graduada em Direito pela Instituto de Ensino Superior de Rio Verde (2012). Atualmente é Procuradora Jurídica da Universidade de Rio Verde - UniRV. Advogada. hericacpnascimento@gmail.com. ORCID: <https://orcid.org/0000-0001-8890-9064>.

2 Mestrando no mestrado profissional em Direito da Empresa e Negócios pela Universidade do Vale do Rio dos Sinos - UNISINOS (2019-2021). Especialista em Direito e Processo do Trabalho com capacitação para o Ensino no Magistério Superior pela Faculdade Damásio (2018). Graduado em Direito pela Universidade La Salle - Canoas (2009). Sócio e Gestor de escritório de advocacia com Matriz em Porto Alegre/RS e filial na cidade de Caxias do Sul/RS. Advogado atuante nas áreas do Direito Tributário, Direito do Trabalho, Direito Civil, do Consumidor e na área planejamento sucessório. Email: maique27@hotmail.com.

mais necessária e resolutiva em tempos de pandemia como o que se presencia. É quase automática a decisão tendente ao protecionismo quando se está diante de uma situação nunca antes vivida, ao menos na proporção e velocidade como tem sido a crise de saúde causada pelo COVID-19. Contudo, tal medida não se mostra adequada, não mais em tempos tão interconectados como o do presente século, onde as cadeias globais de valor precisam ser mantidas a fim de permanecer a pulsação vital do comércio nacional, que também depende do comércio internacional. A proposta do presente trabalho é responder à pergunta: de que forma a regulação da OMC tem sido afetada pela pandemia do COVID-19? Com isso faz-se uma análise acerca da criação da OMC e sua regulação no capítulo 2, passando para uma análise mais específica da regulação de produtos e serviços afetados pela pandemia no capítulo 3, seguindo para uma conclusão acerca do cenário econômico vivenciado e sua projeção para o futuro próximo, ao menos naquilo recomendado pela OMC para manutenção do comércio internacional com a liberação de produtos mais flexibilizada frente à crise humanitária que ainda não finalizou.

Palavras-chave: OMC; Comércio Internacional; Pandemia de COVID-19; Impactos Regulatórios.

Abstract: International trade dates back to the beginnings when the great civilizations used their military power to ensure the maintenance of trade routes to other peoples, in order to connect and market their products, making this exchange modality grow, which has been strengthened over the centuries until it became what we see today. With this, countries came to realize that negotiating to establish foreign trade policy was more than necessary for their nation's subsistence, since no single country is capable of producing everything it needs and is not even capable of consuming everything that produces. Linked to an internal and external policy, the regulation of world trade is a growing process that has proved to be even more necessary and decisive in times of pandemic like the one we are witnessing. The decision towards protectionism is almost automatic when faced with a situation never experienced before, at least in the proportion and speed as the health crisis caused by COVID-19 has been. However, such a measure is not adequate, not anymore in times as interconnected as that of the present century, where global value chains need to be maintained in order to remain the vital heartbeat of national trade, which also depends on international trade. The purpose of this paper is to answer the question: how has the regulation of the WTO been affected by the COVID-19 pandemic? With this, an analysis is made about the creation of the WTO and its regulation in chapter 2, moving on to a more specific analysis of the regulation of products and services affected by the pandemic in chapter 3, following to a conclusion about the economic scenario experienced and its projection for the near future, at least in what is

recommended by the WTO to maintain international trade with the release of products more flexible in the face of the humanitarian crisis that has not yet ended.

Keywords: WTO; International Trade; COVID-19 pandemic; Regulatory Impacts.

1 Diretrizes ee Trabalho da OMC

1.1 Organização Mundial do Comércio

O comércio internacional encontra suporte histórico desde o século III a. C., quando a política externa da China fora adaptada, inclusive com o uso de poderio militar, para promover interesses comerciais relacionados à manutenção da Rota da Seda, durante a Dinastia Han. Desde então as sociedades tradicionais e de importância no comércio entre países desenvolveram políticas que sustentaram e permitiram que o comércio internacional fluísse, considerando que através dele é possível promover o crescimento das democracias, levando a perspectivas aprimoradas de se alcançar a paz mundial.³

Apesar disso as nações travaram batalhas épicas que ficaram marcadas na história como a Primeira e a Segunda grandes Guerras Mundiais. Assim, diante da devastação da economia internacional provocada pela Segunda Guerra Mundial os países atores do comércio internacional idealizaram a instituição de organizações que fossem capazes de estruturar novamente a economia global.

Dessa forma, com o fim da guerra, as reuniões da Conferência de Bretton Woods, em 1944, ensejaram a criação do Fundo Monetário Internacional (FMI), do Banco Mundial (antes criado como BIRD, Banco Internacional para a Reconstrução e Desenvolvimento) e a Organização Internacional do Comércio (OIC), sendo que no lugar desta última restou criado o GATT (General Agreement on Trade and Tariffs, Acordo Geral sobre Comércio e Tarifas), um

3 OMC: Organização Mundial do Comércio. DDG Wolff: Trade and foreign policy have always been intertwined, 2018. Disponível em: https://www.wto.org/english/news_e/news18_e/ddgra_09feb18_e.htm#fntext-1. Acesso em 24 jul. 2021.

sistema permanente de negociações comerciais e importante ator no estabelecimento de um sistema comercial multilateral forte e próspero que se tornou cada vez mais liberal através de rodadas de negociações comerciais⁴ que fomentaram um ambiente propício para a criação de blocos econômicos entre os países que optavam por negociar de forma isolada e com parceiros escolhidos previamente. Tal situação ensejou uma revisão completa do GATT, cuja modificação levou à Rodada do Uruguai que criou a Organização Mundial do Comércio (OMC).⁵

A OMC, em funcionamento desde 1 de janeiro de 1995, passou a negociar áreas comerciais que não faziam parte do GATT, além de incluir novos temas nas negociações, se tornando um órgão mundial multipartidário. Seu objetivo passou a ser o de promover o desenvolvimento sustentável no âmbito do comércio internacional, além de apoiar países em vias de desenvolvimento, ao mesmo tempo em que trabalha para construir um quadro institucional comum tão necessário para a condução das relações comerciais entre os seus países-membros.

Dentre suas funções principais está a de promover facilidades que tornem aplicáveis as “as normas do comércio internacional já acordadas internacionalmente, além de servir também como foro para negociações de novas regras, dotada também de um sistema de controvérsias em comércio internacional”.⁶

Este tratado surgiu e estabeleceu um conjunto de normas e concessões tarifárias, tendo o objetivo de impulsionar a liberalização multilateral do comércio, que consiste na negociação dos mais diversos temas, que variam desde o comércio internacional até

4 OMC: Organização Mundial do Comércio. The GATT years: from Havana to Marrakesh. Disponível em: https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact4_e.htmhttps://www.wto.org/english/thewto_e/whatis_e/tif_e/fact4_e.htm. Acesso em 23 jul. 2021.

5 MINEIRO, A. S. As discussões para a reforma da OMC: uma nova agenda ou mais do mesmo? REPRIB, 2021. Disponível em: <http://www.rebrip.org.br/publicacoes/as-discussoes-para-a-reforma-da-omc-uma-nova-agenda-ou-mais-do-mesmo-71d3/>. Acesso em 24 jul. 2021.

6 ULTEMAR DA SILVA, José. Gestão das relações econômicas internacionais e comércio exterior. São Paulo: Cengage Learning, 2008. p. 163.

a segurança coletiva, com a participação efetiva de três ou mais países e combater as práticas protecionistas, que vinham sendo adotadas pelos países desde a década de 1920.⁷

Nesse sentido, as normas acordadas entre os países integrantes do GATT se restringiam apenas ao intercâmbio de mercadorias, enquanto as normas da OMC trazem um escopo bem mais amplo que engloba serviços e também direitos de propriedade intelectual, tudo com vistas a instaurar um comércio internacional com regras mais claras que garantam uma melhor competição entre produtores estrangeiros. Essas regras devem ser orientadas por dois grandes princípios norteadores das negociações, o da não-discriminação e o da reciprocidade. O primeiro garante que haja o livre comércio com a concessão de tratamento favorável a um determinado produto ou serviço a ambos os atores do comércio internacional, não a apenas um, caso exista, bem como ao tratamento igualitário daquele produto ou serviço no âmbito nacional, sem qualquer tratamento desfavorável. Já o segundo estabelece a observância de contrapartidas por parte de cada país negociador que está disposto a oferecer algo que favoreça o comércio do qual faz parte. “A adoção deste princípio complementa a cláusula da nação mais favorecida, uma vez que impede a adoção de medidas protecionistas particulares e inerentes a um grupo restrito de países.”⁸

1.2 Regulação do Comércio pela Organização Mundial do Comércio

A OMC se consolidou como uma organização internacional global responsável pelas regras de comércio entre as nações. Dentre as discussões realizadas em seu âmbito estão as negociações

7 ULTEMAR DA SILVA, José. Gestão das relações econômicas internacionais e comércio exterior. São Paulo: Cengage Learning, 2008. p. 163.

8 ULTEMAR DA SILVA, José. Gestão das relações econômicas internacionais e comércio exterior. São Paulo: Cengage Learning, 2008. p. 164.

internacionais relacionadas a diversos temas, cujo objetivo é o de ajudar produtores de bens e serviços, bem como, exportadores e importadores a conduzir melhor os seus negócios. Voltada para a abertura comercial, o fórum recebe governos para negociarem seus acordos internacionais e resolverem disputas comerciais que enfrentam uns com os outros. Além disso, a OMC é dirigida por seus governos membros, cujas decisões principais são tomadas pela adesão como um todo, seja na pessoa de seus ministros ou na pessoa de seus embaixadores ou delegados, reunindo-se regularmente em Genebra, na Suíça, onde se localiza a sua sede física.⁹

Pela análise dos relatórios das negociações e discussões dos Estados membros dos anos de 2017¹⁰, 2018¹¹, 2019¹², 2020¹³ e 2021¹⁴ é possível ter uma noção dos diversos itens negociados no âmbito da Organização Internacional do Comércio, não havendo modificações negativas em razão da pandemia do COVID-19, que ensejou, na verdade, por mais negociações que fossem capazes de melhor regular as novas demandas por produtos médicos, remédios, insumos para produção de vacinas, equipamentos de proteção individual, dentre outros, tudo com vistas a manter o fluxo do comércio, respeitando a proteção à saúde das nações dos membros da OMC, sem contudo, focar apenas no protecionismo

9 OMC: Organização Mundial do Comércio. What is the WTO? Disponível em: https://www.wto.org/english/thewto_e/whatis_e/whatis_e.htm. Acesso em: 24 jul. 2021.

10 OMC: Organização Mundial do Comércio. WTO Annual Report 2017. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep17_e.htm. Acesso em 24 jul. 2021.

11 OMC: Organização Mundial do Comércio. WTO Annual Report 2018. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep18_e.htm. Acesso em 24 jul.

12 OMC: Organização Mundial do Comércio. WTO Annual Report 2019. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep19_e.htm. Acesso em 24 jul. 2021.

13 OMC: Organização Mundial do Comércio. WTO Annual Report 2020. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep20_e.htm. Acesso em 24 jul. 2021.

14 OMC: Organização Mundial do Comércio. WTO Annual Report 2021. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep21_e.htm. Acesso em 24 jul. 2021.

sem abertura comercial.

Relatórios Anuais da OMC 1

Pelo quadro acima é possível notar um fluxo intensificado nas discussões que modificaram o padrão de negociação da OMC para o ajuste exigido na contenção da pandemia, uma vez que a sua permanência no tempo também pode trazer consequências negativas e talvez até irreversíveis a longo prazo.

2. Pandemia de Covid-19 e regulação do comércio internacional

2.1 Pandemia de COVID-19 e consequências econômicas

A OMC publica anualmente relatório que fornecem uma visão geral e abrangente de suas atividades ao longo de cada ano que se passou, bem como informações aprofundadas das principais áreas de atuação da organização.¹⁵

Em seu último relatório a OMC destaca questões relativas ao processo de seleção de seu Diretor-Geral, questões relacionadas à pandemia do COVID-19 e o comércio mundial.¹⁶

Em parte do respectivo relatório a OMC aponta a criação e adoção de 335 medidas relacionadas à restrição do comércio internacional em razão do COVID-19, todas implementadas no ano de 2020, ao menos nos estágios iniciais da pandemia, situação que fora considerada até mesmo benéfica, considerando que 195 medidas (que correspondem a 58% do seu total) se encaixavam como facilitadoras do comércio, ao passo que 140 delas (correspondentes a 42% do seu total) poderiam ser consideradas

15 OMC: Organização Mundial do Comércio. WTO Annual Report. Disponível em: https://www.wto.org/english/res_e/reser_e/annual_report_e.htm. Acesso em 24 jul. 2021.

16 OMC: Organização Mundial do Comércio. WTO Annual Report 2021. Disponível em: https://www.wto.org/english/res_e/booksp_e/anrep_e/anrep21_e.pdf. Acesso em 24 jul. 2021.

restritivas ao comércio mundial.¹⁷

Inúmeras medidas foram tomadas pelos países para conter a disseminação da doença e em razão disso paralisaram grande parte da economia mundial de um lado, com o aumento da demanda por produtos médicos capazes de combater a pandemia de outro, cuja marca é sem precedentes. Nesse contexto 80 países e territórios alfandegários distintos introduziram restrições ou proibições de exportação como resultado da pandemia, dentre os quais 46 membros da OMC (72 se os estados membros da União Europeia forem contados individualmente), de um total de 164 membros¹⁸, com a promessa de que as medidas seriam temporárias.¹⁹

Os produtos abrangidos por tais proibições e restrições à exportação variaram entre suprimentos médicos, produtos farmacêuticos e equipamentos médicos, em sua maioria, até ao controle de produtos adicionais como alimentos e produtos de higiene pessoal.

Com isso percebeu-se, no início, um fechamento do comércio internacional para contenção da propagação do vírus entre os países, que aplicaram restrições e proibições aos produtos e serviços objetos das negociações mundiais, dada a insegurança provocada pela pandemia.

Ocorre que dentre os acordos firmados pelos países para criação do GATT, transformado na OMC anos mais tarde, está a proibição ampla de restringir ou mesmo proibir exportações pelos países signatários (Artigo XI do GATT²⁰), a não ser em situações

17 OMC: Organização Mundial do Comércio. COVID-19 and world trade. Disponível em: https://www.wto.org/english/res_e/booksp_e/anrep_e/anrep21_spotlight_covid_e.pdf. Acesso em 24 jul. 2021.

18 OMC: Organização Mundial do Comércio. Members and observers. Disponível em: https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm. Acesso em 24 jul. 2021.

19 OMC: Organização Mundial do Comércio. Export prohibitions and restrictions. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/export_prohibitions_report_e.pdf. Acesso em 24 jul. 2021.

20 OMC: Organização Mundial do Comércio. Article XI: general elimination of quantitative restrictions. Disponível em: https://www.wto.org/english/res_e/publications_e/ai17_e/gatt1994_art11_gatt47.pdf. Acesso em 20 jul. 2021.

temporárias que justifiquem a prevenção da escassez crítica de alimentos ou outros produtos essenciais.

A preocupação da organização é a de que tantas restrições e proibições aplicadas por grandes exportadores reduzam, no curto prazo, os preços internos das mercadorias objeto das restrições, posto que aumenta a disponibilidade interna, reduzindo a oferta mundial desses produtos principalmente para países que não os produzem, mas dependem da importação para sua manutenção. Tal situação também gera consequências a longo prazo, uma vez que com os preços internos reduzidos o incentivo para produção de tais produtos também começa a diminuir. Disso conclui-se que nos países onde exista a necessidade de tais mercadorias o contrabando passa a ser incentivado, ao passo que a saída dos produtos de um país, agora com baixa produção, passa a gerar escassez interna, prejudicando assim ambos os atores do comércio internacional, importadores e exportadores de um modo geral, desencadeado um choque de oferta.²¹

Assim, a OMC tem se pautado pela manutenção das negociações comerciais a fim de evitar um colapso da economia mundial, a curto e longo prazo, apesar da pandemia ainda não ter acabado, pois, o retorno rápido da comércio internacional depende do fim da crise de saúde instalada.

No último relatório anual emitido em 31 de março de 2021²² a OMC apontou que a desaceleração do comércio mundial de mercadorias marcou em 5,3%, número até menor do que o que projetado para o período, de 9,2 na previsão revisada da OMC em outubro de 2020. A organização credita esse resultado otimista à ação rápida de muitos governos em fornecer apoio fiscal e monetário para ajudar a mitigar alguns efeitos econômicos negativos

21 OMC: Organização Mundial do Comércio. Export prohibitions and restrictions. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/export_prohibitions_report_e.pdf. Acesso em 24 jul. 2021.

22 OMC: Organização Mundial do Comércio. WTO Annual Report 2021. Disponível em: https://www.wto.org/english/res_e/booksp_e/anrep_e/anrep21_e.pdf. Acesso em 24 jul. 2021.

da pandemia ajudando a limitar a queda da demanda global com a formalização de flexibilizações no comércio de produtos relacionados ao combate da pandemia. Somado a isso, conta-se também com a abstenção dos membros da OMC em grande parte de políticas protecionistas que teriam estrangulado o comércio caso fossem mantidas, considerando que medidas restritivas e proibitivas ao comércio internacional foram implementadas por muitos países no início da crise do COVID-19 como resposta ao atendimento de seu mercado interno e também como forma de conter o avanço de uma doença até então desconhecida. Com o passar das negociações dos países observou-se a reversão das medidas restritivas ao comércio impostas no início, bem como a introdução de novas medidas de liberalização comercial, dentro do contexto da pandemia.²³

Em razão de tal comportamento a OMC estima para 2021 um aumento de 8% no comércio de mercadorias, impulsionado por uma forte recuperação em inúmeras partes do mundo. Essa situação, no entanto, também é marcada por disparidades regionais de comércio, fraqueza contínua no comércio de serviços, principalmente relacionadas a viagens internacionais, notadamente pelo atraso no calendário de vacinação, particularmente em países pobres. A aceleração no crescimento do comércio está condicionada à produção rápida de vacinas e a sua distribuição para imunização da população, que pode gerar um aumento de 2,5% ao ritmo de expansão comercial, mas também pode reduzir até 2% caso isso não seja observado.²⁴

2.2 Tratamento de produtos médicos no contexto do

23 OMC: Organização Mundial do Comércio. Frequently asked questions: The WTO and COVID-19. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/faqcovid19_e.htm. Acesso em 24 jul. 2021.

24 OMC: Organização Mundial do Comércio. Frequently asked questions: The WTO and COVID-19. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/faqcovid19_e.htm. Acesso em 24 jul. 2021.

combate ao COVID-19

O comércio internacional é importante para todas as economias mundiais, não ficando de fora dele nem mesmo os países mais desenvolvidos, visto que nenhum país é autossuficiente o bastante para não necessitar de importações ou exportações, seja porque necessita atender seu mercado interno naquilo em que não produz, seja porque necessita vender o produto de sua produção, nem sempre absorvido nacionalmente.

Sendo assim, o comércio desempenha um papel importante na garantia da disponibilidade e da acessibilidade de produtos diversos, incluindo insumos médicos, medicamentos vitais e serviços de saúde a qualquer nação, principalmente entre os países mais vulneráveis.

Dentro da OMC as negociações para a circulação de bens e serviços entre os países-membros obedece a esse paradigma e fornece um espaço amplo para que seus membros adotem medidas comerciais consideradas necessárias para proteger a saúde pública e o bem-estar público, ainda que estejam incluídas regras de restrição e proibição de importação e exportação. Contudo, essas medidas devem ser adotadas de modo a não discriminar os membros da organização para que não se construa uma restrição disfarçada ao comércio internacional.²⁵

Com isso a OMC tem sempre pautado pela transparência como alicerce fundamental do compromisso para manter os mercados abertos, contudo ela também pontuou acerca da falta de transparência por partes de seus membros no tocante às medidas internas que eles vinham adotando no início da pandemia, ainda que a em Declaração Ministerial do G20, de 30 de março de 2020, tenha ficado enfatizado que as medidas de emergência destinadas a combater a COVID-19, caso fossem necessárias, deveriam ser direcionadas, proporcionais, transparentes e temporárias, sem a

²⁵ OMC: Organização Mundial do Comércio. Frequently asked questions: The WTO and COVID-19. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/faqcovid19_e.htm. Acesso em 24 jul. 2021.

criação de barreiras desnecessárias ao comércio ou interrupção do fornecimento global. Tal situação ensejou recomendações do Diretor-Geral da OMC, Roberto Azevêdo, a fim de que os países-membros exercessem ao máximo a contenção no uso de restrições à exportação e outras medidas que poderiam interromper as cadeias de abastecimento, com a melhoria significativa da transparência sobre quaisquer novas medidas relacionadas ao comércio introduzidas como resultado da pandemia do COVID-19, principalmente com a notificação da OMC acerca das medidas que seriam adotadas por cada um de seus membros.²⁶

Com isso, no ano de 2020 foram submetidas 171 notificações ou comunicações de 38 membros à OMC relacionadas às modificações dos países em seus padrões de comércio, como simplificação de certificação para garantia da segurança de produtos médicos e flexibilização de regulamentos técnicos para a disponibilização de alimentos, todas amparadas em critérios de urgência e emergência dos Acordos sobre Barreiras Técnicas ao Comércio e sobre a Aplicação de Medidas Sanitárias e Fitossanitárias. Contudo, a organização tem lembrado acerca da necessidade do cumprimento de medidas que evitem barreiras discriminatórias ou desnecessárias ao comércio, garantindo uma base científica para as medidas e consonância com os padrões internacionais.²⁷

Dentre as medidas adotadas pelos países há a isenção de tarifas sobre alguns tipos de EPIs e equipamentos médicos (Brasil: máscaras, respiradores, óculos de proteção, protetores faciais, jalecos descartáveis e demais adereços); permissão de comércio de desinfetantes para mãos sem a observância de todos os requisitos de rotulagem ou embalagem bilíngues (Canadá); suspensão

26 OMC: Organização Mundial do Comércio. Export prohibitions and restrictions. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/export_prohibitions_report_e.pdf. Acesso em 24 jul. 2021.

27 OMC: Organização Mundial do Comércio. Standards, regulations and covid-19 – what actions taken by wto members? Disponível em: https://www.wto.org/english/tratop_e/covid19_e/standards_report_e.pdf. Acesso em 24 jul. 2021.

temporária de requisitos de autorização para medicamentos e desinfetantes (Suíça); adoção de procedimentos excepcionais e temporários que ampliam o acesso ao mercado para EPI e dispositivos médicos sem a devida certificação técnica que ocorria antes da pandemia (Ucrânia); aprovação temporária de registro facilitado para dispositivos médicos e produtos farmacêuticos (Tailândia); aceitação de cópias ou documentos digitalizados no lugar dos originais, com a implementação de assinaturas eletrônicas e criação de sites dedicados à verificação de documentos (União Europeia), todos no contexto do controle e combate da pandemia.²⁸

Dessa forma, as importações de máscaras aumentaram 80,09% em 2020, chegando a US\$ 141,4 bilhões; as importações e exportações de produtos médicos aumentaram 16% em 2020, atingindo US\$ 2.343 bilhões, ao mesmo tempo que o comércio mundial total de mercadorias diminuiu em 7,6% em valor; as restrições à exportação de equipamentos de proteção individual, como luvas e máscaras, drogas e remédios tomados nos estágios iniciais da pandemia foram gradualmente eliminadas; aumento de 49% nas exportações de algumas matérias-primas críticas para a produção de vacinas, chegando a cerca de US\$ 15,5 bilhões; e, muitos países tomaram medidas para isentar as importações de tarifas e para agilizar as alfândegas e outros procedimentos.²⁹

Dentre as medidas facilitadoras do comércio ainda é possível pontuar a redução ou eliminação temporária das tarifas de importação de todos os produtos essenciais, incluindo os alimentícios. Com isso a OMC vem produzindo relatórios de monitoramento do comércio internacional a fim de oferecer mecanismos de políticas comerciais com maior transparência multilateral para seus membros, permitindo um fluxo de comércio

28 OMC: Organização Mundial do Comércio. Standards, regulations and covid-19 – what actions taken by wto members? Disponível em: https://www.wto.org/english/tratop_e/covid19_e/standards_report_e.pdf. Acesso em 24 jul. 2021.

29 OMC: Organização Mundial do Comércio. COVID-19 and world trade. Disponível em: https://www.wto.org/english/res_e/booksp_e/anrep_e/anrep21_spotlight_covid_e.pdf. Acesso em 24 jul. 2021.

mais livre e consistente, apesar da crise causada pelo COVID-19.³⁰

3. CONSIDERAÇÕES FINAIS

A crise causada pela pandemia do COVID-19 revelou que os países tendem a seguir regras próprias de protecionismo de seu mercado interno, notadamente para evitar a propagação da doença e também como forma de preservar a sua economia nacional. Contudo, diante de uma economia global tão entrelaçada e interdependente, esse comportamento não se mostra mais adequado, notadamente diante das lições deixadas pela história recente e remota, bem como, porque tal medida não se mostra capaz de, de fato, proteger a economia de uma nação.

No âmbito da OMC o exemplo que fica claro diante dos dados e resultados diariamente noticiados é o de que a negociação e a abertura comercial, ainda que com certas cautelas, é o meio mais adequado de manter saudável a economia de um país e, conseqüentemente, da economia global.

Em resposta à pergunta feita no início deste trabalho percebe-se uma grande virada diante do protecionismo inicial adotado pelos países-membros da OMC, no início da pandemia, para uma flexibilização e maior abertura ao comércio internacional, em sua maioria de produtos relacionados ao combate do avanço do vírus, chegando até a produtos diversos, como os de ordem alimentícia, dada a sua relevância para a economia de países não tão favorecidos. Com isso, vislumbra-se no início uma reação imediata dos membros da OMC frente à pandemia mas que, depois de analisada, negociada e repensada mostrou-se impertinente para o fluxo do comércio global e até mesmo para o fim acelerado da crise instalada, gerando um ambiente muito fértil para diversas

30 OMC: Organização Mundial do Comércio. How wto members have used trade measures to expedite access to covid-19 critical medical goods and services. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/services_report_16092020_e.pdf. Acesso em 24 jul. 2021.

concessões econômicas e tarifárias com uma única finalidade: o retorno o mais breve possível do fluxo do comércio internacional, com seus membros mais experientes e mais confiantes diante do resultado vivenciado com as práticas regulatórias adotadas neste tempo de pandemia.

Referências Bibliográficas

MINEIRO, A. As discussões para a reforma da OMC: uma nova agenda ou mais do mesmo? REPRIB, 2021. Disponível em: <http://www.rebrip.org.br/publicacoes/as-discussoes-para-a-reforma-da-omc-uma-nova-agenda-ou-mais-do-mesmo-71d3/>. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. Article XI: general elimination of quantitative restrictions. Disponível em: https://www.wto.org/english/res_e/publications_e/ai17_e/gatt1994_art11_gatt47.pdf. Acesso em 20 jul. 2021.

OMC: Organização Mundial do Comércio. COVID-19 and world trade. Disponível em: https://www.wto.org/english/res_e/booksp_e/anrep_e/anrep21_spotlight_covid_e.pdf. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. DDG Wolff: Trade and foreign policy have always been intertwined, 2018. Disponível em: https://www.wto.org/english/news_e/news18_e/ddgra_09feb18_e.htm#fntext-1. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. Export prohibitions and restrictions. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/export_prohibitions_report_e.pdf. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. Frequently asked questions: The WTO and COVID-19. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/faqcovid19_e.htm. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. How wto members have used trade measures to expedite access to covid-19 critical medical goods and services. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/services_report_16092020_e.pdf. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. Members and observers. Disponível em: https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. Standards, regulations and covid-19 – what actions taken by wto members? Disponível em: https://www.wto.org/english/tratop_e/covid19_e/standards_report_e.pdf. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. The GATT years: from Havana to Marrakesh. Disponível em: https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact4_e.htmhttps://www.wto.org/english/thewto_e/whatis_e/tif_e/fact4_e.htm. Acesso em 23 jul. 2021.

OMC: Organização Mundial do Comércio. WTO Annual Report 2017. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep17_e.htm. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. WTO Annual Report 2018. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep18_e.htm. Acesso em 24 jul.

OMC: Organização Mundial do Comércio. WTO Annual Report 2019. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep19_e.htm. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. WTO Annual Report 2020. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep20_e.htm. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. WTO Annual Report 2021. Disponível em: https://www.wto.org/english/res_e/publications_e/anrep21_e.htm. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. WTO Annual Report.

Disponível em: https://www.wto.org/english/res_e/reser_e/annual_report_e.htm. Acesso em 24 jul. 2021.

OMC: Organização Mundial do Comércio. WTO reports on COVID-19 and world trade. Disponível em: https://www.wto.org/english/tratop_e/covid19_e/covid_reports_e.htm. Acesso em 24 jul. 2021.

ULTEMAR DA SILVA, José. Gestão das relações econômicas internacionais e comércio exterior. São Paulo: Cengage Learning, 2008.

A defesa do consumidor frente ao A.ISPLAINING

The consumer law facing the A.ISPLAINING

Karlo Messa Vettorazzi¹

Julia de Mello Bottini²

Sumário: 1. O Mansplaining; 2. O A.Isplaining; Considerações Finais.

Resumo: O presente trabalho visa, por meio de uma pesquisa pautada no método dedutivo e da análise de conteúdo e bibliográfica, apresentar reflexões iniciais sobre o significado do termo A.Isplaining, bem como a sua relação com o Direito do Consumidor. Assim, se caracteriza como um estudo doutrinário, que analisa, em um primeiro momento, a origem do termo A.Isplaining, que deriva diretamente da ideia do Mansplaining, difundido pela socióloga Rebecca Sonit. Diante da percepção de que o termo se associa a uma ideia de poder sobre outrem e da consolidação do que seria o A.Isplaining, parte-se para a análise do termo como fator de desencadeia consequências na seara consumerista. Assim, percebe-se que o mundo atual se baseia em uma dinâmica na qual consumidores se veem vulneráveis aos instrumentos e artifícios da inteligência artificial, que são constantemente utilizados como ferramentas de vendas onlines e que estas consequências são notadas aos poucos, com impactos na vida e no dia a dia frente ao poder de escolha dos consumidores. Após as análises, percebe-se que se vive em um mundo do A.Isplaining, onde as inteligências artificiais conhecem mais os seres humanos do que eles próprios, induzindo escolhas e tornando o ato de consumo um fluxo contínuo, onde não há uma ação pensante, mas sim, uma ação impulsionada por estas mesmas inteligências artificiais.

Palavras-chave: A.Isplaining; Direito do Consumidor; Inteligência Artificial.

Abstract: The present work aims, through a research based on the deductive method and the content and bibliographic analysis, to present initial reflections on the meaning of the term A.Isplaining, as well as its relationship with

1 Doutorando e Mestre em Direito Socioambiental da Pontifícia Universidade Católica do Paraná – PUCPR, Brasil. Professor do Centro Universitário UNISANTACRUZ de Curitiba, Brasil. Advogado. E-mail: karlo.vettorazzi@gmail.com

2 Doutoranda e Mestre em Direito Socioambiental da Pontifícia Universidade Católica do Paraná – PUCPR, Brasil. Professora do Centro Universitário UNIFACEAR de Curitiba, Brasil. Advogada. E-mail: julia.bottini@hotmail.com

Consumer Law. Thus, it is characterized as a doctrinal study, which analyzes, at first, the origin of the term A.Isplaining, which derives directly from the idea of Mansplaining, disseminated by sociologist Rebecca Sonit. In view of the perception that the term is associated with an idea of power over others and the consolidation of what A.Isplaining would be, the analysis of the term as a factor triggering consequences in the consumerist field is part of the analysis. Thus, it is clear that the current world is based on a dynamic in which consumers find themselves vulnerable to the instruments and devices of artificial intelligence, which are constantly used as online sales tools and that these consequences are noticed little by little, with impacts on life and in everyday life in the face of consumers' power of choice. After the analyses, it is clear that we live in a world of A.Isplaining, where artificial intelligences know more about human beings than they do, inducing choices and making the act of consumption a continuous flow, where there is no thinking action, but an action driven by these same artificial intelligences.

Keywords: A.Isplaining; Consumer Law; Artificial Intelligence.

1. O Mansplaining

O fenômeno do mansplaining acontece quando um homem, ao falar com uma mulher, se mostra condescendente ou paternalista. Este fenômeno é um eco da forma comportamental e de pensamento da sociedade tradicional³. Este comportamento está comumente relacionado a um modo machista.⁴

O termo provém do inglês e é composto pelas palavras “man” e “explain”⁵, respectivamente. O mais comum é que se refira à maneira que alguns homens agem diante das mulheres, como se elas não tivessem suficiente capacidade o suficiente para se desenvolver seja em uma conversa ou em uma situação na qual um

3 O QUE é mansplaining? - A mente é maravilhosa. 2018. Elaborada por A Mente é Maravilhosa. Disponível em: <https://amenteemaravilhosa.com.br/mansplaining/>. Acesso em: 04 set. 2021.

4 O QUE é mansplaining? - A mente é maravilhosa. 2018. Elaborada por A Mente é Maravilhosa. Disponível em: <https://amenteemaravilhosa.com.br/mansplaining/>. Acesso em: 04 set. 2021.

5 O QUE é mansplaining? - A mente é maravilhosa. 2018. Elaborada por A Mente é Maravilhosa. Disponível em: <https://amenteemaravilhosa.com.br/mansplaining/>. Acesso em: 04 set. 2021.

homem não estivesse presente. Os casos, de mansplaining podem ser vistos quando um homem fala sobre assuntos tradicionalmente masculinos, tentando, sempre, se mostrar mais entendido e com a intenção de fazer com que a mulher se cale e, apenas, aprenda, do modo que este homem ache mais adequado⁶.

Definitivamente, o mansplaining tem um claro efeito sobre as relações de poder, o que pode supor que a mulher seja anulada em âmbitos tanto pessoais como profissionais. Isso acontece em conversas com colegas, chefes que se consideram mais sábios, experientes e inteligentes⁷.

Segundo Stocker e Dalmaso⁸, o mansplaining refere-se a uma fala didática direcionada à mulher, como se ela não tivesse a capacidade de compreender ou executar determinada tarefa, justamente pelo fato de ser mulher. No mansplaining o homem acredita que tem mais conhecimento de determinado tema do que uma mulher, sendo que muitas vezes está ligado ao maninterrupting, que se caracteriza por interrupções que o homem faz na fala da mulher para mostrar que sabe mais do que ela⁹.

A intenção por detrás do mansplaining é desmerecer o conhecimento que uma mulher tem, desqualificando seus argumentos, contendo falas dirigidas às mulheres que estão relacionadas com “entender/aprender” e explicar/desenhar” são comuns neste tipo de violência. Dessa forma, o mansplaining tira a confiança, a autoridade e o respeito da mulher sobre o que ela está falando e a trata como inferior e como se tivesse menos capacidade

6 O QUE é mansplaining? - A mente é maravilhosa. 2018. Elaborada por A Mente é Maravilhosa. Disponível em: <https://amenteemaravilhosa.com.br/mansplaining/>. Acesso em: 04 set. 2021.

7 O QUE é mansplaining? - A mente é maravilhosa. 2018. Elaborada por A Mente é Maravilhosa. Disponível em: <https://amenteemaravilhosa.com.br/mansplaining/>. Acesso em: 04 set. 2021.

8 STOCKER, Pâmela Caroline; DALMASO, Silvana Copetti. Uma questão de gênero: ofensas de leitores à Dilma Rousseff no Facebook da Folha. Rev. Estud. Fem. [online]. 2016, vol.24, n.3, pp.679-690. Acesso em: 04 set. 2021.

9 STOCKER, Pâmela Caroline; DALMASO, Silvana Copetti. Uma questão de gênero: ofensas de leitores à Dilma Rousseff no Facebook da Folha. Rev. Estud. Fem. [online]. 2016, vol.24, n.3, pp.679-690. Acesso em: 04 set. 2021.

intelectual do que o homem¹⁰.

O termo mansplaining foi criado por Rebecca Solnit em 2008, no livro “Homens explicando coisas para mim”¹¹. Esses comportamentos nem sempre são percebidos pelos homens, devido a sua socialização com essas práticas de discriminações de gênero. Muitas mulheres nem sequer sabem de sua existência, por naturalizarem o fenômeno, como explica STOLCKER e DALMASO, ao analisar o mansplanning¹².

2 O A.Isplaining

A Inteligência Artificial é o conceito macro. Aquele que remonta à conferência da Dartmouth College (USA), em 1956, quando John McCarty, Marvin Minsky e seus colegas inauguraram o debate sobre o tema. Começou a se desenvolver no cenário pós-guerra, uma década depois do lançamento do primeiro computador elétrico de grande escala.

Desde o início, a proposta era estudar e desenvolver o ramo da computação que permitiria a existência de máquinas dotadas de habilidades praticamente humanas, como raciocínio e resolução de problemas. Seis décadas se passaram e há quem defenda que a evolução da Inteligência Artificial se deu a passos curtos e demorados. No entanto, a área originou outras frentes de estudo e aplicações. As mais atuais, o Machine Learning e o Deep Learning, são consideradas minas de ouro para o mercado global.

Quando se em Machine Learning nos referimos ao braço da Inteligência Artificial que se dedica a usar algoritmos para analisar

10 STOCKER, Pâmela Caroline; DALMASO, Silvana Copetti. Uma questão de gênero: ofensas de leitores à Dilma Rousseff no Facebook da Folha. Rev. Estud. Fem. [online]. 2016, vol.24, n.3, pp.679-690. Acesso em: 04 set. 2021.

11 STOCKER, Pâmela Caroline; DALMASO, Silvana Copetti. Uma questão de gênero: ofensas de leitores à Dilma Rousseff no Facebook da Folha. Rev. Estud. Fem. [online]. 2016, vol.24, n.3, pp.679-690. Acesso em: 04 set. 2021.

12 STOCKER, Pâmela Caroline; DALMASO, Silvana Copetti. Uma questão de gênero: ofensas de leitores à Dilma Rousseff no Facebook da Folha. Rev. Estud. Fem. [online]. 2016, vol.24, n.3, pp.679-690. Acesso em: 04 set. 2021.

dados, aprender com eles e fazer previsões sobre uma determinada matéria. Ou seja, no lugar de configurar uma máquina para realizar uma tarefa como se espera, ela é “treinada” para absorver uma grande quantidade de dados e concluir “sozinha” como se comportar diante daquele desafio.

Um dos exemplos mais comuns trata-se do sistema de recomendações de produtos. Nada mais é que o bom e velho “quem comprou isso, comprou também” ou “quem gostou disso, gostou também”. Os algoritmos de recomendação podem indicar opções considerando as escolhas anteriores de consumidores similares ou mesmo fazendo combinações entre o conteúdo do seu perfil público (gênero, idade) e o dos produtos (categoria, marca, preço). O que, antes, era feito manualmente ganha rapidez e assertividade com uma ajudinha da Inteligência Artificial.

Para vender é preciso fazer com que o produto ideal chegue ao consumidor certo, no momento em que ele precisa. A busca é um dos principais aliados para cumprir essa missão, por isso, ela deve ser efetiva. O Machine Learning aplicado a essa ferramenta crítica para o funil de vendas do e-commerce pode otimizar, por exemplo, o sistema de ranking. Assim, coloca os resultados mais relevantes em destaque considerando não só a frequência com que o termo é pesquisado. O algoritmo cruza este elemento com dados do perfil do usuário (visualizações e buscas anteriores, faixa etária). Então, pode oferecer as melhores respostas. É muito mais que uma combinação de palavras, mas uma “indicação” do que o consumidor quer e precisa. O melhor, é que o sistema pode, inclusive, prever o que o comprador deseja ou necessita, antes que ele próprio decida por isso.

Hoje, os robôs estão por toda parte. São eles, muitas vezes, que escolhem os anúncios que você vê na internet. Outros robôs conseguem detectar se você se interessou por algum produto ou alguma viagem e, então, passam a oferecer descontos e promoções. Também existem aqueles que disparam e-mails de acordo com

seu comportamento: se você assinou uma newsletter, colocou um produto no carrinho ou se não usa os serviços da empresa há algum tempo, por exemplo. Todas essas são aplicações da inteligência artificial (AI) na jornada de compra.

Neste sentido, faz-se a relação entre o mansplaining e a atividade da inteligência artificial, através do que chamamos de A.Isplaining.

Com o uso mais assertivo da inteligência artificial adentra-se em uma seara, na qual apenas parecemos totalmente conscientes de nossas escolhas e vontades, o que nos conduz para que surja uma espécie de mansplaining por parte da Inteligência Artificial.

No cenário atual, no qual a máquina acha que sabe - e por vezes de fato sabe - mais sobre um tópico do que o próprio ser humano, quando esta mesma máquina nos mostra as escolhas que devemos fazer, por serem as melhores, por economizarem a nossa energia e por nos pouparem de pensar, temos a possível figura de um A.Isplaining. Ou seja, podemos utilizar este termo quando a máquina demonstra que o seu conhecimento é superior ao do humano, mesmo no que concerne aos seus próprios desejos e vontades íntimas. É a simples junção da palavra Artificial Intelligence (A.I) com explaining (explicar).

O Código de Defesa do Consumidor – CDC brasileiro e suas normas principiológicas regem todas as relações do consumo, uma vez que é um sistema independente estruturado para reger normas de proteção ao consumidor. Diante disso, tem como um de seus princípios basilares a ideia de que há vulnerabilidade por parte consumidor na relação consumerista. Isto pode ser visto logo no artigo 4º, inciso I do CDC e, Segundo Rizzatto Nunes (2009):

A vulnerabilidade é uma fragilidade real sofrida naturalmente pelo consumidor, e concreta em razão de uma diferenciação de ordem técnica e econômica eminentemente fática entre fornecedor e consumidor, havendo inclusive a possibilidade de se falar em

níveis de vulnerabilidade, pois se tem por base o homem médio¹³.

Conforme o CDC a vulnerabilidade das pessoas físicas enquanto consumidores, é presumida, uma vez que não provêm de meios efetivos para produzir provas e estão presos as possibilidades apresentadas pelos produtos fornecidos, sendo a boa-fé e confiança os pilares da relação de consumo na qual estão inseridos. Assim, segundo Cláudia Lima Marques, toda a vulnerabilidade jurídica decorre, portanto, de uma falta de conhecimento, não apenas jurídico, mas técnico, que o consumidor não possui.¹⁴ Portanto, o consumidor além de possuir um déficit informacional, possui um déficit jurídico.¹⁵

Considerando a falta de conhecimento, Paulo Valério, entende que o saber jurídico do consumidor, é um déficit informacional sendo uma vulnerabilidade técnica, e não a jurídica, contrariando o que a professora Cláudia Lima Marques entende quanto ao elemento caracterizador que permitiria, assim, diferenciar os dois institutos.¹⁶

Ressalva-se aqui a diferença entre a vulnerabilidade e a hipossuficiência, também disposta no artigo 6º do Código de Defesa do Consumidor. A hipossuficiência apresenta-se no campo processual, de forma exclusiva, sobre isso, Leciona Flávio Tartuce (2017):

O conceito de hipossuficiência consumerista é amplo, devendo ser apreciado pelo aplicador do direito caso a caso, no sentido de reconhecer a disparidade técnica ou informacional, diante de uma situação de desconhecimento a hipossuficiência.¹⁷

É possível perceber que todo consumidor será considerado

13 RIZZATTO NUNES, Luiz Antônio. Curso de Direito do Consumidor. 4. ed. São Paulo, Saraiva, 2009

14 MARQUES, Cláudia Lima. Comentários ao Código de Defesa do Consumidor. 3.ª Ed. São Paulo: Revista dos Tribunais. 2010.

15 MARQUES, Cláudia Lima. Comentários ao Código de Defesa do Consumidor. 3.ª Ed. São Paulo: Revista dos Tribunais. 2010.

16 MORAES, Paulo Valério Dal Pai. CDC: O princípio da vulnerabilidade no contrato, na publicidade e nas demais práticas comerciais. 6. ed. Porto Alegre. Síntese, 2011.

17 TARTUCE, Flávio. Manual de Direito do Consumidor. 6.ed. São Paulo. Editora: Método.

vulnerável, mas nem todo consumidor será hipossuficiente. O que contribuiu para o surgimento da vulnerabilidade eletrônica foi o grande número de práticas abusivas que ocorrem, de forma constante, no mundo virtual.

Nesse momento, é preciso atentar-se para o fato de que o ser humano abre espaço para uma ascensão da máquina, mas, de forma inconsciente, a inteligência artificial passa ser utilizada no lugar da inteligência humana, sendo este substituído por aquele.

É possível ponderar que ainda não se vive em uma era do A.Isplaining por motivos que permeiam a ética, porém, os fatos nos mostram que estamos cada vez mais próximos desse cenário. É quando a indução passa a ser a única opção e tudo se encontra dentro de padrões pré-estabelecidos no qual sair desta caixa seria por demasiado perigoso.

A inteligência artificial aprende tarefas simples, aprende comportamento dos consumidores, aprende a medida que seu banco de dados informacional aumenta, aprende porque faz ligações lógicas entre comportamento e desejo, entre ações humanas e omissões. A I.A aprende porque observa passos, hábitos, padrões.

Porém, o A.Isplaining só é possível, como já relatado, porque a máquina possui uma gama enorme de informações sobre cada pessoa e lugar, assim, com essas informações torna-se possível mapear padrões de comportamento. Nesta seara é possível perceber que nós, seres humanos, entregamos dados pessoais, como nome, sexo, documentos pessoais, bem como os dados sensíveis, orientação política, sexual e religiosa, que fazem com que as inteligências artificiais aprendam cada dia mais e com um maior poder de precisão.

A maioria desses dados são obtidos graças a aplicativos ou reder sociais, como o Facebook, por exemplo, nós, ao concordamos com as políticas de privacidade permitimos que todas as informações sejam utilizadas. Mas nos é dito para benefício de quem ou do que?

Porém, é certo que há uma tensão entre o direito à privacidade e a necessidade de uso e fluxo de dados, o principal responsável é o avanço exponencial da tecnologia da informação, especialmente em suas formas mais pervasivas.

Considerações Finais

A lei é importante porque estimula que as empresas sejam mais claras em relação ao tratamento de dados, tende a fazer com que termos de uso se tornem mais padronizados, visíveis e fáceis de entender. A intenção é que os usuários fiquem menos sujeitos a venda ou exploração desses dados, o usuário poderá, também, mudar de ideia em relação ao consentimento já cedido e ter seus dados apagados.

O tratamento de bancos de dados virou uma atividade econômica com lucros multimilionários em um terreno até então desregulado. Com a implantação de legislações de proteção de dados, as empresas passam a ter obrigações de proibição de venda ou compartilhamento entre empresas de dados sensíveis, que são os referentes à saúde, religião, política, salvo se o titular queira se valer da portabilidade para transferir suas informações de um serviço para outro. A lei também veta o uso de dados para discriminação ou prática abusiva, reforçando a necessidade de serem respeitados direitos fundamentais.

Essa proteção de dados é um benefício aos usuários nessa era informacional, porém, e as informações já coletadas e, alguns casos, vendidas e vazadas? Dados sensíveis e pessoais não se alteram da noite para o dia, são dados permanentes e é certo que algum estrago já foi feito.

O único jeito de fugir das A.Is seria quebrar os padrões, e fazê-la com que ela não aprenda com o que você faz de forma repetitiva. Fazer o igual até a máquina faz, mas fazer o diferente só o cérebro humano é capaz de fazer. Talvez já se está na era do

A.Isplaining, e de tão induzidos e padronizados ainda não se tenha percebido isso.

Referências Bibliográficas

MARQUES, Cláudia Lima. Comentários ao Código de Defesa do Consumidor. 3.^a Ed. São Paulo: Revista dos Tribunais. 2010.

MORAES, Paulo Valério Dal Pai. CDC: O princípio da vulnerabilidade no contrato, na publicidade e nas demais práticas comerciais. 6. ed. Porto Alegre. Síntese, 2011.

O QUE é mansplaining? - A mente é maravilhosa. 2018. Elaborada por A Mente é Maravilhosa. Disponível em: <https://amenteemaravilhosa.com.br/mansplaining/>. Acesso em: 04 set. 2021.

RIZZATTO NUNES, Luiz Antônio. Curso de Direito do Consumidor. 4. ed. São Paulo, Saraiva, 2009

STOCKER, Pâmela Caroline; DALMASO, Silvana Copetti. Uma questão de gênero: ofensas de leitores à Dilma Rousseff no Facebook da Folha. Rev. Estud. Fem. [online]. 2016, vol.24, n.3, pp.679-690. Acesso em: 04 set. 2021.

TARTUCE, Flávio. Manual de Direito do Consumidor. 6.ed. São Paulo. Editora: Método.

ÉTICA JURÍDICA NA ERA DIGITAL

O livro debate analiticamente os principais assuntos que envolvem os problemas de ordem ética e jurídica relacionados com os mecanismos de Inteligência Artificial (IA), seja nas relações com a atividade humana ou com os sistemas automáticos ou autónomos de IA. Os diversos temas apresentados discorrem sobre os impactos que a IA causa direta ou indiretamente na vida das pessoas ou os riscos de abuso ou violação dos direitos subjetivos.

Como objetivo final, discute-se os limites éticos do progresso económico em consequência da massiva digitalização das operações empresariais e das atividades públicas.



IBEROJUR

P.PORTO
ISCAP

CEOS.PP
CENTRO DE ESTUDOS ORGANIZACIONAIS
E SOCIAIS DO POLITECNICO DO PORTO

FCT Fundação
para a Ciência
e a Tecnologia