Privacy and Data Protection Magazine

REVISTA CIENTÍFICA NA ÁREA JURÍDICA

N.º 06 – DEZEMBRO 2022
REVISTA ONLINE, QUADRIMESTRAL

Direção Executiva
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Privacy and Data Protection Magazine

Data: dezembro 2022

Publicações: 3 números anuais

ESTATUTO EDITORIAL

1.º Objeto. A Revista Privacy and Data Protection Magazine é uma publicação científica que tem por objeto a Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual; Direito do Consumo; Direito da Saúde, Direito Digital e Inteligência Artificial.

2.º Princípios Deontológicos. Tudo o que, nesta Revista, se venha a publicar, obedecerá rigorosamente à metodologia científica do Direito e à sua praxis quotidiana, sem quaisquer ingredientes políticos ou religiosos. Assim, será sempre no respeito dos princípios deontológicos da imprensa periódica e da ética profissional que se pautará a orientação desta Revista.

3.º Propriedade. É proprietária da Revista a ENSILIS – Educação e Formação, Unipessoal Lda, detentora da Universidade Europeia, com sede na Quinta do Bom Nome, Estrada da Correia, n.º 53, 1500-210.

4.º Edição. A edição da Revista está a cargo da Universidade Europeia.

5.º Objetivo. A Revista visa contribuir para a criação e transmissão do conhecimento científico na área da Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual, Direito do Consumo, Direito da Saúde, Direito Digital e Inteligência Artificial.

6.º Direção Executiva e Editorial. A Revista é dirigida por uma diretora: Cristina Maria de Gouveia Caldeira, que é co-coordenadora do Privacy and Data Protection Centre, email: centro.dataprotection@universidadeeuropeia.pt

7.º Colaborações. A Revista publica em acesso aberto artigos doutrinários e outros estudos, legislação e jurisprudência comentadas e recensões de obras científicas.

8.º Conselho Editorial. Após revisão por pares, a seleção dos trabalhos a publicar é feita por um Conselho Editorial integrados por 6 especialistas de reconhecido mérito.

9.º Periodicidade. A Revista terá periodicidade quadrimestral.

10.º Secções. A Revista compreende quatro secções: (i) Artigos Doutrinários; (ii) Outros Estudos; (iii) Legislação e Jurisprudência Comentadas; (iv) Recensões.

11.º Sistema de Publicação. A Revista com publicação online em três línguas (português, inglês e espanhol), pretende ter um alcance nacional e internacional.

Ficha Técnica

Título
Privacy and Data Protection Magazine

Subtítulo
Revista Científica na Área Jurídica

Número
005

Ano de Publicação
2022

Afiliação
Privacy and Data Protection Centre Universidade Europeia

Conselho Editorial
Alexandra Chícharo das Neves
Ana Cristina Roque
Eduardo Vera-Cruz
Ingo Wolfgang Sarlet
Luís Filipe Coelho Antunes
Pedro Barbas Homem

Autores
Allan Carvalho
Cristina Maria de Gouveia Caldeira
Isadora Formenton Vargas
Lisiane Feiten Wingert Ody
Manuel David Masseno
Renato Dolabella Melo

Prefácio
Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez

Direção Executiva
Cristina Maria de Gouveia Caldeira

ISSN
2184-920X

Número de Registo
127600

Propriedade
ENSILIS - Educação e Formação, Unipessoal, Lda., detida a 100% por Omnymission, Unip. Lda.

Chief Executive Officer
Miguel Carmelo

NIPC/NIF
504 669 788

Editor e Redação
Universidade Europeia, Quinta do Bom Nome, Estrada da Correia, 53, 1500-210, Lisboa

Índice

Prefácio

A revista *Privacy and Data Protection Magazine* prossegue o seu compromisso de publicação regular, oferecendo aos investigadores de mérito, especialistas, professores e estudantes, um palco de reflexão sobre temas pertinentes, que vão desde o direito fundamental à proteção de dados ao direito digital, passando pelo ecossistema industrial, saúde e novas tecnologias, abrindo as portas para áreas de grande atualidade como a neurociência, a neurotecnologia e o neurodireito.

Aproximando-se a presente publicação do dia 28 de janeiro de 2023, data em que se celebra o Dia Internacional da Proteção de Dados (celebração que remonta ao ano em que foi assinada a Convenção 108 do Conselho da Europa – 1981, relativa à proteção das pessoas singulares no que diz respeito ao tratamento automatizado de dados pessoais), não poderíamos deixar de sublinhar a sua influência na construção dos princípios que presidiram à Diretiva 95/46/CE, de 24 de outubro, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, bem como, ao instrumento jurídico que a revogou, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD). O referido regulamento entrou plenamente em vigor em 25 de maio de 2018, com o objetivo de responder aos desafios colocados pela revolução tecnológica ocorrida nas últimas décadas, e aumentar a proteção das pessoas singulares, no que diz respeito aos tratamentos de dados pessoais e à livre circulação desses dados.

Em Portugal, o Direito à proteção de dados encontra-se positivado na Constituição da República Portuguesa, e concretiza-se através da Lei n.º 58/2019, de 8 de agosto, diploma que assegura a execução na ordem jurídica nacional do RGPD, garantindo que os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais, são respeitados, independentemente da nacionalidade ou do local de residência.

A emergência do Direito à proteção de dados, que consubstancia mais um reflexo da era digital, encontra-se consagrado num substancial número de instrumentos jurídicos internacionais, europeus e nacionais, de entre os quais se destacam os tratados europeus, sendo igualmente notável o contributo da jurisprudência do Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos do Homem.

O artigo de abertura da presente publicação aborda a proteção dos dados pesoais no contexto das transferências para países terceiros ou organizações internacionais. E, nesse domínio, o aumento dos fluxos transfronteiriços de dados pessoais criou novos desafios e novas preocupações em relação à sua proteção, o que torna exigível que o nível de proteção das pessoas singulares garantido pelo RGPD não seja comprometido, quando os dados pessoais são transferidos para países terceiros, inclusivamente em caso de transferências ulteriores.

Prossegue-se com um estudo comparado entre os Estados Unidos da América e o Brasil, no qual se analisa a robustez do sistema jurídico brasileiro, quer em termos normativos, quer em termos jurisprudenciais, quando se trata da violação do domicílio. A hipótese de partida centra-se na identificação da privacidade como fundamento da inviolabilidade do domicílio, em contextos digitais.

O reconhecimento da insuficiência do apagamento dos dados pelo responsável pelo tratamento, em face das especificidades da *Internet*, levou à consagração do «direito a ser esquecido» no artigo 17.º do RGPD. O direito ao esquecimento é analisado nesta publicação, a partir do Recurso Extraordinário 1.010.606/RJ, cujo objeto de afetação era a "*aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares*". O artigo examina o tema do direito ao esquecimento a partir desse precedente, fazendo-o sob a perspectiva do direito comparado, permitindo-nos concluir que o direito ao esquecimento está estritamente relacionado com o meio digital.

Num contexto em que os sistemas de inteligência artificial são cada vez mais sofisticados, o artigo seguinte procura compreender como o direito brasileiro enquadra os casos de discriminação causados pelo uso de algoritmos enviesados. O texto contém uma análise crítica do sistema regulatório positivo, visando identificar insuficiências normativas, concluindo que «a revisão humana de decisões automatizadas é talvez a melhor ferramenta para prevenir a discriminação algorítmica».

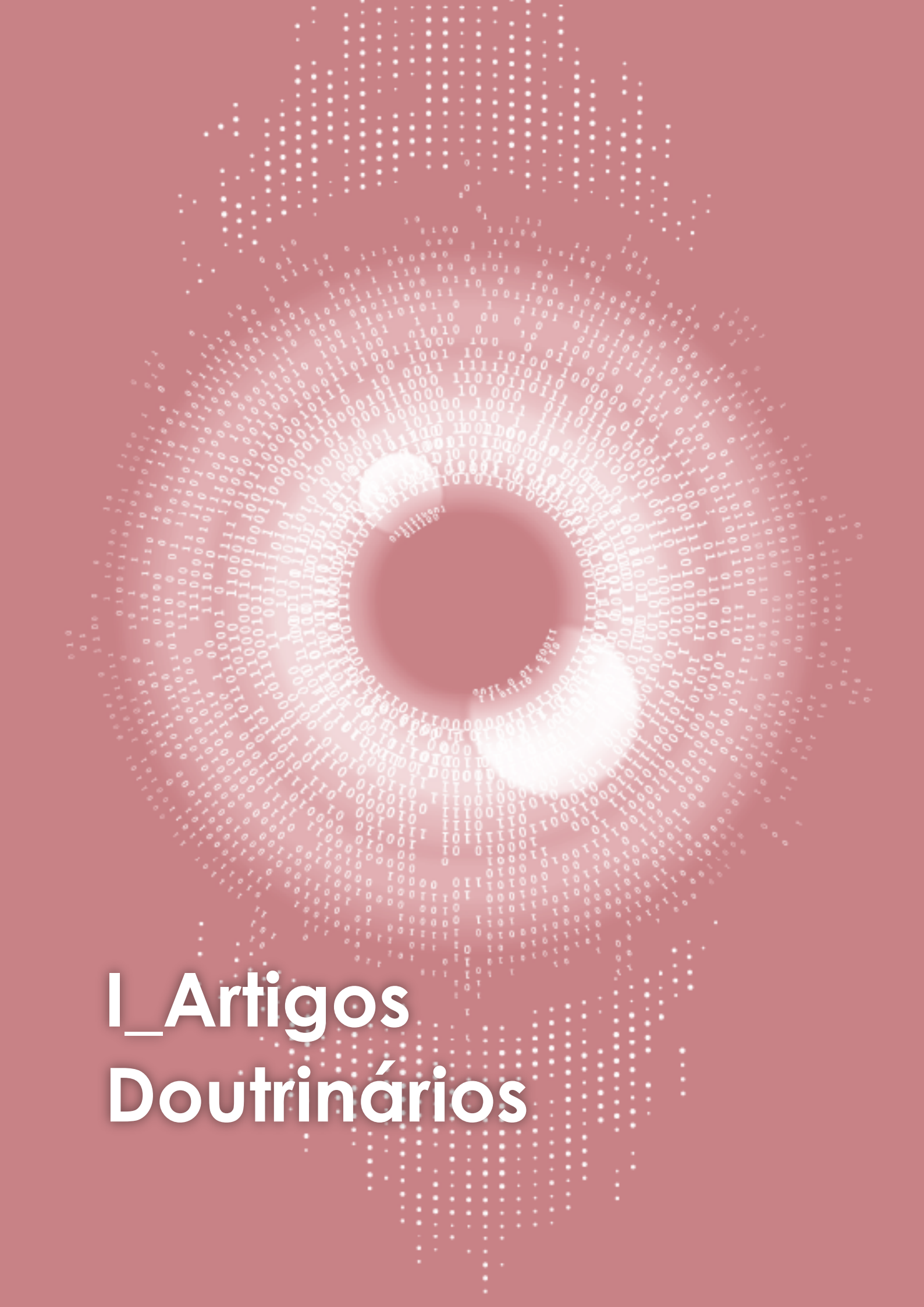
Por último, a instabilidade dos limites legais entre os dados pessoais e os dados não pessoais voltam à ordem do dia. Essa instabilidade assenta no desenvolvimento de tecnologias de anonimização e de personalização potenciadas pela Inteligência Artificial, com riscos crescentes para os responsáveis pelo tratamento e os subcontratantes.

Em sede de "outros estudos", inclui-se um tema de grande atualidade em matéria de propriedade intelectual: a venda de obras digitais certificadas por um *non-fungible token* (NFT). Trata-se de um contrato de compra e venda de obras de artes plásticas, distinto dos contratos tradicionais: como explica neste interessante estudo. No da venda de um NFT, o adquirente não mantém sob sua posse um objeto tangível, mas sim um certificado único de autenticidade, validado por meio de *blockchain*.

No campo da Jurisprudência, a publicação contempla o Acórdão do Tribunal de Justiça nos processos apensos C-37/20 | Luxembourg Business Registers e C-601/20 | Sovim Diretiva antibranqueamento: a disposição que prevê que as informações sobre os beneficiários efetivos das entidades societárias constituídas no território dos Estados-Membros devem estar acessíveis em todos os casos a qualquer membro do público em geral é inválida.

Por último, em matéria de recensão, apresentam-se duas obras distintas, mas que se complementam na sua problematização. Pedro Domingos, na sua obra: *A revolução do algoritmo mestre*, publicada em 2017, refere que vivemos na era dos algoritmos, e que os mesmos se encontram inseridos no "tecido da vida quotidiana". António Damásio, na sua obra: *A estranha ordem das coisas - a vida, os sentimentos e as culturas humanas*, cuja 1ª edição foi igualmente publicada em 2017, refere que, embora haja indícios de que é possível conceber organismos artificiais de modo a que operem de forma inteligente, chegando mesmo a ultrapassar a inteligência dos organismos humanos, nada sugere que por si só consigam constituir a base daquilo que nos torna "distintivamente humanos".

Cristina Maria de Gouveia Caldeira
Pedro Rebelo Botelho Alfaro Velez



I_Artigos Doutrinários

Transferências de Dados Pessoais Para Países Terceiros ou Organizações Internacionais

Cristina Maria de Gouveia Caldeira[1]

RESUMO

Da análise global do sistema europeu e transnacional de trocas internacionais, verifica-se um profundo desequilíbrio entre a robustez e celeridade dos mecanismos de intercâmbio comercial e a ausência de instrumentos supraestaduais de proteção do cidadão, ajustados à realidade internacional, justificando a reforma legislativa da União Europeia em matéria de proteção de dados, adotada no Regulamento Geral de Proteção de Dados (RGPD). Com a aprovação do regulamento, a União Europeia conseguiu um texto paradigmático e unificador da proteção de dados, com uma maior abertura à circulação internacional de dados. Como ficará exposto neste artigo, trata-se de um instrumento ao serviço da Era Digital, essencial às empresas, aos consumidores e à sociedade em geral. No domínio das transferência de dados, o legislador europeu introduziu alterações significativas, face à Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, consagrando no capítulo V um aprofundamento normativo, além de expandir também às organizações internacionais, aos subcontratantes, e às transferências subsequentes oriundas de um país terceiro ou de uma organização internacional.

PALAVRAS-CHAVE:

Princípio geral das transferências, decisão de adequação, garantias adequadas, regras vinculativas aplicadas às empresas, derrogações para situações específicas

[1] Advogada e Docente na área do Direito. Pós-Doutora na área da Propriedade Intelectual pela UNL. Doutorada na área do Direito, na Especialidade em Ciências Jurídcas e Política pela UAL. Bolseira da Fundação Gulbenkian na Universidade de Oxford. Investigadora FCT. I.P. nas áreas do neurodireito e da neuroética, aplicadas ao setor da saúde. E-mail: cristina.caldeira@universidadeeuropeia.pt

Transfers of Personal Data to Third Countries or International Organizations

Cristina Maria de Gouveia Caldeira

ABSTRACT

From the global analysis of the European and transnational system of international exchanges, there is a profound imbalance between the robustness and speed of commercial exchange mechanisms and the absence of superstate instruments for the protection of the citizen, adjusted to the international reality, justifying the legislative reform of the Union European Union on data protection, adopted in the General Data Protection Regulation (GDPR). With the approval of the regulation, the European Union achieved a paradigmatic and unifying text on data protection, with greater openness to the international circulation of data. As will be explained in this article, it is an instrument at the service of the Digital Age, essential for companies, consumers, and society in general. In the field of data transfer, the European legislator introduced significant changes, in view of Directive 95/46/EC, of the European Parliament and of the Council, of October 24, 1995, enshrining in Chapter V a normative deepening and expanding its application as well international organisations, subcontractors, and subsequent transfers from a third country or an international organisation.

KEYWORDS

General principle for transfers, adequacy decision, appropriate safeguards, Binding corporate rules, Derogations for specific situations.

Introdução

No plano europeu, para além da proteção de dados pessoais fazer parte dos fundamentos constitucionais dos Estados membros da União Europeia, a proteção das pessoas relativamente ao tratamento dos seus dados, está igualmente prevista no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE), disposição que tem origem na Convenção 108 de 1981 do Conselho da Europa e na Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

O artigo 16.º do Tratado de Funcionamento da União Europeia (TFUE) constitui a base jurídica do direito derivado em matéria de proteção de dados, arguindo que "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" (n.º 1)" e atribuindo à União Europeia "a competência para legislar sobre a matéria em todas as áreas da sua incumbência" (n.º 2). Sublinha-se que o referido artigo encontra-se integrado na Parte I do TFUE, Título II, onde aí se consagram as *disposições de aplicação geral* e se estabelece um regime geral de proteção de dados aplicável a todos os Estados-Membros.

O legislador europeu atribuiu ao direito de proteção dos dados pessoais um tratamento autónomo, fundado na CDFUE, na qual se estabelece a separação entre o respeito pela vida privada e familiar (artigo 7.º) e o direito fundamental à proteção de dados pessoais (artigo 8.º). Posição distinta adotaram os instrumentos internacionais de proteção dos direitos humanos, que garantem o direito à proteção de dados como uma extensão do direito à privacidade, designadamente a Declaração Universal dos Direitos Humanos (artigo 12.º) e o Pacto Internacional sobre os Direitos Civis e Políticos (artigo 17.º).

A proteção de dados pessoais não se limita, no entanto, ao espaço europeu e, tal como se afirma no considerando 116 do Regulamento Geral de Proteção de Dados (RGPD)[2], "sempre que os dados pessoais atravessarem fronteiras fora do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações". Ou seja, em virtude dos países terceiros[3] não se encontrarem vinculados ao RGPD, ocorre uma maior desproteção do titular dos dados e pode dificultar a intervenção das autoridades de controlo, impedindo-as de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras, além de restringir os poderes preventivos ou insuficiência das medidas de reparação, bem como de outros obstáculos de natureza prática, tais como a limitação de recursos.[4]

---

[2] JOUE. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 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 que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, pp. 1–88).

[3] «País terceiro», qualquer país que não é um Estado-Membro do EEE. «EEE», o Espaço Económico Europeu; inclui os Estados-Membros da União Europeia, a Islândia, a Noruega e o Listenstaine. O RGPD aplica-se a estes últimos por força do Acordo EEE, em especial os seus anexo XI e protocolo 37.

[4] Considerando 116 do RGPD.

O Capítulo IV da Diretiva 95/46/CE, de 24 de outubro, já abordava a «Transferência de dados pessoais para países terceiros», não se tratando assim de um tema novo. Porém, a evolução tecnológica e a globalização proporcionam um aumento significativo da recolha e partilha de dados pessoais, contribuindo assim para facilitar a sua circulação, concedendo quer às empresas privadas, quer às entidades públicas, a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades[5].

Porém, face ao impacto económico das transferências internacionais, e à vulnerabilidade dos cidadãos, em parte devido à ausência de limites jurisdicionais ao processamento dos seus dados, imponha-se um sistema normativo intransigente na defesa do direito fundamental à proteção dos dados pessoais, sem obstaculizar o tráfego de dados. O capítulo V do RGPD, projetado em sete disposições (artigos nºs 44.º; 45.º; 46.º 47.º, 48.º 49.º e 59.º), resulta desse contexto, e da necessidade de assegurar a continuidade do elevado nível de proteção sempre que os dados pessoais são transferidos para um país terceiro[6].

Veremos ao longo do texto que os países e as organizações internacionais têm à sua disposição um catálogo rigoroso e pormenorizado de elementos que a Comissão deve ter em conta quando avalia a adequação da proteção de um sistema estrangeiro. Na sua avaliação de um país terceiro ou de um território ou setor específico de um país terceiro, a Comissão deve avaliar se o país respeita o primado do Estado de Direito, se o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos são cumpridas, bem como a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, e ainda, a lei da ordem pública e a lei penal[7].

1. O impacto da evolução tecnológica e da digitalização nas transferências de dados pessoais

Em matéria de fluxos transfronteiriços de dados pessoais, o RGPD não constitui uma grande novidade, uma vez que o registo substantivo é o mesmo. No entanto, veio clarificar e simplificar a sua utilização à medida que introduz novos instrumentos no capítulo dedicado às transferências, expandindo a sua aplicação também às organizações internacionais, aos subcontratantes, e às transferências subsequentes oriundas de um país terceiro ou de uma organização internacional.

A Diretiva 95/46/CE, de 24 de outubro de 1995[8], considerava que os fluxos transfronteiriços de dados eram necessários ao desenvolvimento do comércio

[5] Considerando 6 do RGPD..

[6] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS. Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE Versão 2.0 Adotado em 18 de junho de 202, p. 3. Disponível em: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pt.pdf

[7] Considerando 104 do RGPD.

[8] JOCE. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Jornal Oficial das Comunidades Europeias, L 281, 23 de novembro de 1995, era complementada por exemplo pela Decisão-Quadro 2008/977/ JAI do Conselho, de 27 de novembro de 2008, relativa à

internacional e que a proteção garantida não obstava às transferências de dados pessoais para países terceiros que assegurassem um nível de proteção adequado, sendo que o nível de proteção oferecido por um país terceiro deveria ser apreciado em função de todas as circunstâncias associadas à transferência ou a uma categoria de transferências[9]. Em contrapartida, sempre que um país terceiro não oferecesse um nível de proteção adequado, a transferência de dados pessoais para esse país deve ser proibida[10]. Em todo o caso, as transferências para países terceiros só poderiam ser efetuadas no pleno respeito pelas disposições adotadas pelos Estados-Membros nos termos da diretiva[11].

Da análise global do sistema europeu e transnacional de trocas internacionais, verifica-se um profundo desequilíbrio entre a robustez e celeridade dos mecanismos de intercâmbio comercial e a ausência de instrumentos supraestaduais de proteção do cidadão, ajustados à realidade internacional, justificando a reforma legislativa da União Europeia em matéria de proteção de dados, adotada no RGPD. Com a aprovação do regulamento, a União Europeia conseguiu um texto paradigmático e unificador da proteção de dados, com uma maior abertura à circulação internacional de dados. Como ficará exposto neste artigo, trata-se de um instrumento ao serviço da Era Digital, essencial às empresas, aos consumidores e à sociedade em geral. Nele, o legislador europeu introduziu alterações significativas face à Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, no capítulo V do RGPD, expandindo a sua aplicação também às organizações internacionais, aos subcontratantes, e às transferências subsequentes oriundas de um país terceiro ou de uma organização internacional.

A referida diretiva foi revogada pelo RGPD, instrumento que veio harmonizar e simplificar o enquadramento jurídico no domínio da proteção dos dados e na livre circulação dos dados pessoais, tornando a atividade empresarial mais fácil, ao mesmo tempo que reforça a confiança dos consumidores na economia digital. Nessa conformidade, as empresas devem proceder ao levantamento e mapeamento dos dados pessoais tratados, alterar a sua política de comunicação interna e externa e designar o responsável pela *compliance*. Essa harmonização constitui uma vantagem comparativa do espaço europeu face ao resto do mundo e uma vantagem competitiva para as empresas europeias, na medida em que oferecem a garantia de regulação, relevante para quem tem visto os seus dados sistematicamente usados indevidamente.

Um pouco por todo o mundo, as empresas, de países externos à União Europeia, especialmente as de dimensão mundial tentam o alinhamento com as políticas de privacidade do RGPD, não só porque o consideram um modelo a seguir, mas também porque pretendem continuar a exercer as suas atividades comerciais na Europa. Assim

---

proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal e que se aplica para a proteção de dados pessoais nestas matérias. Além disso, como a Diretiva de Proteção de Dados tem como destinatários os Estados, foi necessário adotar o Regulamento nº 45/2001 para proteger os dados de caráter pessoal do uso que as instituições, órgãos e organismos da UE façam deles.

[9] Cfr. Considerando 56 da Dir.

[10] Cfr. Considerando 57 da Dir.

[11] Cfr. Considerando 60 da Dir.

é em África, na Ásia e na América Latina, onde a proteção de dados pessoais desempenha um papel fundamental no advento das novas tecnologias. O Chile, a Colômbia, o México, o Peru, a Argentina e em particular o Brasil com a Lei n.º 13.709, de 14 de agosto de 2018, complementada pela Medida Provisória n.º 869, de 27 de dezembro de 2018, criaram um enquadramento legal à semelhança do RGPD. Outros, como o Japão, os EUA e a Índia, adotaram nova legislação ou atualizaram a legislação existente em matéria de proteção de dados, para aproveitar as oportunidades oferecidas pela economia digital global e responder à procura crescente de reforço da segurança dos dados e da proteção da privacidade. De salientar que a proteção de dados e o intercâmbio comercial crescem paralelamente.

Relevante é também, a celebração de acordos de comércio livre celebrados entre a União Europeia e os EUA, o Japão, o Mercosul, o México, a Tunísia e países da ASEAN, em 2017. E, embora existam diferenças entre os países, no que toca a abordagem adotada e ao nível do desenvolvimento legislativo, existem sinais de uma maior convergência em relação a importantes princípios de proteção de dados nos vários continentes.

A grande quantidade de dados produzidos ao nível global, *big data*, requer técnicas complexas de processamento e leva-nos a uma sociedade em rede que vai sendo configurada pelas novas tecnologias. Na atual sociedade, a evolução tecnológica e a digitalização estão a transformar, um porco por todo o mundo, as indústrias, os empregos e as carreiras profissionais, assim como os sistemas educativos e de segurança social. Em muitos países assiste-se ao apoio de projetos estratégicos em domínios de vanguarda como a inteligência artificial, os supercomputadores, a cibersegurança ou a digitalização industrial, bem nas competências digitais. Todos se preparam para um mercado digital, ao mesmo tempo que se verifica uma enorme mudança na sociabilidade, que é totalmente suportada pela lógica própria das redes de comunicação, que se adaptam perfeitamente na forma de construir sociabilidades em redes.

A sociedade em rede contém uma característica central que se traduz na "transformação da área da comunicação, incluindo os media. A comunicação constitui o espaço público, ou seja, o espaço cognitivo em que as mentes das pessoas recebem informação e formam os seus pontos de vista através do processamento de sinais da sociedade no seu conjunto."[12]. Por sua vez, a cooperação científica bem como a introdução coordenada de novas redes de telecomunicações exigem e facilitam a circulação transfronteiras de dados pessoais.

2. Artigo 44.º - Princípio geral das transferências de dados pessoais

O princípio geral das transferências, vertido no artigo 44.º do RGPD, enuncia que qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional, só é realizada se, sem prejuízo das outras disposições do regulamento, as condições estalecidas no capítulo V forem respeitadas pelo responsável pelo tratamento e pelo

[12] CASTELLS, Manuel e CARDOSO, Gustavo, A Sociedade em Rede Do Conhecimento à Acção Política, Conferência promovida pelo Presidente da República 4 e 5 de março de 2005, no Centro Cultural de Belém, 2005, Lisboa. Disponível em: http://eco.imooc.uab.pt/elgg/file/download/51670

subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. O princípio geral das transferências é clarificado no considerando 101, ao referir que,

> "(…) quando os dados pessoais são transferidos da União para responsáveis pelo tratamento, para subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional."

O principio geral plasmado no artigo 44.º concretiza-se em várias soluções que são apresentadas de forma ordenada nas disposições seguintes do capítulo V. Assim, uma transferência de dados pessoais para um pais terceiro ou uma organização pode ser realizada mediante a existência de uma decisão de adequação da Comissão, tal como se extrai do n.º 1 do artigo 45.º do RGPD. Por sua vez, «Não tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, os responsáveis pelo tratamento ou subcontratantes, só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentados garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.» (n.º 1 do artigo 46.º do RGPD).

É ainda atribuída a possibilidade de realização de acordos entre o exportador de dados europeu e o importador de dados, cujo país não seja dotado de uma decisão de adequação, de modo a superar a insuficiente proteção conferida pelo país terceiro. Assim, as "carências de proteção de dados do país terceiro podem ser supridas pela configuração de garantias adequadas estabelecidas pelo artigo 46.º"[13].

Todas as disposições do capítulo V são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo RGPD. (artigo 44.º *in fine*). Os dados pessoais só podem ser transferidos se o destinatário der garantias de oferecer um nível adequado de proteção, sendo relevante observar, que à luz do artigo 44.º do RGPD, o responsável sediado na União Europeia, responde por negligência na seleção e vigilância das transferências para o país terceiro ou organização internacional[14]. O considerando 101 reforça este entendimento ao observar que,

> "(…) as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento. Só poderão ser realizadas transferências se, sob reserva das demais disposições do presente regulamento, as condições constantes das disposições do

[13] MENEZES CORDEIRO. *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, Coimbra, 2021, p. 331.

[14] SCHRODER. Anotação ao artigo 44.º do RGPD em Kuhling/Buchner, Rn.24., in MENEZES CORDEIRO. *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, Coimbra, 2021, p. 321, nota de rodapé 21.

> presente regulamento relativas a transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante."

Do exposto, verifica-se que o capítulo V do RGPD assume uma importância crucial na regulação das transferências de dados, tutelando: (i) a defesa do desenvolvimento económico e reforço da cooperação internacional através do tráfego de dados; e (ii) a garantia de que os dados dos titulares são protegidos ao longo da transferência dos seus dados. Essa garantia encontra-se expressa no considerando 114, segundo o qual,

> "Os titulares dos dados deverão ter direito a apresentar reclamação a uma única autoridade de controlo única, particularmente no Estado-Membro da sua residência habitual, e direito a uma ação judicial efetiva, nos termos do artigo 47.º da Carta, se considerarem que os direitos que lhes são conferidos pelo presente regulamento foram violados ou se a autoridade de controlo não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas necessárias para proteger os seus direitos."

A transferência de dados para um destinatário de um país terceiro configura uma operação de tratamento, à luz do n.º 2 do artigo 4.º do RGPD. Essa transferência poderá ser direta ou por intermédio da *internet*, bem como de qualquer outro meio utilizado para disponibilizar dados pessoais em benefício desse terceiro. Sublinhe-se que os nºs 1 e 2 do artigo 2.º do RGPD, aplicam-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados. Em qualquer circunstância, é necessário assegurar que o nível de proteção das pessoas singulares garantido pelo RGPD não é comprometido quando os dados pessoais são transferidos para países terceiros, inclusivamente em caso de transferências ulteriores.

O RGPD estabelece que qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional, só é realizada se forem observadas pelos destinatários dos dados pessoais (responsáveis, subcontratantes e outros destinatários), todas as condições estabelecidas no capítulo V do regulamento. Ou seja, independentemente de tratamentos de dados pessoais posteriores pelo seu recetor, o responsável ou subcontratante, deverão assegurar a conformidade com o RGPD.

3. Os instrumentos destinados às transferências internacionais

Artigo 45.º - Transferências com base numa decisão de adequação

Reforçando o que anteriormente mencionamos, a transferência com base numa decisão de adequação[15] está prevista no artigo 45.º do RGPD, e a avaliação a realizar

[15] Cfr. COMISSÃO EUROPEIA. COMISSÃO EUROPEIA. *Adequacy decisiona. How the EU determines if a non-EU country has na adequate level of data protection.* Decisões de adequação para consulta. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt

pela Comissão deve ter em conta, entre outros os seguintes elementos: o primado do Estado de Direito; o respeito pelos direitos humanos e liberdades fundamentais; a legislação pertinente em vigor, nomeadamente em matéria de proteção de dados; segurança pública; defesa e segurança nacional; direito penal e o respeitante ao acesso das autoridades públicas a dados pessoais (n.º 2).

Prevê-se explicitamente a avaliação da adequação da proteção num território específico de um país terceiro ou num setor ou indústria específico de um país terceiro, a que designamos adequação formal. Nesses termos, o artigo 45.º do RGPD refere:

> 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.
> (...)
> 8. A Comissão publica no Jornal Oficial da União Europeia e no seu sítio web uma lista dos países terceiros, territórios e setores específicos de um país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, se asseguram ou não um nível de proteção adequado

O princípio de proteção adequado é central na legislação de proteção de dados da União Europeia e pressupõe que uma transferência para um país terceiro/organização internacional só seja permitida se estiver assegurado um nível adequado de proteção para os dados pessoais a transferir. Esse princípio já constava da Diretiva 95/46/CE, de 24 de outubro de 1995, a qual previa que a transferência de dados pessoais para um país fora da União Europeia ou fora do Espaço Económico Europeu, só podia realizar-se se o país terceiro assegurasse um nível de proteção adequado e, a lei de execução dos Estados-Membros de outras disposições da diretiva tiver sido respeitada antes de efetuada a transferência. A Diretiva 95/46/CE exigia um nível de proteção substancialmente equivalente, exigência que era apurada pela análise da legislação interna e respetivos compromissos internacionais do país terceiro. Nesses casos, cabia à Comissão Europeia determinar se o país terceiro em causa, garantia ou não o nível de proteção adequado.

A Comissão pode decidir, com efeitos no conjunto da União, que um país terceiro, um território ou um setor determinado de um país terceiro, ou uma organização internacional, oferece um nível adequado de proteção de dados adequado, garantindo assim a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro ou à organização internacional que seja considerado apto a assegurar tal nível de proteção. Nesses casos, podem realizar-se as transferências de dados pessoais para esse país ou organização internacional, sem que para tal seja necessária mais alguma autorização. A Comissão pode igualmente decidir, após enviar ao país terceiro ou organização internacional uma notificação e uma declaração completa dos motivos, revogar essa decisão.[16]

A adoção de uma decisão de adequação é exigente, e tal como afirmamos anteriormente, obriga à conformidade com os valores fundamentares e os direitos humanos defendidos pela União. Por sua vez, os critérios que presidem à avaliação

[16] Considerando 103 do RGPD.

devem ser claros e objetivos, exigindo-se ao país terceiro que garanta o controlo efetivo e independente da proteção dos dados e estabeleça regras de cooperação com as autoridades de proteção de dados dos Estados-Membros. Deve ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial."[17]

Quando um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, deixa de assegurar um nível adequado de proteção de dados, cabe à Comissão reconhecer essa inadequação, proibindo a transferência de dados pessoais para esse país terceiro ou organização internacional, a menos que sejam cumpridos os requisitos constantes do presente regulamento relativos a transferências sujeitas a garantias adequadas, incluindo regras vinculativas aplicáveis às empresas, ou se verifiquem derrogações. Nesses casos, deverão ser tomadas medidas que visem uma consulta entre a Comissão e esse país terceiro ou organização internacional, competindo à Comissão informar o país terceiro ou a organização internacional das razões da proibição e iniciar consultas com o país ou organização em causa, a fim de corrigir a situação."[18]

Análise do Tribunal de Justiça da União Europeia (TJUE): Acórdão "Schrems"

Pela relevância que apresenta para o tema em estudo, relembramos a Decisão 2000/520/CE de 26 de julho de 2000[19], tomada com base no n.º 6 do artigo 25.o da Diretiva 95/46[20], no pressuposto de que estariam devidamente protegidas as

[17] Considerando 104 do RGPD.

[18] Considerando 107 do RGPD.

[19] JORNAL OFICIAL DAS COMUNIDADES EUROPEIA. Decisão da Comissão 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América, publicado no Jornal Oficial das Comunidades de 25 de agosto de 2000. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=PT

[20] *Artigo 25.º* Princípios

1.Os Estados-Membros estabelecerão que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adotadas nos termos das outras disposições da presente diretiva, o país terceiro em questão assegurar um nível de proteção adequado. 2.A adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou setoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país. 3.Os Estados-Membros e a Comissão informar-se-ão mutuamente dos casos em que consideram que um país terceiro não assegura um nível de proteção adequado na aceção do n.º 2. 4.Sempre que a Comissão verificar, nos termos do procedimento previsto no n.º 2 do artigo 31.º, que um país terceiro não assegura um nível de proteção adequado na aceção do n.º 2 do presente artigo, os Estados-Membros tomarão as medidas necessárias para impedir qualquer transferência de dados de natureza idêntica para o país terceiro em causa. 5.Em momento oportuno, a Comissão encetará negociações com vista a obviar à situação resultante da constatação feita em aplicação do n.º 4. 6.A Comissão pode constatar, nos termos do procedimento previsto no n.º 2 do artigo 31.º, que um país terceiro assegura um nível de proteção adequado na aceção do n.º 2 do presente artigo em virtude da sua legislação interna

transferências de dados pessoais da União Europeia para empresas norte-americanas que subscreveram voluntariamente o regime do «porto seguro» ou *safe harbor* (um mecanismo de auto-certificação de um conjunto de regras acordadas pela Comissão Europeia e o US Department of Commerce).

No Acórdão de 6 de outubro de 2015, no processo C-362/14, Maximilian Schrems/Data Protection Commissioner, EU:C:2015:650 («acórdão Schrems I»), o TJUE invalidou a Decisão 2000/520/CE relativa ao Safe Harbour que permitiria a empresas americanas, entre as quais, as gigantes do mundo da Internet, transferir dados pessoais de clientes e utilizadores, da União Europeia para os EUA[21].

O referido acórdão foi proferido em resposta a um pedido de decisão prejudicial apresentado pelo High Court of Ireland sobre se a decisão da Comissão Europeia relativa ao Safe Harbour, que tem como efeito impedir uma autoridade nacional de proteção de dados de investigar uma queixa na qual se alegue que um país terceiro, no caso do presente acórdão, os EUA, não asseguram um nível de proteção adequada dos dados pessoais transferidos.

A factualidade deste processo, refere-se a Maximillian Schrems, cidadão austríaco e utilizador da rede social Facebook, que em 2013, na sequência das revelações feitas por Edward Snowden, apresentou uma queixa junto do regulador de dados pessoais da Irlanda, na qual denunciou falhas na proteção dos dados transferidos para os EUA ao abrigo do referido acordo «porto seguro».

A autoridade reguladora irlandesa considerou-se impedida de avaliar o grau de proteção de fluxos de dados processados nesse âmbito, em virtude da decisão 2000/520/CE de 26 de julho de 2000, o que levou Maximillian Schrems a interpor recurso para o Supremo Tribunal de Justiça da Irlanda, que entendeu suspender a instância e submeter ao TJUE, a questão prejudicial, tendo o processo culminado no acórdão do TJUE que, além de responder às questões prejudiciais, declarou a invalidade da decisão da Comissão[22].

---

ou dos seus compromissos internacionais, subscritos nomeadamente na sequência das negociações referidas no n.º 5, com vista à proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas. Os Estados-Membros tomarão as medidas necessárias para dar cumprimento à decisão da Comissão.

[21]TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção) de 6 de outubro de 2015. Maximillian Schrems contra Data Protection Commissioner. Pedido de decisão prejudicial apresentado pela High Court (Irlanda). Reenvio prejudicial — Dados pessoais — Proteção das pessoas singulares no que diz respeito ao tratamento desses dados — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.°, 8.° e 47.° — Diretiva 95/46/CE — Artigos 25.° e 28.° — Transferência de dados pessoais para países terceiros — Decisão 2000/520/CE — Transferência de dados pessoais para os Estados Unidos — Nível de proteção inadequado — Validade — Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos — Poderes das autoridades nacionais de controlo. Processo C-362/14. Disponível: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62014CJ0362

[22] De recordar que em abril de 2014 o TJUE invalidou um instrumento jurídico comunitário com grande impacto na proteção de dados pessoais. Nessa data, o TJUE declarou inválida a Diretiva 2006/24/CE relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas. Assim o acórdão "Schrems" constitui a segunda vez que um instrumento jurídico comunitário é invalidado em matéria de proteção de dados.

A existência de um nível muito elevado de acessos a dados pessoais realizados por diversas entidades governamentais dos EUA, incluindo a NSA (National Security Agency), denunciados por Edward Snowden em 2013, influenciou de forma determinante a análise da legislação norte-americana. Para além de não serem reconhecidos aos cidadãos os direitos fundamentais de exercício de retificação e de apagamento dos seus dados então transferidos, as entidades americanas poderiam utilizar os dados pessoais, sem quaisquer limitações, sempre que a segurança nacional ou o interesse público o imponham.

As autoridades reguladoras dos Estados-Membros pronunciaram-se no sentido de não emissão de novas autorizações para transferências de dados com base nesse acordo. Contudo, assumiram posições distintas no que toca às transferências para os EUA ao abrigo de outros instrumentos alternativos ao «porto seguro». Assim, a autoridade reguladora da Alemanha adotou uma das posições mais rígidas ao revelar que não iria emitir novas autorizações de transferências de dados para os EUA, ainda que fundamentadas em outros instrumentos alternativos, como sejam as Binding Corporate Rules ou outros contratos ad-hoc. E, para o futuro todas as empresas estabelecidas na Alemanha que pretendam transferir dados para os EUA terão de seguir as resoluções da autoridade reguladora alemã sobre "Human Rights and Electronic Communication" e "Cloud Computing", de março e outubro de 2014, respetivamente, não devendo as respetivas transferências ocorrer de forma massiva ou repetitiva.

Bem mais moderada foi a posição da Comissão Nacional de Proteção de Dados, que no comunicado de 23 de outubro de 2015, veio informar que iniciaria a partir dessa data um processo formal de revisão de todas as autorizações concedidas com base nos pressupostos do «porto seguro». Mais informou que continuaria a emitir autorizações para transferências de dados para os EUA com base noutros instrumentos alternativos, ainda que a título provisório e sujeitas a revisão num futuro próximo. Assim, do ponto de vista jurídico, as empresas estabelecidas em Portugal que pretendessem transferir dados para os EUA puderam continuar a fazê-lo, desde que para isso revissem os instrumentos ao abrigo dos quais esses fluxos se realizam, recomendando-se a adoção de cláusulas contratuais modelo UE.

O acórdão do Tribunal de Justiça, de 16 de julho de 2020[23] "Schrems II", para além da importância crucial na interpretação do princípio da adequação, permite-nos concluir que:

1) O artigo 2.º, n.ºs 1 e 2, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 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 que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), deve ser interpretado no sentido de que está abrangida pelo âmbito de aplicação deste regulamento uma transferência de dados pessoais efetuada para fins comerciais por um operador económico estabelecido num Estado-Membro para outro operador económico estabelecido num país terceiro, não obstante o facto de, no decurso ou

[23] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020. Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems. Pedido de decisão prejudicial apresentado pela High Court (Irlanda)

C-311/18 - Facebook Ireland e Schrems. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-311/18&language=PT

na sequência dessa transferência, esses dados serem suscetíveis de ser tratados pelas autoridades do país terceiro em causa para efeitos de segurança pública, de defesa e de segurança do Estado.

2) O artigo 46.º, n.º 1, e o artigo 46.º, n.º 2, alínea c), do Regulamento 2016/679 devem ser interpretados no sentido de que as garantias adequadas, os direitos oponíveis e as medidas jurídicas corretivas eficazes, exigidos por estas disposições, devem assegurar que os direitos das pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas-tipo de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União Europeia por este regulamento, lido à luz da Carta dos Direitos Fundamentais da União Europeia. Para este efeito, a avaliação do nível de proteção assegurado no contexto dessa transferência deve, nomeadamente, ter em consideração tanto as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União Europeia e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro, nomeadamente os enunciados no artigo 45.º, n.º 2, do referido regulamento.

3) O artigo 58.º, n.º 2, alíneas f) e j), do Regulamento 2016/679 deve ser interpretado no sentido de que, a menos que exista uma decisão de adequação validamente adotada pela Comissão Europeia, a autoridade de controlo competente está obrigada a suspender ou a proibir uma transferência de dados para um país terceiro com base em cláusulas-tipo de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar, à luz de todas as circunstâncias específicas dessa transferência, que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União, em particular pelos artigos 45.º e 46.º deste regulamento e pela Carta dos Direitos Fundamentais, não pode ser assegurada por outros meios, no caso de o responsável pelo tratamento ou o seu subcontratante estabelecidos na União não terem eles próprios suspendido ou posto termo à transferência.

4) O exame da Decisão 2010/87/UE da Comissão, de 5 de fevereiro de 2010, relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, conforme alterada pela Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de dezembro de 2016, à luz dos artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais não revelou nenhum elemento suscetível de afetar a validade desta decisão.

5) A Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, é inválida

Artigo 46.º Transferências sujeitas a garantias adequadas

Com bem o observamos, na falta de uma decisão de proteção adequada, as transferências internacionais podem efetuar-se com base em vários instrumentos de transferências alternativos que prevejam as garantias adequadas em matéria de proteção de dados. No n.º 1 do artigo 46.º observa-se que

> «1. Não tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes."

Importa sublinhar que o artigo 46.º reporta-se aos casos cujo âmbito de aplicação não se encontra abrangido pelo artigo 45.º do RGPD. O n.º 2 do artigo 46.º estabelece um elenco de garantias adequadas, sem que seja necessário requerer uma autorização específica de uma autoridade de controlo, designadamente: um instrumento juridicamente vinculativo (alíne a); regras vinculativas (alínea b); cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame (alínea c); claúsulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame; um Código de conduta ou procedimentos de certificação (alínea e) e f)).

Cláusulas-tipo de proteção de dados adotadas pela Comissão

Do elenco das garantias previstas no n.º 2 do artigo 46.º, destacamos as cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros (alínea c), as quais foram alvo de uma Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021. No considerando 3 da Decisão clarifica-se o papel das cláusulas contratuais-tipo, em matéria de garantias técnicas e organizativas de modo a minimizar os riscos que a operação de transferência de dados determina. Nessa medida,

> "(…) o responsável pelo tratamento ou subcontratante que transfere os dados pessoais para um país terceiro («exportador de dados») e o responsável pelo tratamento ou subcontratante que recebe os dados pessoais («importador de dados») têm a liberdade de incluir essas cláusulas contratuais-tipo num contrato mais abrangente e de acrescentar outras cláusulas ou garantias adicionais, desde que não colidam, direta ou indiretamente, com as cláusulas contratuais-tipo, e sem prejuízo dos direitos ou das liberdades fundamentais dos titulares dos dados."

Não tendo sido tomada qualquer decisão nos termos do n.º 3 do artigo 45.º do RGPD, o responsável pelo tratamento ou o subcontratante pode recorrer às cláusulas-tipo de proteção de dados adotadas pela Comissão, e são encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas contratuais-tipo. O argumento é reforçado no 109 do RGPD, onde aí se enfatiza:

> "A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo não os deverá impedir de incluírem estas cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e

> outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados."

O considerando 114 do RGPD reforça que em qualquer caso, se a Comissão não tiver tomado nenhuma decisão relativamente ao nível de proteção adequado de dados num determinado país terceiro, o responsável pelo tratamento ou o subcontratante deverá adotar soluções que confiram aos titulares dos dados direitos efetivos e oponíveis quanto ao tratamento dos seus dados na União, após a transferência dos mesmos, e lhes garantam que continuarão a beneficiar dos direitos e garantias fundamentais.

Na Recomendação 01/2020, de 18 de junho de 2021, o Comité Europeu da Proteção de Dados (CEPD) [24], adota um roteiro de auxílio aos exportadores que passa pelas seguintes etapas:

Etapa 1: Conhecer as transferências

O CEPD recomenda ao exportador que conheça as suas transferências. E, assumindo que será complexo o levantamento de todas as transferências de dados pessoais para países terceiros, ainda assim incita o exportador a conhecer o destino dos dados pessoais, de modo a garantir que estes beneficiam de um nível de proteção essencialmente equivalente. Recomenda ainda que o exportador verifique se os dados transferidos são adequados, pertinentes e limitados ao necessário relativamente aos fins para os quais são tratados.

Etapa 2: Identificar os instrumentos de transferência utilizados

Impõe-se a verificação dos instrumento de transferência enumerados no capítulo V do RGPD. Em caso da Comissão Europeia já ter declarado que o país, a região ou o setor para os quais são transferidos os dados são adequados, através de uma decisão de adequação (45.º do RGPD) ou ao abrigo da anterior Diretiva 95/46, enquanto a decisão estiver em vigor, o exportador deverá apenas verificar se a decisão de adequação permanece válida. Na ausência de uma decisão de adequação, o exportador deve recorrer a um dos instrumentos de transferência enumerados no artigo 46.º do RGPD.

Etapa 3: Avaliar se o instrumento de transferência do artigo 46.º do RGPD utilizado é eficaz tendo em conta todas as circunstâncias da transferência

O CEPD recomenda que o exportador analise a legislação do país terceiro e as práticas das autoridades públicas desse país, com pertinência para a sua transferência e para o instrumento de transferência do artigo 46.º do RGPD utilizado, de modo a verificar se é assegurada a proteção efetiva dos dados pessoais transferidos. Caso não se verifique a proteção adequada, o exportador deve suspender a transferência ou aplicar

[24] COMITÉ EUROPEU DE PROTEÇÃO DE DADOS. Recomendação 01/2020, relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE.

Disponível em: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pt.pdf

medidas complementares adequadas, se desejar prosseguir com a transferência. O exportador deve efetuar a referida avaliação com a devida diligência e documentá-la integralmente, para efeitos de fiscalização e controlo.

Etapa 4: Adotar medidas complementares

A presente etapa apenas se justifica se a avaliação do exportador revelar que legislação e/ou as práticas do país terceiro afetam a eficácia do instrumento de transferência do artigo 46.º do RGPD que o exportador utiliza ou pretende utilizar no contexto da transferência.Nesse caso, deve fazer uso do anexo 2 da Recomendação 1/2020 do CEPD, onde encontra uma lista exaustiva de exemplos de medidas complementares e algumas das condições necessárias à sua aplicação.

Etapa 5: Etapas do processo a seguir quando o exportador identifica medidas complementares eficazes

O exportador deve adotar todas as medidas processuais formais que a medida complementar possa exigir, em função do instrumento de transferência do artigo 46.º do RGPD que utilizar. Consoante o grau de risco que oferece, poderá justificar uma consulta às autoridades de controlo competentes, relativamente a algumas das referidas medidas.

Etapa 6: Reavaliar com a frequência adequada

Esta última etapa consiste em reavaliar, com a periodicidade adequada, o nível de proteção concedido aos dados transferidos para países terceiros e controlar eventuais desenvolvimentos passados ou futuros que o possam afetar.

Artigo 47.º - Regras vinculativas aplicáveis às empresas

Pelo procedimento de controlo da coerência previsto no artigo 63.º, a autoridade de controlo competente aprova regras vinculativas aplicáveis às empresas, garantias que compartilham a mesma natureza das previstas no artigo 46.º do RGPD, as quais nos termos do n.º1 do artigo 47.º devem:

a) ser juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento;
b) conferir expressamente aos titulares dos dados direitos oponíveis relativamente ao tratamento dos seus dados pessoais; e
c) preencher os requisitos estabelecidos no n.º 2.

As regras vinculativas aplicáveis às empresas, na terminologia inglesa *Binding Corporate Rules* (BCR), devem ser adotadas por estas como diretrizes internas, obrigando juridicamente os destinatários. As BCR encontram-se referenciadas no considerando 108 do RGPD, e são regras que devem assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do

titular de dados e de medidas jurídicas corretivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indemnização, quer no território da União quer num país terceiro. Deverão estar relacionadas, em especial, com o respeito pelos princípios gerais relativos ao tratamento de dados pessoais (artigo 5.º do RGPD) e pelos princípios de proteção de dados desde a conceção e por defeito (artigo 25.º do RGPD).

Artigo 48.º - Tranferências ou divulgações não autorizadas pelo direito da União

O artigo 48.º faz depender a transferência de dados pessoais fundada em decisão de um tribunal ou de uma autoridade administrativa e da existência de um acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros, que contemple essa possibilidade[25].

Artigo 49.º - Derrogações para situações específicas

O artigo 49.º contempla derrogações para situações específicas, no âmbito das quais, em face de situações excecionais não poderão ser vedadas as transferências de dados, mesmo na ausência de uma decisão de adequação ou de uma BCR. Releva-se no entanto, que o nível de proteção do titular dos dados nunca deverá ser inferior à proteção concebida pelo RGPD. As derrogações sustentam-se maioritariamente na autodeterminação dos titulares e ainda em interesses públicos. Importa sublinhar que o exportador apenas poderá recorrer a uma das derrogações previstas no artigo 49.º do RGPD, desde que cumpra as condições estipuladas, limitadas a situações específicas e não podem tornar-se a «regra».

Artigo 50.º - Cooperação internacional no domínio da proteção de dados pessoais

Por último, o RGPD contempla no artigo 50.º a cooperação internacional no domínio da proteção de dados, apresentando-se como complementar às disposições anteriores e abrangendo a cooperação entre a Comissão e as autoridades de controlo europeia com os paises terceiros e organizações internacionais.

Considerações finais

O caminho percorrido, permitiu observar como o acórdão Schrems II, no processo C-311/18, reposicionou a União Europeia a um nível externo em matéria de direitos fundamentais, ao realizar os princípios previstos no Tratado de Lisboa e na CDFUE. De salientar também o impacto do acórdão relativamente à vigilância generalizada aos serviços de informações estatais e à violação dos direitos fundamentais daí decorrentes, quer nas relações transatlânticas, quer nas relações entre Estados-Membros.

Vimos também que uma Decisão da Comissão que considere que um país terceiro assegura um nível de proteção adequado na aceção da Diretiva 95/46/CE, tal como a decisão do *Safe Harbour*, não impede uma autoridade nacional de proteção

[25] Considerando 115 do RGPD.

de dados de investigar uma queixa em que se alega que um país terceiro não assegura um nível de proteção adequado.

Relevante é também o facto das autoridades de proteção de dados exercerem com independência as suas funções de fiscalização. Esclarece o TJUE, pela primeira vez, que o conceito de adequação exige ao país terceiro a necessidade de assegurar um nível de proteção dos dados pessoais substancialmente equivalente ao conferido dentro da União Europeia. Desta forma, preserva-se uma margem de abertura para adaptar as apreciações de adequação às diferentes culturas e tradições jurídica.

No mesmo acórdão o TJUE declara a invalidade da totalidade do Safe Harbour com base na invalidade dos artigos 1.º e 3.º da Decisão 2000/520/CE, por concluir que o nível de proteção assegurado pelos EUA não é "substancialmente equivalente" ao consagrado na Diretiva 95/46/CE. Igualmente relevante foi a validação das cláusulas contratuais-tipo pelo TJUE, como instrumentos de transferência que podem assegurar contratualmente um nível de proteção essencialmente equivalente para os dados transferidos para países terceiros. Foi ainda reafirmado que o *Safe Harbour* permitia uma ingerência nos direitos fundamentais dos indivíduos cujos dados pessoais eram transferidos para os EUA ao abrigo do referido instrumento, criticando a Comissão por ter mantido uma posição de inércia, face às deficiências na limitação dessa ingerência.

Referências

CASTELLS, Manuel e CARDOSO, Gustavo, **A Sociedade em Rede Do Conhecimento à Acção Política**, Conferência promovida pelo Presidente da República 4 e 5 de março de 2005, no Centro Cultural de Belém, 2005, Lisboa. Disponível em: http://eco.imooc.uab.pt/elgg/file/download/51670

COMISSÃO EUROPEIA. ***Adequacy decision.*** *How the EU determines if a non-EU country has na adequate level of data protection.* Decisões de adequação para consulta. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt

COMISSÃO EUROPEIA. **Decisão de execução (ue) 2021/914 da Comissão de 4 de junho de 2021** relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021D0914&from=PT

COMITÉ EUROPEU DE PROTEÇÃO DE DADOS. **Recomendações 01/2020** relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE Versão 2.0 Adotado em 18 de junho de 202, p. 3. Disponível em: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_pt.pdf

JORNAL OFICIAL DAS COMUNIDADES EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Jornal Oficial das Comunidades Europeias, L 281, 23 de novembro de 1995, Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L:1995:281:TOC

JORNAL OFICIAL DAS COMUNIDADES EUROPEIA. Decisão da Comissão 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América, publicado no Jornal Oficial das Comunidades de 25 de agosto de 2000. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=PT

JORNAL OFICIAL DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 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 que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, pp. 1–88). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

MENEZES CORDEIRO. ***Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,*** Almedina, Coimbra, 2021, p. 331.

SCHRODER. **Anotação ao artigo 44.º do RGPD em Kuhling/Buchner**, Rn.24., in MENEZES CORDEIRO. *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, Coimbra, 2021, p. 321, nota de rodapé 21.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção) de 6 de outubro de 2015. Maximillian Schrems contra Data Protection Commissioner. Pedido de decisão prejudicial apresentado pela High Court (Irlanda). Processo C-362/14. Disponível: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62014CJ0362

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020. Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems. Pedido de decisão prejudicial apresentado pela High Court (Irlanda)
C-311/18 - Facebook Ireland e Schrems. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-311/18&language=PT

Alexa: Há Relação Entre Privacidade e Proteção de Dados a Partir da Inviolabilidade do Domicílio? Uma Análise Comparada Entre Estados Unidos e Brasil

Isadora Formenton Vargas[26]

RESUMO

Busca-se verificar, a partir de uma análise comparada entre Estados Unidos e Brasil, se o sistema jurídico brasileiro encontra-se suficiente tanto em termos normativos quanto jurisprudenciais para casos que envolvam novas formas de violação do domicílio, como, por exemplo, por sensores de captação. Para isso, a pesquisa divide-se em duas partes. Na primeira, considerando que a Suprema Corte dos Estados Unidos já enfrentou casos que envolvam essa temática, partindo-se da Quarta Emenda à Constituição dos Estados Unidos, busca-se identificar o fundamento da inviolabilidade de domicílio e da descarga argumentativa proposta em duas oportunidades: Katz v. Estados Unidos 389 U.S. 347 (1967), e Kyllo v. Estados Unidos, 533 U.S 27 (2001). Na segunda parte, de forma comparada, busca-se analisar, a partir do art. 5º, inciso XI da Constituição Federal, o fundamento da inviolabilidade do domicílio e a argumentação proposta no Recurso Extraordinário nº 603.616/RO (2015) e no Habeas Corpus nº 444.024/PR (2019). A hipótese de pesquisa centra-se na identificação da privacidade como fundamento à inviolabilidade do domicílio, para enfrentar novas situações de desenvolvimento tecnológico e a proteção de dados.

PALAVRAS-CHAVE:

Inviolabilidade do domicílio. Privacidade. Proteção de dados. Desenvolvimento tecnológico.

[26] Mestre em Direito pela Universidade Federal do Rio Grande do Sul. Mestre em Argumentação Jurídica pela Universidade de Alicante (ESP) e de Palermo (ITA). Integrante do Comitê Permanente de Proteção de Dados Pessoais do Tribunal de Justiça do Estado do Rio Grande do Sul. Assessora Superior na Assessoria Especial Administrativa do Tribunal de Justiça do Estado do Rio Grande do Sul.

Alexa, Is There a Relationship Between Privacy and Data Protection from the Inviolability of the Domicile? A Compared Analysis Between the United States and Brazil

Isadora Formenton Vargas

ABSTRACT

From a comparative analysis between the United States and Brazil, the aim is to verify if the Brazilian legal system is sufficient in both normative and jurisprudential terms for cases involving new forms of domicile violation, such as, for example, by sensors. of capture. For this, the research is divided into two parts. In the first, considering that the United States Supreme Court has already faced cases involving this issue, based on the Fourth Amendment to the United States Constitution, identify the basis of the inviolability of domicile and the proposed argumentative discharge on two occasions: Katz v. United States, 389 U.S. 347 (1967), and Kyllo v. United States, 533 U.S. 27 (2001). In the second part, comparatively, analyze, from art. 5, item XI of the Federal Constitution, the grounds of inviolability of the domicile and the arguments proposed in Extraordinary Appeal No. 603.616/RO (2015) and Habeas Corpus No. 444.024/PR (2019). The research hypothesis focuses on the identification of privacy as a basis for the inviolability of the home, to face new situations of technological development and data protection.

KEYWORDS

Inviolability of the domicile. Privacy. Data protection. Technological development.

Introdução

A temática que envolve o presente estudo se refere aos novos desafios impostos aos direitos fundamentais com o desenvolvimento tecnológico. Atribui-se enfoque à descarga argumentativa no âmbito da jurisprudência da Suprema Corte dos Estados Unidos, voltada ao estabelecimento de critérios a novas situações de afronta à inviolabilidade do domicílio, consubstanciada na Quarta Emenda à Constituição dos Estados Unidos. A partir disso, busca-se identificar tal direito fundamental sob uma perspectiva comparada, entre Estados Unidos e Brasil, levando-se em consideração o aperfeiçoamento tecnológico de sensores e ferramentas de busca em geral.

Tratando-se de comparação entre sistemas jurídicos, importante registro dogmático deve ser realizado. Em que pese o sistema jurídico estadunidense seja considerado de *common law* e o brasileiro, *civil law*, a eleição pelo primeiro deve-se ao fato de haver uma constituição escrita[27] onde há previsão expressa, na Quarta Emenda à Constituição dos Estados Unidos, quanto à inviolabilidade de suas pessoas, casas, papéis, busca e apreensão arbitrárias. No Brasil, passa-se o mesmo, uma vez que o art. 5º, inciso XI, da Constituição da República Federativa do Brasil, estabelece que "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial". Em complementação, também prevê o art. 5º, inciso XII, da CRFB, a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, respeitadas suas exceções, além da proteção à intimidade e à vida privada, à honra e à imagem das pessoas, conforme inciso X do mesmo artigo.

Também, importa referir que, embora a pesquisa confira enfoque a dois casos julgados pela Suprema Corte, tratando-se de um sistema baseado em precedentes, torna-se inevitável citar, mesmo de forma indireta, outros casos relacionados. Isso se deve à formação de teorias jurídicas que são aplicadas e replicadas nos casos tratados.

Assim, a partir da experiência norte-americana, com a análise dos casos Katz v. Estados Unidos 389 U.S. 347 (1967) e Kyllo v. Estados Unidos, 533 U.S 27 (2001), que versam sobre a necessidade de se pensar a inviolabilidade de domicílio desconexa da propriedade tangível e atualizada às inovações tecnológicas, surge a oportunidade de reflexão acerca não só da privacidade, como também da proteção de dados. Com isso, surgem as bases necessárias para, centrando-se nas razões apresentadas pelo STF no Recurso Extraordinário nº 603.616/RO (2015) e pelo STJ, no Habeas Corpus nº 444.024/PR (2019), identificar uma racionalidade argumentativa capaz de identificar no âmbito brasileiro, a inviolabilidade de domicílio com o desenvolvimento tecnológico.

[27] Como refere Gregório Assagra de Almeida: "Esse também é um aspecto complexo e de difícil assimilação nos Estados Unidos, ainda mais com a adoção do sistema da common law, que confere força jurídica vinculante aos precedentes judiciais, ao mesmo tempo em que regras legisladas pelos tribunais (rules), leis criadas pelo legislativo (statutes), competências federal e estaduais amplas e uma Constituição bem sintética" (2016, p. 08).

1 Inviolabilidade do domicílio por novas tecnologias nos estados unidos

1.1 A quarta emenda à constituição dos estados unidos

Stephen Schulhofer identifica na obra *More Essential Than Ever: The Fourth Amendment in the Twenty-First Century* (2012) relevante ponto de partida para que se possa falar em inviolabilidade do domicílio: geralmente, há um descontentamento dos cidadãos em relação a decisões jurídicas que reconheçam a ilegalidade ou inconstitucionalidade de operação policial com base na inviolabilidade do domicílio, sobretudo quando algo de fato foi encontrado, no caso, uma conduta criminosa, ou seja, escolhida pelo Direito como tal.

Há uma concepção leiga, sob o ponto de vista jurídico, de que questões meramente "técnicas" não deveriam obstar operações em prol da segurança pública. No entanto, justamente em razão dos equívocos em torno da inviolabilidade do domicílio, que se nutrem, em grande parte, de um contexto social de insegurança pública e nacional, Schulhofer atribui à sua obra o título "mais essencial do que nunca" falar-se a respeito da Quarta Emenda.

Como refere Schulhofer, a Quarta Emenda "oferece um abrigo contra invasões governamentais injustificadas, que perturbam nossa paz de espírito e nossa capacidade de prosperar como cidadãos independentes em uma vibrante sociedade democrática"[28] (SCHULHOFER, 2012, p. 03). Assim, em tempos nos quais: (i) a liberdade de expressão é censurada institucionalmente[29] e o Ex-Secretário da Cultura brasileiro, Roberto Alvim, parafraseia o Ministro Ministro da Propaganda na Alemanha Nazista, Joseph Goebbels (BBC, 2020, *online*); (ii) se questiona o direito à privacidade, sob o fundamento de que não se tem nada a esconder; (iii) em 2019, no Rio de Janeiro, o número de mortes por intervenção de agente do Estado alcança o maior índice desde o início da série histórica (1988), de acordo com o Instituto de Segurança Pública (G1, 2019, *online*), a obra de Schulhofer ecoa de forma intensa no contexto brasileiro.

Nesse sentido, a Quarta Emenda à Constituição dos Estados Unidos foi introduzida na Declaração de Direitos, *Bill of Rights,* em 1789, cuja versão final foi proposta por James Madison, assim redigida:

> EMENDA IV: O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas[30].

---

[28] Tradução livre de: "It offers a schelter from governmental intrusions that unjustifiably disturb our peace of mind and our capacity to thrive as independent citizens in a vibrant democratic society".

[29] Como, por exemplo, a censura pelo Desembargador Benedicto Abicair, da 6ª Câmara Cível do Rio de Janeiro, ao deferir pedido de tutela antecipada para determinar a suspensão do Especial de Natal Porta dos Fundos "A primeira tentação de Cristo", em 08 de janeiro de 2020. A decisão foi revogada pelo Ministro do Supremo Tribunal Federal, Dias Toffoli, em 09 de janeiro de 2020.

[30] Tradução livre de: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

Originalmente, a Quarta Emenda fortalece a noção de que "a casa de todo homem é seu castelo", frase atribuída a quem foi considerado o maior jurista das eras elisabetana e jacobina (BAKER, 2002), Edward Coke (1552-1634), que identificou esse direito pela primeira vez, em 1604 (SWINDLE, 2013). De acordo com Swindle, Coke referiu que "a casa é para todos como um castelo e fortaleza, servindo tanto à defesa contra ferimentos e violência, quanto para seu repouso"[31] (SWINDLE, 2013).

A história da Quarta Emenda guarda relação com a era colonial, com a cobrança de impostos dos colonos, que iniciaram a contrabandear produtos para evitar o pagamento das taxas impostas pela Coroa Britânica. Em resposta, o Rei George utilizou-se de *Writs of Assistance*, um instrumento semelhante a um mandado legal de busca, extremamente amplo, que permitia aos agentes da Coroa, com assistência de cidadãos - daí porque o termo -, toda e qualquer forma de ingresso na propriedade ou na casa de alguém (SWINDLE, 2013).

O abuso da Coroa consistente nos *Writs of Assistance*, teria sido um dos catalisadores da luta pela Independência dos Estados Unidos (THAI, 2006, p. 1752). Como refere Cunningham, nos termos de John Adams, segundo presidente dos Estados Unidos (1797-1801), "a criança da Independência nasceu" em 1761 (CUNNINGHAM, 2016, p. 221), "quando James Otis apresentou uma petição *pro bono* em nome de um grupo de cidadãos de Boston que se opunha à emissão de mandados de assistência"[32] (CUNNINGHAM, 2016, p. 221). De acordo o resumo dos argumentos apresentados à Corte Superior de Boston, Otis refere que os *Writs of Assistance* constituem "o pior instrumento do poder arbitrário, o mais destrutivo da liberdade inglesa e dos princípios fundamentais da Constituição"[33] (ADAMS PAPER, 1761).

Interessante observar que a ideia de que a Quarta Emenda protege a privacidade contra ações arbitrárias do Estado foi desenvolvida pela Suprema Corte em 1886, com o caso Boyd v. Estados Unidos (116 U.S 616), com a interpretação conjunta da Quinta Emenda[34] (SOLOVE, 2004, p. 63). Note-se que o precedente reconhece essa privacidade somente em relação ao Estado. Assim, a expectativa de privacidade surge antes no âmbito público e depois oponível entre privados, uma vez que a primeira menção à privacidade, sob a perspectiva privada, surge no artigo, *The Right to Privacy*,

---

UNITED STATES OF AMERICA. CONSTITUTION. Disponível em: https://www.law.cornell.edu/constitution/fourth_amendment. Acesso em: 18 jan. 2020.

[31] Tradução livre de: "The house of everyone is to him as his castle and fortress, as well for his defence against injury and violence as for his repose."

[32] Tradução livre de: "(...) when James filed a petition pro bono on behalf of a group of Boston citizens opposing issuance of writs of assistance."

[33] Tradução livre de: "(...) the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of the constitution."

[34] Tradução livre de: "Nenhuma pessoa deve ser responsabilizada por um crime capital ou de outro tipo infame, a menos que seja apresentada ou indiciada por um grande júri, exceto nos casos que surjam nas forças terrestres ou navais ou na milícia, quando em serviço real em tempo de guerra ou perigo público; nem qualquer pessoa será sujeita ao mesmo crime duas vezes em risco de vida ou de membro; nem será obrigada, em qualquer caso criminal, a ser uma testemunha contra si mesma, nem ser privado da vida, liberdade ou propriedade, sem o devido processo legal; nem a propriedade privada será tomada para uso público, sem justa compensação ". UNITED STATES OF AMERICA. CONSTITUTION. Disponível em: https://www.law.cornell.edu/wex/fifth_amendment. Acesso em: 18 jan. 2020.

de Samuel Warren e Louis Brandeis em 1890. Ademais, o fundamento de privacidade da Quarta Emenda é visto por Jeremy Waldron como argumento normativo na filosofia política baseada na teoria dos direitos, uma vez que representa a liberdade de se viver a vida nos próprios termos, circunstância que deve ser respeitada, tendo em vista que é necessária à vida em sociedade:

> Não se esperaria encontrar proposições como a Quarta Emenda à Constituição dos EUA nos fundamentos de uma teoria dos direitos. O direito à proteção da casa contra buscas irracionais provavelmente se baseará na importância oferecida a um interesse individual mais profundo, como a privacidade. O direito à privacidade, por sua vez, pode basear-se em premissas ainda mais profundas sobre a importância da autonomia e de viver a vida nos próprios termos. Conclusões derivadas serão então geradas pela elaboração do que é necessário nas circunstâncias da sociedade moderna para que os interesses mais profundos desta série sejam respeitados. Isso representa o argumento normativo na filosofia política baseada na teoria dos direitos[35]. (WALDRON, 1999, p. 215).

Consolidada como instrumento de liberdade negativa, contra a intervenção do Estado, a Quarta Emenda ultrapassou as fronteiras territoriais, influenciando o Direito Internacional, bem como ordenamentos de outros países. Muitas declarações de Direito derivam dessa compreensão. O art. 12, da Declaração Universal dos Direitos do Homem, de 1948, indica que "ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques" (ONU, 1948). Ademais, também na Convenção Americana de Direitos Humanos e no Pacto de Direitos Civis e Políticos.

Com o aumento da vigilância pelo Estado, em razão da "luta contra o terrorismo", sobretudo após os ataques de 11 de Setembro, acompanhado do desenvolvimento tecnológico, resultou na expedição de robustas ferramentas legais para interceptar comunicações eletrônicas, Patriot Act. Ademais, esse contexto social e político foi responsável por gerar uma onda de medo, de modo que "muitos cidadãos estão convencidos de que é melhor ceder algumas liberdades em prol da minimização dos riscos de um potencial ataque catastrófico"[36] (SCHULHOFER, 2012, p. 04), de modo que as liberdades civis resguardadas pela Quarta Emenda ganham peso distinto para a sociedade a dependender de circunstâncias externas, cabendo à Suprema Corte o sopesamento entre tais liberdades, de um lado, e segurança nacional, de outro.

---

[35] Tradução livre de: "One would not expect to find propositions like the Fourth Amendment to the US Constitution in the foundations of a theory of rights. A right to he protection of one's home against unreasonable searches is likely to be based on the importance afforded to a deeper individual interest such as privacy. A right to privacy may in turn be based on even deeper premises about the importance of autonomy and living life on one's own terms. Derivative conclusions will then be generated by working out what is required in the circumstances of modern society if the deepest interests in this series are to be respected. That is what normative argument amounts in right based political philosophy".

[36] Tradução livre de: "Many citizens are convinced that it is best to give up certain liberties in order to minimize the risk of potentially catastrophic attack."

1.2 Do caso katz v. estados unidos, 389 u.s. 347 (1967), ao kyllo v. estados unidos, 533 u.s 27 (2001)

Em relação a desenvolvimento tecnológico e alcance da Quarta Emenda, inevitável a abordagem do caso Katz v. Estados Unidos (389 U.S 347), julgado pela Suprema Corte, em 1967. Em breve menção aos fatos, o jogador de basquete e apostador, Charles Katz, dirigia-se com frequência a uma cabine telefônica pública, próxima do seu apartamento em Los Angeles, Califórnia, para fornecer apostas a casas de jogos de azar.

O Federal Bureau of Investigation (FBI) implantou um dispositivo de escuta oculto, na parte externa da cabine, e, assim, interceptou as ligações telefônicas. Katz foi preso e acusado de transmitir informações sobre apostas, em violação à Lei Federal (18 USC § 1084). Ao recorrer, Katz alegou que a operação constituía "busca e apreensão", exigindo, para tanto, autorização judicial, mesmo na ausência de ingresso físico na cabine, além de violação à privacidade. O FBI, por sua vez, defendia a inexistência de entrada física, de modo que a operação não gerava afronta à Quarta Emenda (389 U.S 348).

Ao ser julgado pela Suprema Corte, o caso Katz resultou na superação do entendimento tradicional de que "busca", para a Quarta Emenda, consistiria, apenas, na proteção da propriedade tangível, amparada na Teoria da Transgressão, que possuía como precedente o caso Olmstead v. Estados Unidos (277 U.S 438 - 1928). Com o caso Katz, estabeleceu-se a compreensão central de que a Quarta Emenda protege pessoas, e não lugares, como manifestou o Juiz Potter Stewart, responsável pelo voto ao qual a maioria da Suprema Corte aderiu, com fundamento na "expectativa de privacidade".

Relevante mencionar-se o voto do Juiz John Marshall Harlan, que apresentou voto de provimento a Katz, mas com o estabelecimento do teste de duas partes, conhecido por Teste Katz, no sentido de que há um duplo requisito à referida expectativa de privacidade (FROH, 2003, p. 341). Primeiro, de que seja real (subjetiva); segundo, de que seja reconhecida pela sociedade como razoável (398 U.S 361). O único voto dissidente partiu do Juiz Hugo Black, que argumentou no sentido de que a Quarta Emenda se destina apenas à proteção de "coisas", e não para proteger a privacidade.

Assim, o caso Katz também foi responsável por gerar os primeiros passos da doutrina de terceiros (Third-Party Precedent), consolidada pelos casos julgados em 1976 e em 1979, Estados Unidos v. Miller (425 U.S 435) e Smith v. Maryland (442 U.S 735), respectivamente. A teoria consiste em não considerar legítima a expectativa de privacidade daqueles que conscientemente disponibilizam dados a terceiros, de modo que não seria objeto de proteção da Quarta Emenda. O caso Katz prenuncia essa tendência, mas também afirma que aquilo que se procura preservar como privado, mesmo em uma área acessível a público, deveria ser protegido (389 U.S 352 e 353).

Após Katz e antes de Kyllo, muitos casos interessantes foram apreciados pela Suprema Corte, havendo a confirmação da expectativa de privacidade, embora se admita que o Teste Katz tenha sido responsável por gerar muita confusão quanto ao que constituiria uma expectativa "razoável" de privacidade (FROH, 2003, p. 342). De

acordo com Amanda Froh, com base no caso Kyllo, a dificuldade geral de aplicação surge quando a busca ocorre em lugares que não são vistos como "áreas constitucionalmente protegidas", tais como agendas telefônicas, veículos, áreas descobertas em residências (FROH, 2003, p. 342).

Apenas para verificar a relevância, cita-se o caso Califórnia v. Ciraolo, 476 U.S. 207 (1986), que pode ser facilmente pensado em um contexto de vigilância estatal por aeronaves remotamente pilotadas (drones). Nessa oportunidade, pareceu haver um lapso na aplicação do precedente de Katz, uma vez que a Corte determinou que o uso de um avião privado pela polícia, implantado com câmeras de vigilância por vídeo, não constituía uma "busca", prescindindo, portanto, da expedição de um mandado de busca e apreensão, vindo a considerar lícita a operação que captou plantação de cannabis em um quintal, sob o fundamento central de que a operação foi realizada dentro do "espaço público aéreo navegável"[37]. No entanto, parece razoável entender que essa afirmação consequente não elimina a expectativa legítima de privacidade.

Ann Cavoukian, responsável pela teoria Privacy By Design, privacidade desde a concepção, ao tratar sobre drones e privacidade (CAVOUKIAN, 2012), refere, especialmente ao analisar os precedentes da Suprema Corte, que as expectativas individuais acerca da privacidade tendem a mudar na medida em que as tecnologias de vigilância se tornam mais difundidas. Ann indica que em 2011, no caso Estados Unidos v. Jones (565 U.S 400), por unanimidade, a Suprema Corte considerou que a implantação pela polícia, sem mandado, de um GPS em um automóvel, para fins de rastreamento, violava as garantias da Quarta Emenda (CAVOUKIAN, 2012, p. 11), de modo que o Tribunal reconheceu que os mandados judiciais podem representar meios constitucionalmente exigíveis para proteção da privacidade geradas pelo uso de tecnologias de vigilância sofisticadas, inclusive em espaços públicos.

O caso Kyllo v. Estados Unidos, 533 U.S 27 (2001), contribuiu ao estabelecimento de quatro perguntas-teste para situações que envolvam a dualidade desenvolvimento tecnológico, de um lado, e interpretação da Quarta Emenda, de outro, como prolongamento do Teste de Katz. Como refere Froh, os quatro fatores primários não estão definidos especificamente no acórdão de Kyllo, mas cada um deles é mencionado para levar à conclusão obtida (FROH, 2003, p. 342).

Ademais, a partir de Kyllo, restringiu-se a doutrina de terceiros (Third-Party Doctrine) às formas avançadas de vigilância (THAI, 2006, p. 1752), aproximando a temática à proteção de dados. Basicamente, como pontua Joseph Thai, o caso Kyllo "destacou o papel fundamental que desempenha a Quarta Emenda na proteção de

[37] A título de curiosidade, em matéria de responsabilidade civil, o mesmo argumento de "espaço público navegável" foi utilizado pelo Ministério de Defesa francês em caso envolvendo propriedade e espaço aéreo. Em 24 de agosto de 2010, aviões militares sobrevoaram a uma altitude baixa a fazenda de um avicultor em Pléguien, na região de Bretanha, gerando ruídos tão intensos que causaram a morte de 4.800 galinhas. Não foi necessário adentrar no âmbito da intencionalidade, bastando a comprovação do nexo causal entre as mortes das galinhas e o ruído pela autópsia dos animais. Assim, o Ministério de Defesa francês pagou uma indenização de noventa mil euros ao fazendeiro, montante que engloba não só a morte das aves, como também o prejuízo decorrente da redução na produção e na diminuição da qualidade dos ovos após o ocorrido. Disponível em: <https://www.ouest-france.fr/bretagne/saint-brieuc-22000/4-800-poules-mortes-de-peur-pleguien-cotes-darmor-536409>. Acesso realizado: 03 jan. 2020.

nossas atividades dos olhares indiscretos do governo, mesmo quando a tecnologia nos torna impotentes para excluir os olhares indiscretos dos outros"[38] (THAI, 2006, p. 1735).

Quanto aos fatos, a partir da suspeita de que Danny Kyllo estava cultivando cannabis em sua residência, agentes da polícia utilizaram um sensor térmico para captar o calor que irradiava da sua casa, sem a expedição de mandado de busca e apreensão. Percebeu-se que a residência de Kyllo, especialmente na garagem e na parte lateral, emanava calor em quantidade muito superior em relação ao restante da casa e às demais residências da rua. Com isso, a hipótese refere-se à necessidade de grande quantidade de luz para a ocorrência de fotossíntese destinada ao cultivo da cannabis. Essas informações foram utilizadas à obtenção posterior de mandado de busca e apreensão, que foi concedido judicialmente, resultando na apreensão da droga e na prisão de Kyllo (533 US 27).

Kyllo recorreu, levando o caso à Suprema Corte. Os fundamentos não são novos, e referem-se, de um lado, à expectativa de privacidade, à confirmação do entendimento de que a Quarta Emenda não exige a invasão física da propriedade. Assim como em Katz em relação às ondas sonoras, as ondas térmicas não são visíveis a olho nu, mas a partir do dispositivo, a radiação é convertida em imagens que possuem coloração de acordo com o calor emitido. De outro lado, os Estados Unidos argumentaram que a captação de calor não era capaz de detectar "detalhes íntimos", de modo que não haveria violação à referida expectativa de privacidade, bem como que Kyllo não tentava manter a informação privada. A questão jurídica central consistia em saber se o dispositivo de imagem térmica utilizado para captar, a partir de uma via pública, o calor emanado por uma residência, constituiria "busca" na acepção da Quarta Emenda.

Em acirrado julgamento, com resultado de 5 a 4, concluiu-se que a captação de imagem térmica da casa de Kyllo constituía busca, para fins da exigência prévia de mandado judicial. O Magistrado Antonin Scalia proferiu o voto majoritário, com a ratificação dos precedentes que, desde Katz, reconheciam a expectativa razoável de privacidade. Didaticamente, os quatro fatores para se analisar a existência dessa expectativa de forma que se possa acompanhar o desenvolvimento tecnológico, com a manutenção da interpretação atualizada da Quarta Emenda pela jurisprudência, são as seguintes: (i) a técnica melhora os sentidos; (ii) a intromissão é realizada em área tradicionalmente associada à privacidade pessoal, como uma casa; (iii) o tipo de dispositivo ou técnica em questão geralmente não está disponível ao público, e, por último, (iv) a informação só poderia ser obtida com a invasão física na área, se não fosse o auxílio do dispositivo (FROH, 2003, p. 349).

Se as respostas foram positivas, entende-se que há afronta à Quarta Emenda. Em contrapartida, em voto dissidente, do Juiz Paul Stevens argumentou que qualquer pessoa poderia detectar as emissões de calor. Para corroborar seu argumento, Stevens referiu que a área onde havia concentração de calor poderia gerar o derretimento de gelo mais rapidamente, de modo que o público em geral poderia reunir essas informações sem a expedição de mandado de busca e apreensão (533 U.S 42-43).

[38] Tradução livre de: "(...) Kyllo v. United States, which underscored the fundamental role that the Fourth Amendment plays in protecting our private activities from the prying eyes of the government, even when technology renders us helpless to exclude the prying eyes of others."

Basicamente, a teoria de fundo sobre a qual Stevens estava se amparando consistia na distinção entre "fora da parede" e "através da parede". Ele e os demais magistrados que acompanharam o voto dissidente argumentaram que a vigilância consistia em "fora da parede", porque não detectou nada íntimo (533 U.S 41). O magistrado Scalia refere que essa distinção é incompatível com o caso, uma vez que a maioria dos dispositivos de imagem térmica continuam a medir calor "fora da parede", de modo que, assim como em Katz, essa interpretação mecânica da Quarta Emenda deveria ser afastada (533 U.S 35).

Em síntese, os casos analisados demonstram que situações novas que envolvem desenvolvimento de sensores e artefatos tecnológicos exigem do intérprete, em matéria de inviolabilidade do domicílio, um fundamento central de expectativa de privacidade. Caso esse fundamento fosse inexistente, dificilmente a argumentação resultaria na conclusão de necessidade de expedição de mandado de busca e apreensão. Os precedentes da Suprema Corte seguem as razões expostas, que iniciam com a superação da propriedade tangível, além de uma interpretação histórica da Quarta Emenda, relacionada à proteção da liberdade individual perante as arbitrariedades do Estado, culminando no teste Katz, cujo fundamento se centra na expectativa de privacidade.

Vale ressaltar que, a partir de Kyllo, houve um enfraquecimento da doutrina de terceiros, quanto à disponibilização consciente de informações a terceiros, de modo que haveria dispensa de expedição de mandado de busca e apreensão. Com o desenvolvimento da tecnologia em matéria de dados, tornou-se difícil - o que foi compreendido pela Corte - determinar o que seria uma exposição consciente de dados pessoais. Joseph Thai, em artigo publicado em 2006, justamente pretende responder à questão: mineração de dados sempre consiste em "busca" sob a Quarta Emenda de Steven?

Ademais, na linha do presente estudo, relevante aporte teórico recrudesce a compreensão aqui desenvolvida. Stephen Schulhofer, já citado, quanto à importância, "mais essencial do que nunca", de se falar da Quarta Emenda no século XXI, logo no início da sua obra, afirma:

> As ameaças à privacidade mudaram enormemente ao longo dos séculos. Mas a importância da privacidade para o bem-estar dos indivíduos e para o florescimento da democracia não diminuiu em nada. As salvaguardas da Quarta Emenda foram aprimoradas por séculos - garantias, restrições à discrição, supervisão e prestação de contas - tornaram-se, se alguma coisa, cada vez mais necessárias. Longe de se tornarem obsoletas, elas são mais essenciais do que nunca no mundo da alta tecnologia do século XXI (SCHULHOFER, 2012, p. 21)[39].

Importa fazer referência ao encaminhamento recente da jurisprudência da Suprema Corte. Isso porque, assim como iniciado em Kyllo, a doutrina de terceiros tem sido enfraquecida, culminando, inclusive, em previsões legais para além da

[39] Tradução livre de: "The threats to privacy have changed enormously over centuries. But the importance of privacy to the well-being of individuals and to the flourishing of democracy has not diminished in the least. Fourth Amendment safeguards that have been honed for centuries - warrants, constraints on discretion, oversight, and accountability - have become, if anything, increasingly necessary. Far from being obsolete, they are more essential than ever in the high-tech world of the twenty-first century.

jurisprudência. Em recente e histórico caso, Carpenter v. Estados Unidos (585 U.S __)[40], julgado em 2018, a Suprema Corte considerou, em uma decisão de 5 a 4, com voto majoritário do Juiz Roberts, que o acesso a registros históricos contendo as localizações físicas de telefones celulares constituem "busca", de acordo com a Quarta Emenda, exigindo-se, previamente, a expedição de mandado de busca e apreensão.

Embora o caso Carpenter tenha sido bastante restrito, no sentido de não possuir o condão de superar a doutrina de terceiros nem de anular casos anteriores, a tendência apresentada pela Corte, como bem pontua Orin Kerr, permite que as razões jurídicas expostas em Carpenter sejam aplicadas, de forma geral, aos registros de internet quando três requisitos forem atendidos: (i) os registros existem em razão da era digital, (ii) foram criados sem "escolha voluntária significativa", e (iii) tendem a revelar esferas da vida privada (KERR, 2018, p. 01).

Assim, a Quarta Emenda na era digital e virtual parece estar se aproximando da temática da proteção de dados, lançando luz sobre questões jurídicas que envolvem essa matéria, como, por exemplo, a temática do consentimento. O caso Carpenter representa uma vitória à garantia das liberdades civis, sendo considerada pela Corte uma das decisões mais importantes desta geração (NEW YORK TIMES, 2019, online), e será influente nas próximas decisões da Corte.

No entanto, não foi capaz de livrar o acusado Carpenter da prisão, que foi sentenciado a 116 anos de prisão em junho de 2019, por um Tribunal Federal. Embora os advogados de Carpenter tenham argumentado que os dados de rastreamento do celular deveriam estar sujeitos à regra de exclusão, os juízes entenderam que o FBI estava agindo de boa-fé (NEW YORK TIMES, 2019, online). Critério que já havia sido aplicado pela Suprema Corte em 2011, no caso Davis v. Estados Unidos (564 U.S 229), com a tese de que a boa-fé afasta a regra de exclusão.

Na esteira das conclusões de Kerr, entende-se que os tribunais devem desenvolver novas regras para reequilibrar as proteções da Quarta Emenda. Como refere o autor, "precisam fazer isso de maneira abrangente, em vários casos diferentes. O resultado deve ser um novo corpo de novas regras específicas a computadores, criadas pelos tribunais apenas para buscas computacionais" (KERR, 2016).

Por fim, a título exemplificativo, como consequência do caso Carpenter, pode-se citar a primeira lei destinada à proteção de dados eletrônicos privados armazenados por terceiros, com a determinação da necessidade de expedição de mandado para acesso pelo Estado (FORBES, 2019, online), como superação legal da doutrina de terceiros. Trata-se da Lei de Privacidade de Dados ou Informações Eletrônicas[41], aprovada pelo estado de Utah, em 2019.

---

[40] "Casos mais recentes de volumes futuros subsequentes ainda não têm números de páginas oficiais e geralmente usam três sublinhados no lugar do número de página; por exemplo, *Salman v. Estados Unidos*, 580 U.S ___ (2016). Nesses casos, o número do boleto - geralmente dois dígitos, um hífen e o número do caso de 1 a 4 dígitos - é usado; por exemplo, *Salman v. Estados Unidos* , 15-628. Se uma citação de caso em um volume após 570 for mostrada com um número de página, o número da página será *baseado em relatórios não oficiais e estará sujeito a alterações quando a decisão for encadernada e impressa* ." O número provisório de Carpenter v. Estados Unidos é 16-402. Disponível em: https://en.wikipedia.org/wiki/List_of_United_States_Supreme_Court_cases,_volume_585. Acesso em 13 jan. 2020.

[41] Electronic Information or Data Privacy Act - HB 57.

2 Proposta de argumentação jurídica para casos semelhantes no brasil

2.1 O STF no recurso extraordinário nº 603.616/ro (2015), e o STJ no habeas corpus nº 444.024/pr (2019)

O Recurso Extraordinário nº 603.616/RO, Tema 280 da sistemática de repercussão geral, de relatoria do Ministro Gilmar Mendes, foi paradigmático, uma vez que, a partir dele, o Supremo Tribunal Federal alterou sua jurisprudência. Até então, o STF entendia que, "se dentro da casa está ocorrendo um crime permanente, é viável o ingresso forçado pelas forças policiais, independentemente de determinação judicial (RHC 91.189, Rel. Min. Cezar Peluso, Segunda Turma, julgado em 9.3.2010; RHC 117.159, Relator Min. Luiz Fux, Primeira Turma, julgado em 5.11.2013; RHC 121.419, Relator Min. Ricardo Lewandowski, Segunda Turma, julgado em 2.9.2014)" (BRASIL, 2015, p. 11).

O Tema 280 referiu-se a "provas obtidas mediante invasão de domicílio por policiais sem mandado de busca e apreensão". Por maioria, em 05 de novembro de 2015, foi fixada a seguinte tese:

> A entrada forçada em domicílio sem mandado judicial só é lícita, mesmo em período noturno, quando amparada em fundadas razões, devidamente justificadas *a posteriori*, que indiquem que dentro da casa ocorre situação de flagrante delito, sob pena de responsabilidade disciplinar, civil e penal do agente ou da autoridade, e de nulidade dos atos praticados (TEMA 280, STF).

Inicialmente, importa destacar, o que será posteriormente analisado com mais detalhamento, dada a proposta argumentativa, de que o Supremo Tribunal Federal, ao analisar o enunciado normativo da inviolabilidade do domicílio, não considerou que "flagrante" consiste em limitação interna à inviolabilidade do domicílio, ou seja, a ocorrência de flagrante, por si só, de forma abstrata, não exime a verificação de excesso que implique afronta à inviolabilidade do domicílio. Isso se percebe no momento em que o Tribunal exige, na conclusão do julgamento, justificadas razões para tanto.

Inclusive, como consta na Ementa, afasta-se a falácia do consequente, no sentido de que "não será a constatação de situação de flagrância, posterior ao ingresso, que justificará a medida". Assim, o direito fundamental à inviolabilidade do domicílio não se encontra, a priori, limitado em situação de flagrância.

As razões recursais do recorrente consistem na alegação de violação ao art. 5º, incisos LVI e XI, da CRFB, quanto à inadmissibilidade das provas ilícitas e à inviolabilidade do domicílio, cuidando-se, quanto aos fatos, de apreensão e busca em domicílio, no período noturno, sem mandado judicial. No caso concreto, "o recorrente Paulo Roberto de Lima foi preso em flagrante, porque foram encontrados 8,542 Kg (oito quilos, quinhentos e quarenta e dois gramas) dentro de um veículo Ford Focus de sua propriedade, estacionado na garagem de sua residência" (BRASIL, 2015, p. 20).

Na espécie, quanto ao crime de tráfico de drogas, previsto no art. 33 da Lei 11.343/06, estando a droga depositada em uma determinada casa, o morador está em situação de flagrante delito, dada a natureza de crime permanente. Para busca e apreensão, por exemplo, o Código de Processo Penal exige apenas "fundadas razões", no art. 240, §1º[42]. De qualquer forma, para manter-se o recorte da pesquisa, não será

[42] Art. 240. A busca será domiciliar ou pessoal.

§ 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:

atribuído enfoque às questões penais específicas, e sim à superação, conforme indica o Ministro Gilmar Mendes, do entendimento de que "ao respeitar a literalidade do texto constitucional, que simplesmente admite o ingresso forçado em caso de flagrante delito, contraditoriamente estamos fragilizando o núcleo essencial dessa garantia" (BRASIL, 2015, p. 13). O Ministro Gilmar Mendes, cujo voto foi acompanhado, pela maioria, fez interessante retrospectiva histórica, citando a influência da Quarta Emenda no ordenamento jurídico brasileiro e de outros países, além das exceções previstas no direito comparado, bem como a consolidação em tratados e convenções internacionais dos quais o Brasil é signatário.

O Ministro Relator ratifica que "o papel do mandado judicial como garantia do respeito à privacidade é evidente" (BRASIL, 2015, p. 11), o que demonstra que a interpretação mecânica da inviolabilidade do domicílio prevista na CRFB tem gerado o afastamento dessa compreensão fundamental. Dessa forma, refere que "a proteção contra a busca arbitrária exige que a diligência seja avaliada com base no que se sabia antes de sua realização, não depois" (BRASIL, 2015, p. 13).

Em síntese, em que pese diversas questões que podem dificultar o problema jurídico, exemplificadas por Gilmar Mendes no voto, como bem pontua, "a tese é um avanço para a concretização da garantia. Com ela, estar-se-á valorizando a proteção, na medida em que será exigida justa causa, controlável a posteriori, para a busca" (MENDES, 2015, p. 20), como corolário do art. 5º, inciso XXXV, da CRFB, de que "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito" (BRASIL, 1988). Como contraposição, o Ministro Marco Aurélio divergiu, embora tenha sido vencido. Expõe em seu voto a preocupação de operações arbitrárias (BRASIL, 2015, pp. 56-58), assim como o Ministro Luiz Fux (BRASIL, 2015, p. 30), embora esse tenha acompanhado o Relator.

Embora paire certa insegurança jurídica diante do conceito indeterminado "fundadas razões", com o temor de extensão a operações arbitrárias. Como refere Isabel Lifante Vidal, a discricionariedade pode ser vista, além da indeterminação, como uma liberdade, negativa (permissão de decidir) e positiva (responsabilidade ao decidir),

---

a) prender criminosos;

b) apreender coisas achadas ou obtidas por meios criminosos;

c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;

d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;

e) descobrir objetos necessários à prova de infração ou à defesa do réu;

f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;

g) apreender pessoas vítimas de crimes;

h) colher qualquer elemento de convicção.

§ 2º Proceder-se-á à busca pessoal quando houver fundada suspeita de que alguém oculte consigo arma proibida ou objetos mencionados nas letras *b* a *f* e letra *h* do parágrafo anterior.

bem como um poder, atribuído formalmente e também quanto à avaliação de interesses envolvidos (LIFANTE, 2002, p. 430).

Nesse sentido, importa ressaltar que o Superior Tribunal de Justiça, ao apreciar "fundadas razões", para os casos de flagrante delito e violação do domicílio, tem apresentado importante direcionamento do Tema 280. No Habeas Corpus nº 496.420/SP, julgado em 2019, de relatoria da Ministra Laurita Vaz, foi concedida a ordem em favor do acusado, uma vez que as "fundadas razões" apresentadas pelos agentes consistiam, basicamente, em denúncia anônima. No entanto, a Ministra enfatizou que "as fundadas razões" devem ser compatíveis com a fase de obtenção das provas, de modo que, elementos que não têm força probatória em juízo, não servem para caracterizar as fundadas razões (BRASIL, 2019a).

Já o Habeas Corpus nº 444.024/PR, julgado em 2018 pelo Superior Tribunal de Justiça, de relatoria do Ministro Sebastião Reis Jr, e redatoria do Ministro Rogerio Schietti Cruz, aproxima-se de forma mais específica da hipótese de pesquisa do presente estudo. A relação entre privacidade, dados e inviolabilidade do domicílio é abordada, com interessantes direcionamentos através do Marco Civil da Internet (Lei nº 12.965/2014).

Quanto aos fatos, contra os impetrantes do Habeas Corpus foi instaurado inquérito policial para averiguar possível irregularidade na contratação de obra pública, realizada pela Concessionária da Rodovia Osório-Porto Alegre S.A - CONCEPA, a qual sem prévio procedimento licitatório. Quanto à necessidade da medida de busca e apreensão, assim referiu o Ministério Público Federal:

> [...] No caso em exame, os indícios relacionados pela autoridade policial em face dos investigados apontam a existência de fundadas razões para a autorização judicial de busca e apreensão nos locais (residências e sedes das empresas) indicados, mostrando-se a medida cautelar indispensável às investigações em curso, eis que com a diligência poderão ser obtidas provas essenciais à apuração dos delitos, tais como documentos e objetos, assim como dispositivos de armazenamento de dados, como computadores, telefones celulares, pen drives, entre outros similares, ou, ainda, outros elementos de convicção úteis à apuração das práticas ilícitas em toda sua extensão. (BRASIL, 2019b, p. 27).

Os impetrantes alegam, em síntese, três razões à concessão da ordem: incompetência da Justiça Federal de Porto Alegre; ausência de "fundadas razões" na decisão que determinou a busca e apreensão para o afastamento do direito fundamental à inviolabilidade do domicílio, e, a decisão que autorizou a apreensão de computadores, telefones celulares, notebooks, hard disk, pen-drives, CD's, DVD's e quaisquer outras mídias de armazenamento ou elementos que pudessem constituir prova da prática de crime não observou os requisitos das Leis n. 12.965/2014 (Marco Civil da Internet) e 9.296/1996 (Regulamenta o art. 5º, XII, da CRFB), o que ensejaria violação do direito fundamental ao sigilo de dados (BRASIL, 2019b, p. 28).

O Ministro Relator, cujo voto restou vencido, havia apresentado razões para a concessão, limitada, do Habeas Corpus. No entanto, por maioria, negou-se a ordem

aos impetrantes, com base no voto do Redator Rogerio Schietti Cruz. Relevante referir que questão reside na valoração da decisão jurídica que concedeu o mandado de busca e apreensão, ou seja, não se trata de caso em que a operação tenha sido realizada sem autorização judicial.

Basicamente, de um lado, o Ministro Relator entendeu que a decisão que autorizou a quebra de sigilo, quanto ao acesso do conteúdo dos equipamentos apreendidos, não indicou concretamente a impossibilidade de se prosseguir a investigação por outros meios, além de outros indícios razoáveis de autoria e de participação em infração penal (BRASIL, 2019b, p. 20). Ademais, o Relator ressaltou que a busca e a apreensão em realidade trouxe novas provas, cujas análises podem levar a conclusões diversas (BRASIL, 2019b, p. 21).

Para fundamentar seu voto, superada a preliminar de competência, o Relator apresentou os incisos II e III, do art. 7º do Marco Civil da Internet, quanto à inviolabilidade e sigilo do fluxo de comunicações pela internet e das comunicações privadas armazenadas, salvo por autorização judicial. Também indica que posicionamento diverso ao visto no caso Carpenter v. Estados Unidos (585 U.S __) tratado anteriormente, uma vez que a jurisprudência do STJ aponta para a licitude de "acesso a dados mantidos em aparelho celular diretamente por autoridades policiais, sem prévia autorização judicial (HC n. 392.466/CE, de minha relatoria, Sexta Turma, DJe 12/3/2018)" (BRASIL, 2019b, p. 18). Ainda, referiu que:

> Não obstante a ausência de lei específica delimitadora de quais seriam os requisitos para autorizar a quebra do sigilo dos aparelhos telefônicos apreendidos, tem este Tribunal se utilizado dos arts. 2º e 5º da Lei n. 9.296/1996 para dizer que só é admitida a quebra do sigilo quando houver decisão fundamentada, na qual se indique indício razoável da autoria ou participação em infração penal, se a prova não puder ser obtida por outro meio disponível, em atendimento ao princípio da proibição de excesso; e se o fato investigado constituir infração penal punida com pena de reclusão (RHC n. 67.379/RN, Ministro Ribeiro Dantas, Quinta Turma, DJe 9/11/2016). (BRASIL, 2019b, p. 18).

A partir do art. 10 do Marco Civil da Internet, o Ministro Relator ressalta o fundamento de proteção à privacidade e à intimidade, observado o art. 7º, o qual determina que o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial. Ressalta que o parágrafo único do art. 22, da Lei do Marco Civil da Internet, estabelece os seguintes requisitos à decisão judicial que autoriza a requisição de registros de conexão ou de acesso a aplicações de internet: (i) fundados indícios da ocorrência do ilícito; (ii) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e (iii) período ao qual se referem os registros (BRASIL, 2019b, p. 19).

Em síntese, o Ministro Relator entende que os requisitos expostos não estão presentes na decisão jurídica contra a qual se insurgem os impetrantes, e assim afirma quanto à legislação citada: "acredito eu que a ideia do legislador foi de proteção máxima à privacidade, regra constitucional com exceção possível apenas em razão de decisões judiciais fundamentadas e em casos excepcionais" (BRASIL, 2019b, p. 20).

Já o voto do Ministro Redator, de encontro às razões apresentadas pelo Relator, considerou suficientemente fundamentada a decisão de primeiro grau que concedeu o mandado de busca e apreensão, em consonância com o art. 240 do Código de Processo Penal. Refere, no entanto, ponto de partida fundamental à proposta do presente artigo:

> Decerto que determinadas informações, que se entrelaçam com aspectos ligados à personalidade, devem ser objeto de proteção em grau mais elevado. Por isso, a Constituição protege a intimidade e a vida privada (art. 5º, X da CF), que abrangem uma série de dados pessoais (bancários, fiscais etc), e também a comunicação de dados (art. 5º, XII, da CF), por via telefônica, telemática ou outro meio. Nesse contexto se insere a busca e apreensão domiciliar, que se sujeita à reserva absoluta de jurisdição (art. 5º, XI, da CF). (BRASIL, 2019b, p. 32-33).

Assim, até então parece em consonância com o voto do Ministro Relator, pois reconhece o fundamento de privacidade. No entanto, a distinção inicia com a seguinte construção: "a cláusula absoluta de reserva de jurisdição se limita à comunicação dos dados – que deve ser compreendida como informações dinâmicas –, e não aos dados em si – considerados como informações estáticas –, que possuem proteção distinta, conforme entendimento jurisprudencial" (BRASIL, 2019b, p. 35). Indica "que a existência de sigilo não deve ser confundida com cláusula de reserva de jurisdição" (BRASIL, 2019b, p. 35). Cita entendimento do STF no sentido de que, havendo apreensão de equipamento por mandado de busca e apreensão domiciliar, o próprio mandado judicial já faculta o acesso às informações, como é o caso do Recurso Extraordinário nº 418.416-8, publicado em 19 de dezembro de 2006 (BRASIL, 2019b, p. 35).

Em suma, o Min. Redator entendeu, na esteira da decisão de primeiro grau, pela inaplicabilidade das Leis n. 12.965/2014 (Marco Civil da Internet) e 9.296/1996 (interceptação de comunicações telefônicas), sob o fundamento de que os diplomas legais objetivam tutelar o fluxo das comunicações, no que se refere a "sistemas de informática e telemática, isto é, proteger a fluência da comunicação em andamento, diversamente do que ocorre quando são recolhidos aparelhos informáticos em decorrência de busca e apreensão domiciliar, nos quais os dados são estáticos" (BRASIL, 2019b, p. 37). Concluiu pela denegação da ordem, o que foi acompanhado pela maioria.

2.2 O fundamento de privacidade da inviolabilidade do domicílio na constituição federal

Como visto, a Quarta Emenda à Constituição dos Estado Unidos influenciou, além de tratados e convenções internacionais, diversos ordenamentos, dentre eles, o brasileiro. A Carta Imperial de 1824 previu no art. 179, VIII, pela primeira vez, que "todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a lei determinar" (BRASIL, 1824).

Na Constituição de 1891, já na República, a redação permaneceu semelhante no art. 72, §11: "a casa é o asilo inviolável do indivíduo; ninguém pode aí penetrar, de noite, sem consentimento do morador, senão para acudir as vítimas de crimes, ou desastres, nem de dia senão nos casos e pela forma prescritos na lei" (BRASIL, 1891). Na Constituição de 1934, no art. 113, n. 16, por sua vez, "a casa é asilo inviolável do indivíduo. Nela ninguém pode penetrar, de noite, sem consentimento do morador, senão para acudir a vítimas de crimes ou desastres, nem de dia, senão nos casos prescritos na lei" (BRASIL, 1934).

Como referem Ingo Wolfgang Sarlet e Jayme Weingartner Neto, a Constituição do Estado Novo, de 1937, "embora tenha assegurado a inviolabilidade do domicílio (juntamente com o sigilo da correspondência), o fez de modo genérico, sem proibir o ingresso durante o período noturno e deixando para o legislador regulamentar as hipóteses que autorizavam a intervenção no direito mesmo sem o consentimento do seu titular" (SARLET; WEINGARTNER NETO, 2013, p. 546). Os autores pontuam que com o processo de redemocratização, a inviolabilidade do domicílio voltou a ganhar força (SARLET; WEINGARTNER NETO, 2013, p. 546).

Nesse aspecto, vale ressaltar que a inviolabilidade do domicílio no Brasil sofreu interrupções quanto ao seu desenvolvimento, além de ser considerada nova em relação à Quarta Emenda. Após a Constituição de 1937, ainda sobreveio a Constituição de 1946 e a Constituição de 1967, essa última sob o regime militar, antes da consolidação da Constituição de 1988. Assim, o art. 5º, XI, da CRFB, determina que "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial" (BRASIL, 1988).

Percebe-se que o enunciado normativo atual contém algumas restrições, uma vez que se trata de direito fundamental constitucionalmente previsto, nas hipóteses de "flagrante", "desastre" e "socorro". Tais restrições não são compreendidas como inclusas no suporte fático, não limitam, internamente, a inviolabilidade do domicílio. Diante do cenário apresentado, o conceito de restrição não surge *a priori*, entende-se que "entre o conceito de direito e o conceito de restrição não existe nenhuma relação necessária. Essa relação é criada somente a partir da exigência externa ao direito sem si, de conciliar os direitos de diversos indivíduos" (ALEXY, 2017, p. 277).

Por conseguinte, surge a necessidade de se distinguir a teoria interna da externa (SIEBERT, 1934, p. 85), diferenciando-se limitação de restrição. Quando identificada a possibilidade de restringir uma liberdade, por vislumbrar-se o reequilíbrio de posições jurídicas, confere-se enfoque à argumentação pelo discurso jurídico, em busca de uma correção em atenção à "universalidade ao julgar" (CACHAPUZ, 2018, p. 100), o que justifica a adoção de uma teoria externa de restrição a direitos fundamentais.

Sarlet e Weingartner Neto indicam, especialmente quanto à interpretação e alcance do enunciado normativo, que "há que retomar a vinculação da inviolabilidade do domicílio com a proteção da vida privada e a garantia do livre desenvolvimento da personalidade" (SARLET; WEINGARTNER NETO, 2013, p. 547), na linha adotada no presente estudo, de que a inviolabilidade do domicílio constitui direito fundamental que assegura às pessoas "o direito de serem deixadas em paz, de tal sorte que a proteção

não diz respeito ao direito de posse ou propriedade, mas com a esfera espacial na qual se desenrola e desenvolve a vida privada" (SARLET; WEINGARTNER NETO, 2013, p. 547).

Embora o art. 5º, X, da CRFB, reconheça, por si só, que "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". Quando diante de uma operação, para fins penais, que deva estar de acordo com a Constituição, inevitável que se recorra aos incisos XI (da inviolabilidade do domicílio) e, se for o caso, ao XII (a correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas). Importante registrar que Sarlet e Weingartner Neto, ao analisar outros ordenamentos, assim ratificam a relação indissociável entre inviolabilidade do domicílio e direito à privacidade:

> Assim, apenas em caráter ilustrativo, doutrina e jurisprudência constitucional espanhola afirmam a existência de um nexo indissolúvel entre a inviolabilidade do domicílio e o direito à intimidade, que implica, em princípio, um conceito constitucional mais ampliado de domicílio que o convencional conceito jurídico-privado ou mesmo jurídico-administrativo , o que também se constata no caso do direito português e alemão, sempre a privilegiar um conceito amplo de domicílio e destacando sua conexão com a garantia da dignidade humana e de um espaço (SARLET; WEINGARTNER NETO, 2013, p. 547).

Assim, reconhece-se esse fundamento de privacidade, o que se confirma tanto pela doutrina quanto pela jurisprudência brasileira, embora se perceba que a inviolabilidade do domicílio sofrerá ainda muitos desafios, além dos promovidos durante períodos autoritários anteriores à CRFB de 1988, como também aqueles que ainda permanecem.

A partir disso, no que se refere ao desenvolvimento tecnológico e à operação e ao tratamento de dados pessoais para fins criminais, a proposta consiste em identificar na expectativa de privacidade, assim como feito pela Suprema Corte dos Estados Unidos, um fundamento que permita a atualização da interpretação em consonância com o desenvolvimento tecnológico e à operação e tratamento de dados pelo Poder Público para fins penais. E realmente parece ser esse o caminho, dada a redação do art. 5º, XII, da CRFB: "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".

Com base em Hannah Arendt, como indica Ferraz Jr., cabe para compreensão da linha que se adota no presente estudo, no sentido de que a exclusividade detém três atributos principais: solidão (desejo de estar só), segredo (exigência de sigilo) e autonomia (liberdade de decidir sobre si mesmo como centro emanador de informações) (FERRAZ JR., 1993, p. 441). Com isso, pretende-se demonstrar que a exclusividade se assemelha aos olhos, com a possibilidade de utilização de lentes distintas, para diferentes situações e relações jurídicas, com alcances também diversos, mas que somente são possíveis se entendida a privacidade como fundamento.

A relevância de análise do discurso jurídico em matéria de direitos fundamentais permite que se perceba a influência externa de um contexto social e político. Se há uma tendência maior à proteção das liberdades, ou, ao contrário, se há uma tendência maior à dominação totalitária. Nesse sentido, Habermas refere que a esfera pública não pode ser entendida como uma instituição, nem como uma organização), e sim como uma "estrutura comunicacional" (HABERMAS, 1997, p. 92), que se reproduz através do agir comunicativo, constituído através da linguagem em razão da liberdade comunicativa que uns concedem aos a distinção entre as esferas guarda relação com a identificação e análise da dominação totalitária por Hannah Arendt.

É o ver sem ser visto que destrói a esfera pública e elimina a esfera privada (LAFER, 1988, p. 245). Como pontua Lafer, é a inexistência de limites entre o público e o privado que caracteriza o totalitarismo. Dessa forma, este "ver sem ser visto" está intrinsecamente relacionado, na atualidade, às tecnologias de vigilância, que não permitem identificar quem é aquele que vê, gerando a sensação de espionagem, mesmo quando sua utilização é justificada com base em um possível aumento da segurança.

Daí porque, "a relação estrita entre uma teoria das esferas e um direito geral de liberdade. As esferas servem na medida em que predispõem espaços abstratos ao público e ao privado, ambos conferindo mesmo valor à liberdade" (CACHAPUZ, 2017, p. 1133). Ademais, Cachapuz esclarece que "tratam-se de espaços que abrigam experiências e manifestações distintas e que demandam tipos de proteção também distintos" (CACHAPUZ, 2017, p. 1133).

Nesse sentido, verifica-se que a teoria das esferas, desde que aberta ao discurso jurídico, por meio da teoria da argumentação jurídica (CACHAPUZ, 2018, p. 39), permite a racionalização dos problemas práticos com os quais se depara o intérprete, uma vez que torna possível localizar o exercício coexistente - e colidente - das liberdades pelos indivíduos, de modo que se verifique formal e materialmente "se se está frente a um fenômeno que revele uma circunstância da vida privada ou da intimidade de alguém - devendo, por isso, ser mantido na esfera privada -, ou se é algo que mereça visibilidade pública, dado o interesse público reconhecido" (CACHAPUZ, 2006, p. 106).

Considerações finais

Da mesma forma como privacidade e propriedade foram adquirindo diferentes contornos, também importa referir que a humanidade se desenvolveu a partir de ferramentas, isso denota a atribuição de tecnicidade. A história e suas eras sempre foram marcadas por ferramentas ou pelo aperfeiçoamento tecnológico. Basta recordar: idade da pedra, do fogo, da roda. Essa perspectiva foi estudada pelo autor Bernard Stiegler. Para ele, a sociedade não seria possível sem tecnicidade, referindo que "o humano se inventa no técnico, inventando a ferramenta - tornando-se tecnologicamente exteriorizado" (STIEGLER, p. 141). Lucas Introna sobre a mesma questão indica que "o horizonte transcendental constitutivo do humano é a tecnicidade, da qual emergem as condições de possibilidade do tempo, da sociedade e da cultura" (INTRONA, 2017).

Assim, a relação entre direito e tecnologia não é recente. Quanto à interferência nos direitos de personalidade, especificamente quanto à privacidade, Samuel Warren e Louis Brandeis já alertavam, em 1890, que "invenções e métodos de negócio chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa e para assegurar ao indivíduo o que o Juiz Cooley chama de direito de estar só" (WARREN; BRANDEIS, 1890, p. 195). Atualmente, como refere o autor Daniel Solove, a pessoa ganha uma esfera digital, como indica o próprio título do livro (SOLOVE, 1972), que ratifica a inexistência de limites físicos e aponta para questões atuais que envolvem a proteção de dados.

O presente artigo buscou demonstrar que os direitos fundamentais, quando verificados em uma situação de análise quanto à restrição das liberdades, exigem, como se viu, em muitas ocasiões, a superação de certa descarga argumentativa, para que se possa acompanhar o desenvolvimento tecnológico. O recorte proposto, centrado na inviolabilidade do domicílio, demonstrou que os precedentes dos Estados Unidos se amparam em um fundamento comum, relacionado à "expectativa de privacidade razoável", o que permitiu o avanço da jurisprudência à temática de proteção de dados, confirmando a hipótese de pesquisa.

Basicamente, dos casos analisados da Suprema Corte, com a superação da noção de violação à propriedade tangível (Katz v. Estados Unidos), sedimentou-se a referida "expectativa de privacidade razoável". Com o desenvolvimento tecnológico (Kyllo v. Estados Unidos), houve a ratificação do fundamento de privacidade.

Os casos mais recentes analisados pela Suprema Corte (Carpenter v. Estados Unidos), tratam, de maneira mais específica, da temática de proteção de dados. Percebeu-se que o desenvolvimento tecnológico e o avanço de questões relacionadas ao ambiente virtual e digital têm, de certa forma, enfraquecido a doutrina de terceiros, quanto à dispensa de mandado de busca e apreensão em relação a dados disponibilizados por terceiros, cujo enfoque se centra no consentimento como instrumento de afastamento à expectativa razoável de privacidade. Isso tem dado ensejo à elaboração de leis estaduais específicas em matéria de proteção de dados nos Estado Unidos (Utah, por exemplo), por meio das quais se determina a necessidade de expedição de mandado de busca e apreensão, em contrariedade à doutrina de terceiros.

Ainda, interessante aspecto foi identificado no presente estudo. Nos Estados Unidos, a noção de privacidade surge, inicialmente, na relação entre Estado e indivíduo, justamente com a interpretação conjunta da Quarta e da Quinta Emendas, como visto. Somente após, a privacidade surge como direito oponível entre privados.

Já em relação ao Brasil, percebeu-se que a existência da inviolabilidade do domicílio, derivada da Quarta Emenda, e modificada por tratados e convenções internacionais, possui algumas características distintas, no entanto, a partir do Tema 280, percebeu-se que o STF também atribui ao art. 5º, incisos XI e XII, um fundamento de privacidade. No entanto, quanto ao desenvolvimento tecnológico, ainda se encontra incipiente, motivo que, ao invés de enfraquecer, fortalece o enfoque proposto, que busca lançar luz sobre a relação entre privacidade, proteção de dados e inviolabilidade domicílio.

Além dos direitos fundamentais expressos na CRFB, o Brasil tem avançado na temática da proteção de dados com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com o Marco Civil da Internet (Lei nº 12.965/2014), por exemplo. No entanto, atente-se para o fato de que a referida lei não alcança o tratamento de dados pessoais realizados para fins exclusivos de "atividades de investigação e repressão de infrações penais", de acordo com o art. 4º, III, "d", da referida lei. Embora o sistema jurídico brasileiro indique estar suficiente ao enfrentamento de casos tais quais os da Suprema Corte analisados no presente estudo, o estudo identifica que há necessidade de se desenvolver não só em termos doutrinários, como também acadêmicos, a temática de proteção de dados em face do Estado, a partir do art. 5º, XII, da CRFB.

No Brasil, interessante observar que a privacidade também surge, expressa pela primeira vez, na Lei de Imprensa nº 5.250/678, ao dispor sobre divulgação de questões atinentes à vida privada não motivada por razões de interesse público, que, detém, duplamente, a possibilidade de aplicação em relações entre privados, mas norteada por um princípio de direito público, referente ao interesse público.

Finaliza-se com uma contribuição à reflexão, sobre um acontecimento real, que poderia ser considerado distópico, relacionado à temática analisada e indicador dos caminhos promovidos pelo desenvolvimento tecnológico e pela inteligência artificial. A Alexa, assistente virtual da Amazon, presenciou - em mais de uma oportunidade (2015, 2018 e 2019) cenas de prováveis homicídios nos Estados Unidos (SILVERSTEIN, 2018). A questão tem gerado discussões doutrinárias, especialmente quanto à doutrina de terceiros e quanto à aplicação da Quarta ou da Primeira Emenda (MELANCON, 2018).

Mandados de busca e apreensão já foram expedidos, e a Amazon questiona a existência de razões suficientes que indiquem a impossibilidade de aquisição das informações por outros meios, além de nexo entre as informações coletadas e o objeto da investigação criminal. Mais uma vez, proteção de dados, privacidade e inviolabilidade do domicílio parecem estar aproximadas, e muitas novas questões serão apreciadas pela doutrina e pela jurisprudência. Espera-se pelas próximas perguntas jurídicas que serão formuladas. Talvez Alexa já saiba as respostas.

Referências

ADAMS PAPER. Petition of Lechmere (Argument on Writs of Assistance). 1761. **Massachusetts Historical Society.** Disponível em: http://www.masshist.org/publications/adams-papers/index.php/view/LJA02dg13

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Virgílio Afonso da Silva. 2ª ed. 3ª tiragem. São Paulo: Malheiros, 2017.

ALMEIDA, Gregório Assagra de. O sistema jurídico nos Estados Unidos - Common Law e carreiras jurídicas (judges, prosecutors e lawers): o que poderia ser útil para a reforma do sistema processual brasileiro?. **Revista de Processo**, São Paulo, v. 251, p. 523-560, jan. 2016. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RPro_n.251.19.PDF. Acesso em: 10 nov. 2022.

ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. 10ª ed. Rio de Janeiro: Forense Universitária, 2007.

BAKER, John. **An introduction to English legal history**. Londres: Butterworths, 2002.

BBC. **Brazil's culture minister fired after echoing Goebbels.** 17/01/2020. Disponível em: https://www.bbc.com/news/world-latin-america-51149224. Acesso em: 10 nov. 2022

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

BRASIL. (Código de Processo Penal). **Decreto-Lei no 3.689, de 03 de outubro de 1941.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 10 nov. 2022.

BRASIL.(Código Civil). **Lei no 10.406, de 10 de janeiro de 2002.** Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/2002/l10406.htm. Acesso em: Acesso em: 10 nov. 2022.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 496.420/SP**. Relatora Ministra Laurita Vaz. Sexta Turma. Julgado em: 30 de maio de 2019. Publicado em: 11 de junho de 2019. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201900626870&dt_publicacao=11/06/2019. Acesso em: 10 nov. 2022 (2019a).

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 444.024/PR.** Relator Ministro Sebastião Reis Júnior, Relator para acórdão, Ministro Rogerio Schietti Cruz. Sexta Turma. Publicado em 02 de agosto de 2019. Disponível em:

https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201800782456&dt_publicacao=02/08/2019. Acesso em: 10 nov. 2022. (2019b)

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 603.616/RO**. Relator Ministro Gilmar Mendes. Plenário. Julgado em: 05 de novembro de 2015. Publicado em: 10 de maio de 2016. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=3774503. Acesso em: 10 nov. 2022.

CACHAPUZ, Maria Cláudia. **Intimidade e vida privada no novo Código Civil Brasileiro:** uma leitura orientada pelo discurso jurídico. Porto Alegre: Sergio Antônio Fabris Ed., 2006.

CAVOUKIAN, Ann. **Privacy and Drones**: Uhmaned Aerial Vehicles. Ontario, Canada: Information and Privacy Comissioner, 2012. Disponível em: https://www.ipc.on.ca/wp- content/uploads/Resources/pbd-drones.pdf. Acesso em: 10 nov. 2022.

CUNNINHGAM, Clark D. Apple and the American Revolution: Remembering Why We Have the Fourth Amendment (2016). **Georgia State University College of Law.** Nº. 2016-19. Disponível em: https://ssrn.com/abstract=2765572. Acesso em: 10 nov. 2022.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito de São Paulo**, São Paulo, v. 88. p. 439- 459, jan./dez. 1993.

FORBES. **Utah bans Police from searching digital data without a warrant, closes Fourth Amendment loophol.** Nick Sibilla. 16/04/2019. Disponível em: https://www.forbes.com/sites/nicksibilla/2019/04/16/utah-bans-police-from-searching-digital-data-without-a-warrant-closes-fourth-amendment-loophole/#220e5e176306. Acesso em: 10 nov. 2022.

FROH, Amanda S. Rethinking Canine Sniffs: The Impact of Kyllo v. United States. **Seattle University Law Review**, vol. 26, issue 2, p. 337-364, 2002. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/sealr26&i=295. Acesso em: 10 nov. 2022.

G1. **Em 2019, RJ tem maior número de mortes por policiais desde o início da série histórica, diz ISP**. 25/11/2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/11/25/em-2019-rj-tem-maior-numero-de-mortos-por-policiais-desde-o-inicio-da-serie-historica.ghtml. Acesso em: 10 nov. 2022.

HABERMAS, Jürgen. **Direito e democracia; entre facticidade e validade, volume II**. Tradução: Flávio Beno Siebeneichler. Rio de Janeiro: Tempo Brasileiro, 1997.

INTRONA, Lucas, Phenomenological Approaches to Ethics and Information Technology. **The Stanford Encyclopedia of Philosophy**. Edward N. Zalta (ed.), 2017. Disponível em: https://plato.stanford.edu/archives/fall2017/entries/ethics-it-phenomenology/. Acesso em: 10 nov. 2022.

KERR, Orin S The digital Fourth Amendment. **The John W. Hager Distinguished Lecture in Law**. 11. 2016. Disponível em: https://digitalcommons.law.utulsa.edu/hager/11. Acesso em: 10 nov. 2022.

KERR, Orin S. Implementing Carpenter: the digital Fourth Amendment. **USC Law Legal Studies Paper.** nº. 18-29. Oxford: University Press, 2018. Disponível em: https://ssrn.com/abstract=3301257. Acesso em: 10 nov. 2022.

LAFER, Celso. **A reconstrução dos direitos humanos:** um diálogo com o pensamento de Hannah Arendt. 3ª reimpressão. São Paulo: Companhia das Letras, 1988.

LIFANTE VIDAL, Isabel. Dos conceptos de discrecionalidad jurídica. **DOXA.** nº 25, 2002.

MELANCON, Tara. '**Alexa, Pick an Amendment':** A Comparison of Fourth and First Amendment Protections of Echo Device Data. (February 28, 2018). Disponível em: https://ssrn.com/abstract=3132066 or http://dx.doi.org/10.2139/ssrn.3132066. Acesso em: 10 nov. 2022.

NEW YORK TIMES. **He Won a Landmark Case for Privacy Rights. He's Going to Prison Anyway.** Those who score big victories for the civil liberties of every American sometimes lose their own freedom. Cristian Farias. Junho de 2019. Disponível em:https://www.nytimes.com/2019/06/13/opinion/timothy-carpenter-prison-privacy.html. Acesso em: 10 nov. 2022.

SARLET, Ingo Wolfgang; WEINGARTNER NETO, Jayme. A inviolabilidade do domicílio e seus limites: o caso do flagrante delito. **Revista de Direitos Fundamentais e Democracia**, Curitiba, vol. 14, n. 14, p. 544-562, jul./dez. 2013.

SCHULHOFER, Stephen. **More Essential Than Ever:** The Fourth Amendment in the Twenty-First Century. Oxford: University Press, 2012.

SILVERSTEIN, Ed. Alexa, Tell Me About the Homicide: Judge Orders Amazon to Turn Over Echo Data. **Law.Com.** 26/11/2018. Disponível em: https://www.law.com/legaltechnews/2018/11/26/legal-questions-abound-after-amazon-ordered-to-provide-echo-data-in-homicide-inquiry/. Acesso em 10 nov. 2022.

SOLOVE, Daniel J. The Digital Person: Technology and Privacy in the Information Age. Ex Machina: **Law, Technology and Society**. Jack M. Balkin and Beth Simone Noveck

(Ed.). New York: NYU Press, 2004. Disponível em: https://ssrn.com/abstract=2899131. Acesso em: 10 nov. 2022.

STIEGLER, Bernard. **Technics and Time: The Fault of Epimetheus**. Stanford: Stanford University Press, 1998.

SWINDLE, Jason. The history behind the 4TH Amendment. 21/03/2013. Disponível em: https://www.swindlelaw.com/2013/03/the-history-behind-the-4th-amendment/. Acesso realizado em: 10 nov. 2022.

THAI, Joseph T. Is Data Mining ever a search under justice Stevens's Fourth Amendment?. **Fordham Law Review**. vol. 74, 1731-1758, 2006.

UNITED STATES OF AMERICA. **Constitution**. Disponível em: https://www.law.cornell.edu/constitution/fourth_amendment. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. **Constitution**. Disponível em: https://www.law.cornell.edu/wex/fifth_amendment. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **Boyd v. Estados Unidos, 116 US 616 (1886).** Disponível em: https://supreme.justia.com/cases/federal/us/116/616/. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **California v. Ciraolo, 476 U.S. 207 (1986)**. Disponível em: https://supreme.justia.com/cases/federal/us/476/207/case.html. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **Kyllo v. United States, 533 U.S. 27 (2001).** Disponível em: https://supreme.justia.com/cases/federal/us/533/27/case.html. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **United States v. Miller, 425 U.S. 435 (1976).** Disponível em: https://supreme.justia.com/cases/federal/us/425/435/. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **Carpenter v. United States, 585 US __ (2018).** Disponível em: https://supreme.justia.com/cases/federal/us/585/16-402/. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **United States v. Miller, 425 U.S 435, (1976).** Disponível em: https://supreme.justia.com/cases/federal/us/425/435/. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **Smith v. Maryland, 442 U.S 735 (1979).** Disponível em: https://supreme.justia.com/cases/federal/us/442/735/. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **Davis v. United States, 564 US 229 (2011).** Disponível em: https://supreme.justia.com/cases/federal/us/564/229/. Acesso em: 10 nov. 2022.

UNITED STATES OF AMERICA. Supreme Court of United States. **United States v. Jones, 565 U.S 400 (2012),** Disponível em: https://supreme.justia.com/cases/federal/us/565/400/. Acesso em: 10 nov. 2022.

UNITED STATES SENATE. **Constitution of the United States**. Disponível em: https://www.senate.gov/civics/constitution_item/constitution.htm. Acesso em: 10 nov. 2022.

WALDRON, Jeremy. **Law and disagreement**. Oxford: University Press, 1999.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review,** v. 4, n. 5, p. 193-220, dec. 1890. Disponível em: http://www.jstor.org/stable/1321160?seq=1#page_scan_tab_contents. Acesso em: 10 nov. 2022.

Direito ao Esquecimento: Reflexões a Partir do RE 1.010.606/RJ

Lisiane Feiten Wingert Ody[43*]

RESUMO

O artigo trata do direito ao esquecimento a partir de julgado do STF afetado à sistemática da repercussão geral. Por meio do direito comparado, de métodos indutivo e dedutivo e de estudo de caso, aborda, primeiramente, os casos Lebach e Melvin v. Reid são examinados, a fim de demonstrar que tratam de temas análogos, porém diversos. A análise crítica das razões de decidir do tribunal é iniciada a seguir, examinando-se o conceito e os requisitos do direito ao esquecimento. A pesquisa é relevante por enfrentar tema presente e de importância, oferecendo critérios para a sua compreensão.

PALAVRAS-CHAVE:

Direito ao esquecimento. Sociedade de Informação. Internet.

[43*] Professora Associada da Faculdade de Direito da Universidade Federal do Rio Grande do Sul - UFRGS. Doutora em Direito (UFRGS), com período sanduíche junto à Universidade de Heidelberg, Alemanha. Mestre em Direito Privado (UFRGS). Especialista em Direito do Consumidor e especialista em Direito Internacional (UFRGS). Especialista em Processo Civil (PUC-RS). E-mail: wingert.ody@ufrgs.br

Right to Be Forgotten: Some Thoughts on the "Extraordinary Appeal" 1.010.606/RJ

Lisiane Feiten Wingert Ody

ABSTRACT

The article examines the subject of the right to be forgotten considering case decided by the STF and with authority over all Brazilian courts. Comparative methods are used, as well as induction, deduction and case studies. First, the cases Lebach and Melvin v. Reid are analysed with the aim of proving that they refer to different rights (resocialization and privacy). A critical analysis of the rationale for the court's decision follows, examining the concept and requirements of the right to be forgotten. The value of this study lies in the fact it offers criteria for understanding different hypotheses.

KEYWORDS

Data Leak; Right to be forgotten. Information society. Internet.

Introdução

O Supremo Tribunal Federal julgou, por maioria, sob sistemática da repercussão geral, o Recurso Extraordinário 1.010.606/RJ, cujo objeto de afetação era a "*aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares*".

O presente trabalho examina o tema do direito ao esquecimento a partir desse precedente, fazendo-o sob a perspectiva do direito comparado (método funcional-contextualizado), especialmente do direito europeu e alemão. Além da revisão bibliográfica, são examinados precedentes jurisprudenciais estrangeiros, selecionados qualitativamente, por permitirem conclusões gerais, a fim de a partir deles, mediante emprego de técnica indutiva, evidenciar que o direito ao esquecimento é estritamente relacionado ao meio digital. O tema é de enorme relevância, pois a tecnologia trouxe reflexos diretos no incremento não apenas quantitativo, mas também qualitativo, de violações a direitos de personalidade, o que restou evidenciado pela afetação do caso à sistemática da repercussão geral.

A fim de contextualizar a controvérsia específica, que foi inserida na questão geral do exame da (in)compatibilidade constitucional do direito ao esquecimento, faz-se breves considerações sobre o substrato fático do caso entre a *família Curi e Rede Globo*, que ensejou o recurso extraordinário em questão.

O precedente teve início com o ajuizamento de ação pelos irmãos da falecida *Aída Curi*, objetivando *reparação cível* pelo *uso não autorizado do nome e imagem dela* em reprodução midiática dos fatos que envolveram sua morte, ocorrida quando tinha 18 aos de idade em 14.07.1958, no programa *Linha Direta Justiça*, apresentado pela *Rede Globo* de televisão. O TJRJ julgara improcedente do pedido, porque a Constituição garantiria "*a livre expressão da atividade de comunicação, independente de censura ou licença, franqueando a obrigação de indenizar apenas quando o uso da imagem ou informações é utilizada para denegrir ou atingir a honra da pessoa retratada, ou ainda, quando essa imagem/nome for utilizada para fins comerciais*". O tribunal afirmou, ainda, que "*o esquecimento não é o caminho salvador para tudo*", sendo "*muitas vezes [é] necessário reviver o passado para que as novas gerações fiquem alertadas e repensem alguns procedimentos de conduta do presente*".

Interposto recurso especial ao STJ, foi-lhe negado provimento sob fundamento de que "*o direito ao esquecimento que ora se reconhece para todos, ofensor e ofendidos, não alcança o caso dos autos, em que se reviveu, décadas depois do crime, acontecimento que entrou para o domínio público*". Além disso, constou do acórdão do REsp que "*o reconhecimento, em tese, de um direito de esquecimento não conduz necessariamente ao dever de indenizar. Em matéria de responsabilidade civil, a violação de direitos encontra-se na seara da ilicitude, cuja existência não dispensa também a ocorrência de dano, com nexo causal, para chegar-se, finalmente, ao dever de indenizar*".

O recurso extraordinário foi manejado perante o STF com base na alínea *a* do inciso III do artigo 102 da Constituição, tendo-se: (i) alegado ofensa aos artigos 1º, inciso III (dignidade da pessoa humana), 5º, *caput* e incisos III e X (direitos à vida, à liberdade, à igualdade, à segurança e à propriedade; submissão à tortura e tratamento desumano; e direitos à intimidade, à vida privada, à honra e à imagem das pessoas) e 220, § 1º, da Constituição (liberdade de informação jornalística) e (ii) invocado o direito ao esquecimento.

Uma vez recebido o recurso extraordinário, o ministro relator considerou que a questão extrapolaria os interesses subjetivos das partes, tendo o Plenário do tribunal afetado a controvérsia à sistemática da repercussão geral (Tema 786). O relator iniciou a fundamentação do voto condutor com remissões à expressão francesa *droit à l'oubli,* que teria sido cunhada pelo professor *Gérard Lyon-Caen* em comentários à decisão francesa relacionada ao assassino *Henri Landru*[44], e utilizada pela jurisprudência francesa pela primeira vez no caso *Madame M. c. Filipacchi et Cogedipresse,* julgado pelo *Tribunal de Grande Instance* de Paris em 20 de abril 1983[45]. A seguir, o relator passou a tecer considerações sobre o direito alemão, invocando os casos *Lebach*, e o direito americano, ao referir o caso *Red Kimono* (*Melvin v. Reid*) e as contribuições a partir de *Warren and Brandeis,* introduzindo, então, na p. 40 do PDF de inteiro teor do julgado[46], o *Caso González e Google España*[47], que é considerado o paradigma do direito ao esquecimento.

Diante desse contexto, o voto sistematizou os "*elementos essenciais do direito ao esquecimento*" como sendo a *licitude da informação* e o *decurso do tempo*, concluindo que "*ninguém (...) é obrigado a se desfazer de seu direito à informação para permitir a terceiros uma vida livre do conhecimento de seus erros passados*" (p. 68 do voto). Após, o relator passou então a indagar sobre a existência de direito ao esquecimento em âmbito digital, afirmando, no ponto, que "*no intuito de proteger os caros valores desafiados pela propagação massiva de informações, se combate[ria] o próprio desenvolvimento da tecnologia no que tange à informação, requerendo-se o completo domínio do indivíduo sobre seus dados, com primazia, inclusive, sobre o direito dos demais indivíduos de se informarem*" (p. 75). O relator associou, ainda, o direito ao esquecimento a eventual violação à liberdade de expressão e introduziu, assim, algumas das passagens constantes da ADI 4815 (ADI das Biografias). A tese proposta pelo relator e aprovada pelo colegiado foi a seguinte (p. 88):

> É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais - especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral - e das expressas e específicas previsões legais nos âmbitos penal e cível.

---

[44] Apesar de mal referenciado no acórdão, que dá a entender como ano do *Affaire Landru* 1967, quando os fatos ocorreram após a primeira guerra mundial, identifica-se o caso que deu origem ao texto de Lyon-Caen como sendo o julgado pelo *Tribunal de Grande Instance de Seine*, de 4 de outubro de 1965, em que uma ex-amante de *Landru,* assassino contumaz notório em toda a França, requereu a reparação de danos pelo lançamento de filme por Claude Chabrol com passagem concernente a período de sua vida que preferia manter no passado. No julgado, fora indeferido o pedido *porque a própria requerente havia publicado suas memórias narrando os fatos*, também conhecidos de vários trabalhos jurídicos. Os comentários de *Caen-Lyon* podem ser encontrados em *Juris-Classeur Périodique (JCP)* 1966, II, 14482.

[45] Embora não referenciado no acórdão, o julgado pode ser encontrado em: *JCP* 1985, II, 20434.

[46] Todas as demais referências isoladas a números de páginas no texto correspondem à numeração do PDF com o inteiro teor do julgamento.

[47] Processo C-131/12 – Tribunal de Justiça da União Europeia.

Em relação ao caso específico, prevaleceu no julgado o entendimento de ser "ausente afronta ao nome, à imagem, à vida privada da vítima ou de seus familiares que decorra da exibição do programa televisivo Linha Direta: Justiça" (p. 92).

Os demais membros do colegiado passaram a votar. O ministro Alexandre de Moraes apresentou voto escrito (p. 122-147), acompanhando o relator, assim como os ministros Marco Aurélio (p. 191-192), Luiz Fux (p. 293-314), Rosa Weber (p. 165-201) e Carmen Lúcia (p. 205-220). A ministra Rosa Weber afirmou que a "proteção constitucional à inviolabilidade da intimidade e pelo escopo da legislação de proteção de dados pessoais" seriam suficientes para amparar as pretensões que poderiam ser veiculadas a título de direito ao esquecimento, enquanto a ministra Carmen Lúcia, por sua vez, reiterou a compreensão que já manifestara por ocasião do julgamento da ADI das Biografias, afirmando que "nenhuma censura presta", seja estatal ou particular, assim justificando sua adesão ao voto condutor.

O ministro Nunes Marques aviou voto alinhado com a compreensão geral do relator de que não haveria direito autônomo ao esquecimento no Brasil, mas dando provimento no caso específico da demanda da família Curi para reconhecer o direito à indenização por dano moral, diante do "desprezo da memória da vítima do crime", a ser arbitrada na instância de origem (p. 92-121). O ministro Gilmar Mendes (p. 221-290), apesar de afirmar não haver, no direito brasileiro, "disciplina normativa específica e direta abarcando o provável direito ao esquecimento", situou claramente a questão do direito ao esquecimento no universo digital, tecendo considerações que o associam à proteção de dados. Em relação ao caso concreto da família Curi, Gilmar Mendes acompanhou o ministro Nunes Marques para concluir ser "moralmente indenizável a exposição humilhante e/ou vexatória[48] de dados pessoais (imagem, nome e demais elementos de identificação) de pessoa (autor ou vítima) envolvida em fato ocorrido há décadas, em matéria televisiva de alcance nacional, ainda que presente interesse histórico, social ou público atual, com fundamento no direito à intimidade, à vida privada e à proteção ao nome e à imagem, determinando".

O ministro Edson Fachin também apresentou voto divergente (p. 148-163), porém, com amplitude diversa: reconhecendo a existência de um direito ao esquecimento no ordenamento constitucional brasileiro, mas negando, no caso concreto, a pretensão dos requerentes. Sua compreensão foi no sentido de terem "a liberdade de expressão e o direito à informação precedência sobre o direito ao esquecimento, independentemente do transcurso do tempo", podendo ceder diante de outra pretensão, aludindo à dignidade da pessoa humana ao direito à privacidade, à honra e à imagem e o direito à autodeterminação informacional.

Feito esse breve retrospecto, anota-se que a análise do tema no presente trabalho se divide em duas partes. Na primeira parte, são tratados casos Lebach e Melvin v. Reid mencionados no acórdão do STF, analisando-se o substrato fático deles e a fundamentação utilizada pelo respectivo julgador, a fim de demonstrar que os institutos jurídicos a que se referem, embora análogos, não se confundem com o direito ao esquecimento, que tampouco teria relação com o caso ensejador da afetação da controvérsia à sistemática de repercussão geral, entre a família Curi e a Rede Globo. Na segunda parte, expõe-se os elementos centrais do que se configura como direito ao esquecimento a partir do caso González e Google España. Após, analisam-se dois julgamentos recentes do tribunal constitucional alemão (Das Recht auf Vergessenwerden I und II), que são as referências naquele ordenamento jurídico sobre o tema, demonstrando que a realidade digital imposta pela sociedade de informação e de conhecimento demanda reconhecer no Brasil o direito

[48] Uma escolha inapropriada de palavras, pois não houve humilhação e nem vexame de Aída Curi, mas violação de sua memória e, nesse contexto, da privacidade da família.

ao esquecimento, mais amplo que o simples direito de apagar previsto na LGPD, porque "internet never forgets"[49].

1. Ausência de similitude fática entre os paradigmas invocados pelo STF e o caso entre a *família Curi e Rede Globo*

1.1 Direito à reabilitação: Casos *Lebach I und II*

O direito à reabilitação diz respeito à *ressocialização do criminoso*, sendo recorrentemente confundido com o direito ao esquecimento no Brasil, haja vista que seu propósito é proporcionar que não seja lembrada a prática de ato criminoso por quem o invoca. Embora tenham em comum o "esquecer", isto é, o superar de fato passado, a diferença está na circunstância de que o direito à reabilitação se volta a fatos do passado qualificados por serem associados a crime e que podem ser veiculados em qualquer meio.

No direito comparado, é referência do tema o caso *Lebach*[50], que foi o primeiro decidido pelo tribunal constitucional alemão envolvendo a *liberdade artística em relação a fatos reais,* apresentados em filme e é considerado o paradigma em controvérsia envolvendo direito de personalidade e *liberdade de imprensa e de radiofusão*[51].

A controvérsia estabeleceu-se pelo fato de ter o canal de TV alemão *ZDF* preparado, para exibição em duas etapas, em junho de 1972, programa de televisão sobre a incursão de criminosos a depósito de munições do 261° Batalhão de paraquedistas do exército alemão, em Lebach. No primeiro episódio, seria exposto o crime de *Lebach* e os envolvidos, com seus *nomes e imagens*. No segundo episódio, haveria *reconstituição* do ataque com atuação de atores.

Conforme o processo criminal do ataque a Lebach, em 1969, quatro soldados morreram e um ficou seriamente ferido na ação de criminosos, que teriam a intenção de subtrair armamento para depois usar sua posse como meio de chantagem. Os dois principais acusados foram julgados em 1970 e, como consequência das mortes dos soldados, foram condenados à prisão perpétua. Um terceiro acusado, tido como cúmplice de menor importância, foi condenado a 6 anos de prisão, porque não tinha tomado parte diretamente na ação, mas apenas auxiliado os demais a obterem a arma usada no ataque.

O caso relevante para a discussão do direito à reabilitação e que foi trazido pelo STF à discussão no âmbito do direito ao esquecimento não é, obviamente, o criminal, brevemente descrito, mas o que se configurou a seguir, envolvendo o canal *ZDF*, pois em virtude dele *até hoje nomes e rostos de presidiários não devem ser expostos na imprensa alemã, que pode noticiar apenas os fatos, anonimamente*.

O cúmplice, que à época estava prestes a ter examinado seu pedido de liberdade condicional, buscou proibir a transmissão do programa de TV da *ZDF* por meio de liminar, por entender que a exibição seria prejudicial à sua ressocialização. O pedido foi rejeitado pelo tribunal local (Mainz), cuja decisão foi confirmada pelo tribunal recursal em Koblenz (dt. *Oberlandesgericht*), em outubro de 1972. Nesse contexto, o cúmplice apresentou queixa constitucional (dt. *Verfassungsbeschwerde*), em que, precariamente, o *Bundesverfassungsgericht* obstou a transmissão, até que julgasse definitivamente a causa.

---

[49] CROCKETT, May. The Internet (Never) Forgets, 19 SMU Sci. & Tech. L. Rev. 151 (2016). Disponível em: https://scholar.smu.edu/scitech/vol19/iss2/4

[50] WINGERT-ODY, Lisiane. *Direito e Arte*: o direito da arte brasileiro sistematizado a partir do paradigma alemão. Madri, Barcelona, B.Aires. SP: Marcial Pons, 2018, v.1. p. 54-55.

[51] BVerfGE, 35, 202-245. Julgado em 1973, o precedente diz respeito à exibição do filme documentário "*Soldatenmord von Lebach*" (pt. Assassinato dos soldados de Lebach), que narrou crime ocorrido em 1969.

No julgamento do mérito, o tribunal constitucional federal alemão reconheceu, inicialmente, a existência da liberdade de programação e radiofusão, que incluiria a seleção do material, o modo de apresentação e a forma de transmissão. Salientou que, em confronto o interesse de informação da população sobre crimes graves e os direitos de privacidade do infrator, em geral a liberdade da radiodifusão predominaria. No entanto, o tribunal esclareceu que esse não era o caso do documentário controvertido, pois não servia aos interesses de *informação atualizada*, já que *o fato era passado*, e sua narração poderia comprometer a *reabilitação* do criminoso, prestes a ser colocado em liberdade.

De fato, entendeu o tribunal que o formato de filme/documentário, com imagens e sons, na amplitude proporcionada pela TV, associada a circunstância de que *fatos reais foram trabalhados juntamente com ficção, para despertar fascinação nos telespectadores*, seria excessivamente prejudicial ao requerente, pois seria demasiadamente difícil para o público de TV, mídia que, em geral, conta com grande credibilidade, *diferenciar arte e a realidade*. Essa situação configura o problema da percepção seletiva, em que o telespectador forma inconscientemente sua opinião sobre o declarado, tendo-o como verdade – circunstância que conduziria à rejeição social do retratado, prestes a ser reinserido na sociedade.

Assim, o tribunal afirmou que o documentário seria *mais uma ameaça para a reabilitação social do criminoso, e menos veículo de informação*,[52] julgando a colisão de direitos fundamentais em favor da proteção do requerente.

O segundo caso envolvendo o assassinato dos soldados de Lebach mencionado no voto do RE 1.010.606/RJ foi referido como Lebach II. Ele diz respeito à produção de outro documentário (dt. *Dokumentation Soldatenmord – Die Schüsse von Lebach*) por *Inge Plettenberg*, desta feita para o canal *Sat1*, e que, após longa disputa jurídica[53], foi ao ar em 2005.

Nesse novo julgamento, o tribunal constitucional federal alemão pontuou que no acórdão de 1973, o fator decisivo foi a *ameaça de ressocialização*, questão que seria de alta prioridade e genuinamente relevante para a personalidade, se o programa de televisão da ZDF tivesse sido transmitido – situação que não se verificaria em relação ao documentário do canal *Sat1*.

No novo programa, porém, a possibilidade de identificação do cúmplice seria possível apenas em relação às pessoas que já o conheceriam como participante dos assassinatos de Lebach, não renovando sua estigmatização ou isolamento. O tribunal sinalou, ainda, que o tempo expressivo decorrido desde que o crime foi cometido também deveria ser levado em consideração, pois, em regra, a indignação com as ações dos perpetradores se desvaneceria com o passar dos anos. Nesse contexto, concluíram que limitar o direito de radiofusão não seria acertado.[54]

---

[52] No Brasil, caso análogo e que obteve o mesmo resultado, com ênfase ao argumento no direito ao esquecimento é o REsp 1334097/RJ, rel. Min. Luis Felipe Salomão, Quarta Turma, julgado em 28.05.2013, DJe 10.09.2013.

[53] BVerfG, 1 BvR 348/98 de 25 de novembro de 1999.

[54] Outro caso análogo, não referido no acórdão do STF, mas de importância na jurisprudência alemã sobre o direito à reabilitação, é o de canibal de Rotemburgo (Kannibale von Rohtenburg), em que foi adotada compreensão diversa de Lebach, porque de substrato fático diferente (BGH AfP 2009, 398; BVerfG ZUM-RD 2009, 574). O caso trata de obra baseada em história real, com acréscimo de ficção, que narra a história de um jovem (Armin Meiwes), profissional da computação, que conheceu em fórum da internet engenheiro (Bernd Brandes), o qual manifestou o desejo de ser morto e devorado por outro ser humano. Em 2001, num encontro agendado entre eles, o primeiro matou o segundo e congelou parte de sua carne. Meiwes filmou a maior parte

Como se percebe, foi feita exatamente a mesma ponderação. O resultado oposto, porém, decorreu da mudança do substrato fático: em lugar de um presidiário prestes a ser reinserido na sociedade para ressocialização e que teria seu nome e imagem veiculados na TV em programa que mesclava fatos reais e ficção, tinha-se um indivíduo já reinserido na sociedade há mais de 25 anos, sendo que o novo documentário não o identificava de forma individualizada.

1.2 Direitos ao próprio nome e imagem: *Melvin v. Reid*

Outra referência do direito comparado no precedente do STF é ao artigo de *Warren* e *Brandeis,* que desenvolveram o conceito de *right to privacy* nos Estados Unidos em artigo da *Harvard Law Review*, em 1890[55]. Segundo eles, seria *é o direito do indivíduo determinar, ordinariamente, em que extensão seus pensamentos, sentimentos e emoções serão comunicados a outros*[56]. Caso americano que tratou da questão foi *Melvin v. Reid*, de 1931[57], também referido no voto condutor. Ele envolve a história de *ex-prostituta* acusada de homicídio, que fora absolvida e reconstituíra sua vida, tendo sido posteriormente arrastada para um turbilhão quando lançado o filme "*The red kimono*", que narrava o crime *fazendo uso de seu nome*.

---

de sua ação, inclusive o consumo posterior da carne humana do engenheiro morto. O indivíduo aguardava o julgamento pelo fato quando tomou conhecimento do filme, insurgindo-se contra essa representação da história, que reconheceu como sua, ainda que usados nomes e contexto diferentes, porque o retratava como "assassino monstruoso". Disse que nunca concordou que sua vida fosse retratada em filme, especialmente considerando o processo criminal em andamento. Em primeira instância, seu pedido foi acolhido pelo tribunal de Frankfurt, que entendeu que o ferimento a sua personalidade seria mais expressivo do que o produto artístico do caso, porque Meiwes foi apresentado como assassino selvagem e o filme foi anunciado como Terror-Real, o que ensejaria um prejulgamento por parte da audiência e da mídia. No filme, o acontecimento é examinado por uma jovem americana, que vive na Alemanha, estuda psicologia criminal e prepara trabalho de conclusão com o tema "o assassino canibal homossexual". Em seu texto, ela examina a vida dos principais envolvidos, sendo que parte substancial dos dados corresponde à vida real.

O julgamento do caso pelo tribunal federal superior (*BGH - Bundesgerichthof*), em 2009, reformou a decisão da instância inferior anterior, liberando o filme para exibição e afastando o direito à reabilitação. Na fundamentação, argumentou o tribunal, que atua de forma similar ao STJ brasileiro, que o próprio requerente tornou públicos todos os fatos e as circunstâncias apresentados no filme, pois os descreveu em detalhes em uma entrevista, na qual manifestou, ainda, a sua intenção de publicar um livro e filmar sua visão dos fatos e circunstâncias – motivo pelo qual entendeu não haver interferência em núcleo essencial de sua personalidade. Ao contrário, sustentou que o artigo 2, 1, da Lei Fundamental alemã não assegura um direito de ser mostrado ao público apenas como o indivíduo vê a si mesmo ou gostaria de ser visto por outros, concluindo que a exibição do filme não traria consequências adversas novas ou adicionais para o requerente na sua reabilitação. Sobre o tema: WINGERT-ODY, Lisiane. *Direito e Arte*: o direito da arte brasileiro sistematizado a partir do paradigma alemão. Madri, Barcelona, B.Aires. SP: Marcial Pons, 2018, v.1. p. 56 e seguintes.

[55] Sobre a contribuição desse caso à percepção contemporânea de intimidade e vida privada no direito brasileiro, veja-se: CACHAPUZ, Maria Claudia. *Intimidade e vida privada no novo Código Civil brasileiro*: uma leitura orientada no discurso jurídico. Porto Alegre: Sérgio Antonio Fabris Editor, 2006. p. 76-99.

[56] No original: "*right of determining ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others*".

[57] Melvin v. Reid, 112 Cal. App. 285 (Dist. Ct. App. 1931).

Diversamente do caso Lebach, não houve condenação da acusada, motivo pelo qual não as circunstâncias não se amoldariam perfeitamente no que se concebeu chamar na *Civil Law* de direito à reabilitação/ressocialização. O tribunal, porém, considerou o fato de *Ms. Melvin* ter atuado por anos como prostituta como algo vergonhoso, aduzindo que, tendo ela abandonado "*her life of shame*", "*rehabilitated herself and had taken her place as a respected and honored member of society*", deveria lhe ser permitido continuar nesse curso sem ter sua reputação e posição social prejudicadas com a publicação de "*story of her former depravity with no other excuse than the expectation of private gain by the publishers*".

De certa forma, portanto, ponderaram entre o direito da demandante reconstruir sua vida, "reabilitando-se" após "vida de vergonha" e o direito ao lucro de terceiros, que não tinham autorização para usar *seu nome*, decidindo favoravelmente pelo primeiro.

Esse exemplo deve ser compreendido, porém, como exceção. De uma maneira geral pode-se afirmar que limitações à liberdade de expressão vão contra valores fundamentais norte-americanos[58], que destacam a liberdade em detrimento da privacidade, como o que se vê no tratamento da imprensa – em cujo âmbito a responsabilidade civil exige dolo (en. *actual malice*)[59] como elemento do suporte fático. Em uma série de julgados a *US Supreme Court* sustenta o entendimento de que o reportar histórias reais é interesse da imprensa e se insere em liberdade constitucional, ainda que possa causar embaraço ou danos aos envolvidos[60]. Mas se deve destacar: nem sempre os tribunais americanos se revelam inclinados a insistir no acesso irrestrito à informação, como se vê no caso *Nixon v. Warner Communications, Inc*., em que a SCOTUS reconheceu existir direito geral de inspecionar e copiar registros públicos, mas também sugeriu que os tribunais devem exercer seus poderes de supervisão para impedir o acesso a informações para "uso

---

[58] BENNETT, Steven C. *The "Right to Be Forgotten"*: Reconciling EU and US Perspectives, 30 Berkeley J. Int'l Law. 161, 2012, p. 161-168.

[59] O paradigma do caso é o precedente *New York Times Co. v. Sullivan,* julgado pela Suprema Corte Americana. Nele restou decidido que, havendo eventual alegação de difamação por notícia veiculada na imprensa, incumbe ao difamado provar que a empresa jornalística sabia que a informação era falsa, tendo agido com *actual malice*, isto é, com dolo. A Primeira Emenda da Constituição Americana previu a liberdade de imprensa e a de expressão, porém não trouxe, inicialmente, muita proteção a oradores públicos não populares e organizações jornalísticas. O contexto histórico americano assim o confirma. O *Sedition Act* de 1798 dispunha a criminalização da crítica a autoridades de governo, tendo a *Supreme Court* decidido em muitos julgamentos que publicações difamatórias não estariam incluídas nessa proteção. *New York Times Co. v. Sullivan* representou o fim dessa compreensão. Nele, a controvérsia sequer envolvia uma reportagem, mas mero anúncio, no qual *concerned citizens* pediam apoio ao reverendo *Martin Luther King Jr.* diante de violência policiais em manifestações no Alabama. *Sullivan*, que era o comissário de polícia, o Governador do Estado e outras autoridades locais processaram o jornal, demandando 3 milhões de dólares em danos morais. As decisões favoráveis das instâncias ordinárias foram revertidas pela *Supreme Court*, que atribuiu à *imprensa "the right to be wrong"*, tornando-a responsável apenas nos casos em que restasse provado o dolo na difusão de informação falsa. Sobre o caso, leia-se: MAURO, Tony. *The Supreme Court Landmark decisions*: 20 cases that chenged America. New York: Fall River Press, 2016. p. 67-77.

[60] Veja-se o exemplo de The Florida Star v. B.J.F., 491 U.S. 524, 532 (1989). Em: BENNETT, Steven C. *The "Right to Be Forgotten"*: Reconciling EU and US Perspectives, 30 Berkeley J. Int'l Law. 161, 2012, p. 170-171.

impróprio", como para fins de "gratificar o rancor privado" ou "promover o escândalo público"[61].

A invocação de precedentes europeus e norte-americanos no âmbito de direitos de personalidade (en. *rights relating to personality; right to privacy*) deve considerar a diferença abissal entre as visões tradicionais da União Europeia e dos Estados Unidos sobre o tema (também em relação a dados): enquanto a primeira tem alto grau de envolvimento governamental nos direitos fundamentais para preservar o indivíduo em face do Estado, como o RGPD, os segundos têm editado leis reativas, em tópicos específicos, criando uma colcha de retalhos jurídica.

Não obstante essa fragmentação, existem indicativos de que os Estados Unidos estariam mais receptivos a discutir o mérito de intensificar a proteção de dados no país, o que poderia ser uma excelente oportunidade de harmonizar seu substrato normativo da proteção de dados com o europeu[62]. Isso porque o desenvolvimento tecnológico, o uso cada vez mais intenso de internet e o incremento do comércio eletrônico decorrente da globalização tornam inevitável revisar os standards de privacidade americanos[63] - o que não significa inverter (ou subverter) o sistema jurídico vigente, mas regular soluções para situações específicas[64], o que pode ter sido a intenção do STF, ainda que não tenha tecido considerações sobre quando a conservação da informação no meio eletrônico seria abusiva e, portanto, merecedora de remoção[65].

Exibidos os contextos fáticos e a fundamentação jurídica dos casos referidos pelo relator do tema 786 no STF, fica claro que, embora tenham relação com o esquecer, o superar, de fatos passados, não tem relação com o *direito ao esquecimento* - que, *tecnicamente*, tem outros contornos, associados de forma inarredável ao mundo digital -, estando afeitos, sim, ao direito à reabilitação e ao próprio nome e imagem. Para o direito ao esquecimento se afigurar, deve haver, como se demonstrará a seguir, *a disponibilização de dados desatualizados e irrelevantes, mas prejudiciais, no meio digital*.

Tem havido, porém, confusão no direito brasileiro entre o direito à reabilitação ou ressocialização (e outros direitos de personalidade) e o direito ao esquecimento, tanto no âmbito civil[66], quanto no campo do direito penal – em que se consolidou a compreensão de que, quando registros da folha de antecedentes do réu são muito antigos, pode ser afastada sua análise desfavorável[67]. Pode-se inferir que essa circunstância decorre de "*atalhos* e

---

[61] 435 U.S. 589 (1978).

[62] BENNETT, Steven C. *The "Right to Be Forgotten"*: Reconciling EU and US Perspectives, 30 Berkeley J. Int'l Law. 161, 2012, p. 175 e seguintes; U.S. Federal Trade Commission Staff Comments On The European Commission's November 2010 Communication On Personal Data Protection In The European Union 1-2, Jan. 13, 2011 In: http://www.ftc.gov/os/2011/01/111301dataprotectframework.pdf.

[63] BENNETT, Steven C. *The "Right to Be Forgotten"*: Reconciling EU and US Perspectives, 30 Berkeley J. Int'l Law. 161, 2012, p. 178.

[64] A necessidade de aproximação decorre da questão de problemática autoevidente que é a jurisdição para tornar efetivo o direito ao esquecimento. Na região sem fronteiras do ciberespaço, não se pode adotar a compreensão estreita da territorialidade.

[65] Para não fugir do tema central da pesquisa, que é o *direito ao esquecimento,* não se abordará as questões de exclusão de dados e sua anonimização.

[66] REsp 1736803/RJ, Rel. Ministro RICARDO VILLAS BÔAS CUEVA, TERCEIRA TURMA, julgado em 28/04/2020, DJe 04/05/2020.

[67] AgRg no HC 503912/SP, Rel. Ministro ROGERIO SCHIETTI CRUZ, SEXTA TURMA, julgado em 03/09/2019, DJe 09/09/2019; AgRg no AREsp 1463495/PR, Rel. Ministro ANTONIO

facilitações" muitas vezes tomadas para tornar acessível o direito comparado a indivíduos que não têm compreensão de idioma e cultura jurídica estrangeiros[68].

O direito à reabilitação não tem, porém, os mesmos contornos do direito ao esquecimento, podendo confundir-se com ele apenas na hipótese da ameaça à ressocialização se dar no meio digital, ao qual o direito ao esquecimento é imediatamente conectado – como os casos *González e Google España,* do tribunal europeu, e *Recht auf Vergessen I und II*, do tribunal constitucional alemão claramente evidenciam.

É preciso consignar, ainda, que o caso da *família Curi e Rede Globo* não têm similitude fática nem com o direito à reabilitação e nem com o direito ao esquecimento: não guarda semelhança com o primeiro, porque não são os criminosos que buscaram impedir a veiculação do programa, mas a família da vítima, que buscou ser poupada de reviver, em público, tragédia ocorrida há décadas; não se amolda, tampouco ao direito ao esquecimento, embora claramente a família queira, em termos leigos, "esquecer" o episódio, porque a transmissão do programa em rede de TV não tem relação a dado desatualizado e irrelevante, disponibilizado de forma permanente na internet.

A renovação do sofrimento da família a propósito da violência de que foi vítima a jovem *Aída Curi* evidencia a razão pela qual buscou na justiça obter reparação: foi-lhe negado seu *direito à privacidade* após tantos anos. Esse direito se confrontou com o direito de radiofusão de programa de TV, não jornalístico e voltado a retratar crime atual, mas, misturando ficção e fatos reais, a sinalar a impunidade que impera neste país. Nesse contexto deveria ter se dado o exame pelo tribunal, sendo que eventual reconhecimento de *licitude* da transmissão não inviabiliza indenização, pois há 20 anos a codificação civil brasileira admite de forma expressa a reparação de dano decorrente de ato lícito.

2. A essencialidade do meio digital à conformação do direito ao esquecimento

2.1 Direito europeu anterior ao Regulamento Geral sobre a Proteção de Dados: Caso González v Google España

Há na tese fixada a partir do julgado do RE 1.010.606/RJ[69] pelo menos um equívoco conceitual e uma impropriedade flagrante, que conduziram a uma contradição lógica.

O tribunal lançou como conceito de direito ao esquecimento "*o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e* ***publicados em meios de comunicação social***". Há equívoco conceitual, pois não é esse o âmbito em que o direito ao esquecimento se insere, pois, como se demonstrará a seguir, o direito ao esquecimento não se condiciona a publicação em meio de

SALDANHA PALHEIRO, SEXTA TURMA, julgado em 06/08/2019, DJe 13/08/2019; AgRg no HC 493749/MG, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 06/08/2019, DJe 12/08/2019; RHC 89948/RS, Rel. Ministro RIBEIRO DANTAS, QUINTA TURMA, julgado em 18/06/2019, DJe 25/06/2019; AgRg no REsp 1751708/SP, Rel. Ministro SEBASTIÃO REIS JÚNIOR, SEXTA TURMA, julgado em 05/02/2019, DJe 22/02/2019; HC 391015/MS, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 16/05/2017, DJe 24/05/2017.

[68] FEITEN WINGERT ODY, Lisiane. Direito e Linguagem: Direito comparado e línguas estrangeiras – o papel da tradução. *Direito comparado Alemanha-Brasil vol. II*: Temas de Direito privado em estudos originais e traduzidos. Porto Alegre: Faculdade de Direito da UFRGS, 2022. p. 9-20.

[69] Leia-se: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1.

comunicação social[70], mas à disponibilidade da informação prejudicial, desatualizada e irrelevante, no *ambiente digital* – podendo ela ter sido anteriormente publicada em meio de comunicação social ou não. De fato, a informação pode ser extraída de arquivos ou bases de dados, por exemplo.

A impropriedade flagrante está na referência expressa ao meio *análogico*, que é estranho ao tema do direito ao esquecimento, que se insere no contexto *digital,* decorrente da sociedade de informação e conhecimento em que se vive na atualidade[71].

A contradição lógica (decorrente do equívoco da premissa) está na afirmação de ser "***incompatível com a Constituição Federal a ideia de um direito ao esquecimento",*** mas ao mesmo tempo aduzir que "*eventuais excessos ou abusos no exercício da liberdade de expressão e de informação* ***devem ser analisados caso a caso, a partir dos parâmetros constitucionais".*** Ora, se eventuais abusos devem ser analisados é porque, em alguma medida, há compatibilidade do direito com a Constituição – o que intuitivamente ministros reconheceram, confundindo-o, porém, com outras manifestações de direito de personalidade, como direito à privacidade, à reabilitação e ao nome e imagem, por exemplo.

De fato, a compreensão do STF no precedente, que refere direito a esquecimento em *meio analógico* – confunde o direito ao esquecimento com o direito à reabilitação e com os direitos à imagem e nome da vítima ou mesmo à privacidade dos sucessores[72], em compreensão dissociada da teoria jurídica internacional, em decorrência do uso *não técnico* do termo.

O mesmo parece ocorrer com o STJ, que tem adotado a compreensão de que "*a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento*", entendido como direito de não ser lembrado contra sua vontade, especificamente no tocante a fatos desabonadores à honra[73]. Geralmente, porém, os julgados não se referem propriamente a dados disponíveis na *internet*, mas a fatos veiculados em mídias, como a TV, dizendo respeito, outrossim, ao direito de reabilitação, já consolidado – o que não é o contexto em que concebido do direito ao esquecimento em ordenamentos estrangeiros.

---

[70] São meios de comunicação social conhecidos livros, jornais, revistas, rádio, cinema, televisão, gravações, como discos, cassetes, VHSs, CDs, DVDs, blu-rays, cartões de memória etc., video games e internet.

[71] FEITEN WINGERT ODY, Lisiane. Direitos autorais e sociedade de informação e conhecimento: por um direito de uso adaptado à era digital. In: Propriedade Intelectual – Sociedade de Informação – Inteligência Artificial (FERNANDES, Marcia; CALDEIRA, Cristina (org). No prelo.

[72] A leitura do inteiro teor do julgado, de nada menos que 331 páginas, corrobora essa primeira impressão, pois o substrato fático do recurso em que o STF se pronunciou, sob o rito da repercussão geral, diz respeito à ação indenizatória proposta por sucessores de Aída Curi, assassinada em 1958, que se insurgiam contra o uso não autorizado do nome e imagem dela em programa televisivo que tratava de crimes não resolvidos (Linha Direta Justiça, exibido pela TV Globo). Não há referência a informações armazenadas eletronicamente – que é o requisito fundamental do direito ao esquecimento.

[73] REsp 1660168/RJ, Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 08/05/2018, DJe 05/06/2018; AgInt no REsp 1599054/RJ, Rel. Ministro MOURA RIBEIRO, TERCEIRA TURMA, julgado em 25/04/2017, DJe 11/05/2017; AgInt no REsp 1593873/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 10/11/2016, DJe 17/11/2016; REsp 1369571/PE, Rel. Ministro RICARDO VILLAS BÔAS CUEVA, Rel. p/ Acórdão Ministro PAULO DE TARSO SANSEVERINO, TERCEIRA TURMA, julgado em 22/09/2016, DJe 28/10/2016; REsp 1334097/RJ, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 28/05/2013, DJe 10/09/2013.

Claro que os tribunais brasileiros não se submetem à compreensão da Justiça estrangeira, menos ainda o STF a qualquer outro tribunal, mas seria positivo que nosso ordenamento não fosse na contramão do avanço jurídico internacional – especialmente quando, o fazendo, diminui a proteção oferecida a brasileiros.

A tese do direito ao esquecimento teve origem na pessoa do cientista jurídico e político austríaco *Viktor Mayer-Schönberger,* que defende que as *informações armazenadas eletronicamente* tenham data de validade ou expiração, para que uma *informação digital com referência pessoal* não fique permanentemente disponível[74].

Trata-se de direito que emerge de uma realidade tecnológica atual[75], que, positivamente, tornou informação acessível a todos, mas que, negativamente, *não tem filtros* – morais, temporais, autorais, ou quaisquer outros.

Antigamente, dizia-se "papel aceita tudo"; hoje, dir-se-ia "internet aceita tudo" – inclusive mentiras, notícias inventadas (*fake news*), imagens e palavras de terceiros alheios à publicação, por exemplo. A diferença é que "*internet never forgets*"[76], ao contrário dos seres humanos.

Diz-se em alemão *der Schein trügt* e em inglês *looks can be deceptive,* o que em português também é máxima popular: as aparências enganam. É certo que não existe um direito de ser mostrado ao público apenas como o indivíduo vê a si mesmo ou gostaria de ser visto por outros. Porém, também é certo que nem tudo que acontece com um determinado indivíduo é da conta de toda a coletividade até o final dos tempos. Por isso, *não há sacralidade na manutenção de informações superadas na internet indefinidamente.*

---

[74] Veja-se em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.

2016 .119.01.0001.01. ENG &toc=OJ:L:2016: 119:FULL>.

[75] Vive-se em sociedade em que a tecnologia é onipresente. Por questões ideológicas ou terminológicas, pode-se distinguir entre sociedade de informação e sociedade de conhecimento. A sociedade de informação caracteriza-se, singelamente, pela presença de tecnologias de comunicação e informação em todos os âmbitos da vida. São três os alicerces dessa sociedade: (i) os direitos fundamentais de comunicação (dt. *Kommunikationsgrundrechte*), como as liberdades de opinião, de imprensa e de radiofusão, por exemplo; (ii) o direito de acesso à informação (dt. *Informationszugangsfreiheit*); (iii) a proteção de dados (dt. *Datenschutz*); (iv) a proteção de segredos (dt. *Geheimschutz*); e (v) direitos de personalidade, como o direito à própria imagem (dt. *Recht am eigenem Bild*) e os direitos autorais (dt. *Urheberrecht*), por exemplo. Veja-se: VON DIX, Alexander; FRANSSEN, Gregor; KLOEPFER, Michael; SCHAAR, Peter; SCHOCH, Friedrich; VOSSHOFF, Andrea (org.). *Informationsfreiheit und Informationsrecht*. Berlin: Lexxion Verlagsgesellschaft, 2015. A sociedade de conhecimento, por sua vez, seria aquela que transforma a informação e interpreta dados, gerando, compartilhando e tornando disponível o conhecimento. Relatório Mundial da UNESCO - Organização das Nações Unidas para a Educação, a Ciência e a Cultura apresenta definição, conteúdo e prognóstico para o futuro das sociedades de conhecimento. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000232575. Sem deter-se em eventuais distinções entre sociedade de informação e conhecimento, o presente trabalho tem por ponto de partida o fenômeno fático inconteste: vivemos num mundo que, em lugar de valorizar átomos, valorizamos informações em *bits*. Cf. MURRAY, Andrew. Information, Technology Law: the Law & Society. Oxford: OUP, 2019.

[76] CROCKETT, May. The Internet (Never) Forgets, 19 SMU Sci. & Tech. L. Rev. 151 (2016). Disponível em: https://scholar.smu.edu/scitech/vol19/iss2/4.

O paradigma do tema na Europa foi o *Google v. AEPD*[77], em que foram partes a *Google Spain SL, Google Inc.* contra a *Agencia Española Proteccion de Datos* e *Mario Costeja González*. A compreensão nele estabelecida foi a depois incorporada no Regulamento geral sobre a proteção de dados (en. *General Data Protection Regulation - GDPR),* que foi, ostensivamente, a inspiração do legislador nacional para a Lei geral de proteção de dados (Lei 13.0709/2018). Todavia, deve-se destacar que antes mesmo desse caso ser julgado, precedentes históricos, normativos e jurisprudenciais reconheciam o direito ao esquecimento na Europa[78].

Na controvérsia *Google v. AEPD*, *González* demandava a remoção de seus dados pessoais da base de dados do jornal *La Vanguardia*, que expunham anúncio de procedimentos para leilão de imóvel em virtude de não-pagamento de débitos para com a seguridade social. Os fatos não eram mentirosos, mas verdadeiros; porém, eram irrelevantes depois de passados muitos anos desde o episódio, sendo-lhes prejudiciais porque indicariam ser ele "mau-pagador". Por esse motivo, o autor requereu que as páginas do jornal fossem removidas – ou delas suprimidos seus dados – e que o buscador, Google, não mais relacionasse consulta a seu nome a esse resultado – ou que o ocultasse.

O Tribunal de Justiça da União Europeia decidiu que a interpretação da *privacidade no processamento de dados* não deveria ser restritiva; manifestou, porém, que essa proteção *não poderia ser absoluta*, de forma a sopesar direitos e interesses antagônicos. Concluiu, em síntese, *ser devida a remoção de informação imprecisa, inadequada, irrelevante ou excessiva em relação a seus propósitos, desatualizada ou conservada por tempo superior ao necessário para seu fim, sem justificativa histórica, estatística ou científica*. Aduziu, por fim, que o buscador que desatendesse ao pedido, estaria sujeito à demanda judicial pelo titular dos dados.

O paradigma não assegurou um direito ao esquecimento, mas *tornou as informações que satisfazem os critérios acima mais difíceis de se localizar*. O Regulamento geral sobre a proteção de dados europeu, sim, foi além, passando a prever o direito ao esquecimento, juntamente com o direito de pagar dados (de menor amplitude, o qual será abordado a seguir), no seu artigo 17, ressalvando hipóteses de interesse público no exercício de liberdade de expressão, como casos de saúde pública, interesses históricos, estatísticos ou de pesquisa científica, e os casos de obrigação legal de conservação de dados[79].

De fato, a positivação do direito ao esquecimento na Europa emergiu dos artigos 7º e 8º da Carta de Direitos Fundamentais da União Europeia[80], que preveem o respeito à *vida*

[77] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R.

[78] Diretiva 95/46, 1995 O.J. (L 281) 31 (EC), que dispõe sobre o direito à privacidade.

[79] CROCKETT, May. The Internet (Never) Forgets, 19 SMU Sci. & Tech. L. Rev. 151 (2016). Disponível em: https://scholar.smu.edu/scitech/vol19/iss2/4, p. 165.

[80] https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_pt

privada e familiar e a *proteção de dados pessoais*[81] - direitos que são igualmente protegidos no Brasil, conforme os incisos X e LXXIX do artigo 5º da Constituição.[82]

Análogos os substratos normativos, é de se lamentar que não se tenha reconhecido ao cidadão brasileiro proteção de mesma amplitude. Para demonstrar o contexto dos direitos de esquecimento e de apagar dados (dt. *löschen*; usou-se os termos eliminação ou exclusão em português, na LGPD), passa-se a expor os casos-paradigma do tema no direito alemão, após o advento do RGPD europeu – o qual, *mutatis mutantis* é a base da LGPD brasileira.

2.2 Direito alemão posterior ao Regulamento Geral sobre a Proteção de Dados: *Recht auf Vergessen I und II*

O tribunal constitucional federal alemão recentemente julgou dois casos de direito ao esquecimento, já em face da regulamentação europeia. Os casos ficaram conhecidos como Recht auf Vergessenwerden I e II, literalmente traduzíveis para o português como Direito ao esquecimento I e II.

---

[81] Artigo 7º - Respeito pela vida privada e familiar

Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8º - Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[82] A par do acerto em reconhecer o direito ao esquecimento – entendido em sua concepção técnica, dogmática – no Regulamento geral sobre a proteção de dados, essa compreensão resulta, porém, numa transferência curiosa de atribuições e responsabilidades. A questão é que se transferiu ao Google – sem dúvida o mais importante entre todos os buscadores – o tomar de decisões que são publicamente relevantes, quase como um tribunal ou governo – porém sem seus órgãos de controle. Em outras áreas, tem havido fenômenos análogos, como no controle do direito autoral (Diretiva sobre Direito Autoral 2016/0280), por meio de filtros prévios de upload, e a recente remoção de Trump do Twiter (Notícia do fato em: https://www.cnnbrasil.com.br/internacional/2021/02/11/cfo-do-twitter-banimento-de-trump-e-permanente-mesmo-com-nova-candidatura; https://brasil.elpais.com/tecnologia/2021-01-09/twitter-suspende-permanentemente-a-conta-de-trump.html; https://www.bbc.com/portuguese/internacional-55674897; https://g1.globo.com/economia/tecnologia/noticia/2021/01/08/twitter-tira-conta-de-trump-do-ar.ghtml; todos de acesso realizado em 27.02.2021). Outra implicação grave: a geolocalização do usuário, já usada antes para inibir acessos em virtude de regulamentação dos direitos autorais, agora serve para assegurar que europeus não tenham acesso a versões do site vistas em outros lugares do mundo – o que já compromete a base fundamental da World Wide Web, seu acesso internacional CROCKETT, May. The Internet (Never) Forgets, 19 SMU Sci. & Tech. L. Rev. 151 (2016). Disponível em: https://scholar.smu.edu/scitech/vol19/iss2/4, p. 167)

O caso Recht auf Vergessenwerden I[83] emergiu de ação proposta por indivíduo que fora condenado, em 1982, por matar duas pessoas num iate, em alto mar, em 1981. O periódico Der Spiegel publicou, entre 1982 e 1983, três artigos sobre o caso, referindo o condenado por nome. Ocorre que, desde 1999, a Spiegel Online GmbH, proprietária do periódico, disponibiliza os relatórios de publicações antigas em um arquivo online, de forma gratuita e sem barreiras de acesso. Assim, quando inserido o nome do requerente em um portal de busca comum na internet, como o Google, Safari etc. esses artigos eram exibidos entre os primeiros resultados. Diante desse quadro, o demandante, que tinha sido libertado da prisão em 2002, pediu na justiça, em 2009, que a ré fosse proibida de associar o crime a seu sobrenome, o que foi inicialmente negado, com base no interesse do público pela informação e ao direito à liberdade de expressão do grupo jornalístico.

O recurso foi provido, porém, pelo tribunal constitucional, com base na proteção ao direito de personalidade consagrado na Constituição alemã, no qual consideraram inserido o direito ao esquecimento, que prevaleceria em face da liberdade de opinião e imprensa porque o conflito envolvia informações pessoais no processo de comunicação pública na internet.

Como se sabe, são várias as manifestações que protegem a personalidade de um indivíduo, como nome, imagem, privacidade, autodeterminação informativa, por exemplo. No caso, o tribunal não teve por relevante o direito à autodeterminação informativa, por considerar que ela protege principalmente contra o processamento e o uso não transparente de dados pessoais. Dos fundamentos do julgado, extrai-se, porém, dois elementos centrais: (i) o tempo tem peso específico na comunicação na internet; (ii) o ordenamento jurídico deve proteger os indivíduos contra a disponibilização ao público indefinidamente de posições, declarações e ações superadas.

O tribunal declarou, entretanto, de forma expressa, que não há direito de filtrar informações acessíveis ao público de acordo com sua própria livre decisão e apenas com suas próprias ideias e de limitá-las aos aspectos que a pessoa em questão considera relevantes ou relevantes para sua própria imagem. Consignou, também, não pode haver limites de tempo ou prazos rígidos, devendo-se examinar cada situação.

O segundo caso, Recht auf Vergessenwerden II, tem contexto ligeiramente diverso, pois não envolve crime e nem publicação em jornal. Uma diretora de empresa, ao consultar seu nome num buscador, constatou que era exibido link para relatório da NDR, do ano de 2010, intitulado "Demissão: truques maldosos dos empregadores" (dt. Kündigung: Die fiesen Tricks der Arbeitgeber), na qual fora entrevistada depois de acusações de tratamento injusto de empregado sob sua supervisão. Por esse motivo, requereu na justiça a remoção do resultado.

O tribunal constitucional, porém, ponderou que o buscador tem liberdade empresarial e que restringir os resultados de sua utilização para omitir a entrevista em questão limitaria a liberdade de expressão jornalística da Norddeutscher Rundfunk, que fez a reportagem. Considerou não haver precedência em tese de direitos fundamentais de estatura constitucional, a serem avaliados em pé de igualdade, e anotou que a própria requerente consentira com a entrevista posteriormente impugnada e que o fator tempo não era ainda expressivo.

Como se vê, o direito ao esquecimento, reitera-se, no sentido técnico do termo, é indissociável do meio eletrônico. A questão fundamental que o enseja está no fato de que dados – e também reportagens na imprensa e na radiodifusão - costumavam estar disponíveis ao público apenas por um período limitado de tempo. As possibilidades quase

[83] Julgamento de 06.11.2019, ref.: 1 BvR 16/13.

ilimitadas de armazenamento de conteúdo na internet garantem, porém, que esse conteúdo possa agora ser acessado mesmo depois de muitos anos, quando já desatualizados, obsoletos.

Ferramentas disponíveis na internet para captura de conteúdo, indexam e fornecem links para outros sites quando certas palavras-chave são inseridas. Dessa forma, uma simples busca por nome em um buscador, proporciona visão geral estruturada de todas as informações disponíveis na internet sobre uma pessoa. Assim, os meios social e profissional podem aprender muito sobre uma pessoa, sem esforço, mesmo que os dados sejam desatualizados, irrelevantes e prejudiciais.

Deve-se distinguir, porém, entre o direito ao esquecimento e o direito ao apagamento de dados, mencionado pelo Ministro Gilmar Mendes, que os igualou (p. 246 do PDF), embora haja certa convergência entre eles. Esses direitos têm contornos diversos. O direito ao apagamento importa em que dados pelos quais o responsável não tem mais base legal para processamento devam ser apagados. Isso pode se dar porque (i) o consentimento foi revogado; (ii) o processamento no interesse legítimo do controlador foi contestado; (iii) os períodos contratuais de retenção dos dados expiraram; (iv) a finalidade para a qual os dados foram tratados e armazenados foi plenamente alcançada; ou (v) essa finalidade já não pode mais ser alcançada.

O direito ao esquecimento diz respeito a dados que chegaram a público a partir de rastros em índices de buscadores na internet e que são muito mais fáceis de encontrar hoje do que nos antigos arquivos. Para ainda permitir que o público "deixe em paz" e "esqueça" esses dados é que foi decidido no Google España que motores de busca podem, em certos casos, ser obrigados a apagar resultados do passado de buscas sobre pessoas.

Outra diferença entre o direito de apagar e o direito ao esquecimento está em que o primeiro se aplica ao responsável pela coleta dos dados, enquanto o segundo também se estende a terceiros. Assim, um editor de imprensa, por exemplo, que tenha publicado dados de uma pessoa deve garantir que terceiros removam os links no caso do direito ao esquecimento. Com o direito de apagamento, todos os dados coletados sobre o indivíduo podem ser apagados de forma mais direta - no entanto, isso não alcança dado que possa ter sido repassado a terceiros anteriormente. Os buscadores, isto é, mecanismos de busca – dos quais o Google é, sem dúvida, o mais importante – estão no centro, portanto, das discussões jurídicas acerca do tema do direito ao esquecimento.

O STF falhou em não reconhecer – pelo menos em tese, porque o caso específico não guarda relação com o tema –, à semelhança do Tribunal de Justiça Europeu no caso Google España, o direito à prevalência da vida privada e familiar e à proteção de dados pessoais sobre o interesse econômico do operador do mecanismo de busca e também sobre interesse do público em geral no acesso à informação quando ela é desatualizada, irrelevante e pode ser prejudicial. Aliás, em duas decisões posteriores, ainda em 2019, o TJE aplicou essa mesma compreensão e as especificou ainda mais (acórdão de 24.09.2019, Ref: C-136/17; acórdão de 24.09.2019, Ref: C- 507/17).

Em virtude desse reconhecimento pelo TJE que atualmente, o art. 17 GDPR dispõe de um direito de apagamento e esquecimento, permitindo que resultados sejam removidos de todas as versões do mecanismo de busca da União Europeia (não do mundo todo) se os direitos da pessoa interessada prevalecerem.

O STF já se mantivera analógico e alheio à realidade que a tecnologia impôs quando do julgamento da constitucionalidade da Medida Provisória 954, que previa o compartilhamento de dados pessoais de consumidores entre as empresas de

telecomunicação e o IBGE, na ADI 6.387. Da leitura do acórdão daquele julgamento – que teve votos individuais de 7 dos 9 dos ministros que acompanharam a relatora e 1 único voto divergente – revela consenso quanto à inconstitucionalidade da referida MP, mas não a respeito do direito fundamental que ensejou seu reconhecimento[84] - como aconteceu novamente no RE em exame. Apenas 2 ministros referiram expressamente a existência de um direito fundamental à autodeterminação informativa na Constituição brasileira, tendo os demais optado pela interpretação mais confortável de que a inconstitucionalidade decorreria da inviolabilidade da vida privada e o sigilo de dados.

A grande questão, porém, é que a mera interpretação extensiva dos direitos à privacidade ou sigilo oferece apenas defesa do cidadão perante o Estado, mas não tem efeitos entre particulares (eficácia horizontal dos direitos fundamentais) e nem constitui dever de proteção do particular pelo Estado (dimensão objetiva). A mesma consequência imediata se revela do não reconhecimento do direito ao esquecimento como direito fundamental autônomo. Não se trata de mera questão formal ou detalhe técnico irrelevante, tendo sido um avanço na ordem legislativa brasileira a inclusão, pela Emenda Constitucional 115/2022, do direito à proteção de dados, no inciso LXXIX do artigo 5º da Constituição. Por meio dela o lapso no julgamento do STF no julgamento da ADI 6.387 quanto à proteção de dados e autodeterminação informativa foi superado, inserindo-se esse direito do indivíduo de forma expressa em nosso ordenamento.

Enquanto não houver, porém, reconhecimento do direito ao esquecimento, resta enfraquecido o indivíduo, pois o Estado não tem dever de proteger direito que não é reconhecido como tal e tampouco pode o ofendido invocar esse suposto direito em face de particular. É claro que se pode decidir casos concretos a partir da inviolabilidade da vida privada, por exemplo, como vinha ocorrendo até o julgamento do precedente do STF sobre o tema. Essa opção, porém, além de exigir a cada nova violação enorme esforço interpretativo do jurista que opera no caso, perpetua a falta de clareza e de rigor científico do sistema.

Por fim, refletindo sobre as variáveis que afetam o direito ao esquecimento, pode-se esboçar critérios para a acolhida ou rejeição da tese em caso concreto, examinando-se: (i) a licitude da origem da informação e quem as divulgou; (ii) a característica dessa informação – se precisa, adequada, relevante ou excessiva em relação a seus propósitos, se atualizada ou conservada por tempo superior ao necessário para seu fim, se conta com justificativa histórica, estatística ou científica; (iii) o grau de comprometimento/exposição do indivíduo, especialmente no caso da informação não ser atual e sua manutenção tornar inviável a potencial realização pessoal do indivíduo; e (iv) as circunstâncias das informações trazerem consequências adversas novas ou adicionais à situação de quem invoca direito a ser esquecido.

Considerações finais

A leitura do inteiro teor do RE 1.010.606/RJ proporciona muitas reflexões críticas. Em relação à tese de repercussão geral da compatibilidade do direito ao esquecimento, o trabalho demonstrou que o tema passou em grande parte alheio às considerações do relator, que não identificou de maneira adequada suas características essenciais, materializadas a partir da experiência europeia, causando certa confusão com outros direitos análogos, como o

[84] Essa é questão que sistematicamente prejudica a uniformização de jurisprudência em nosso país. Tribunais superiores, em especial o STF, deveriam prolatar decisões *per curiam*, e não votos individuais, como é a *Supreme Court of the United States*.

direito à reabilitação ou ressocialização, o direito ao próprio nome e imagem e à privacidade.

A simples referência ao termo *droit d'oubli* há mais de 50 anos na doutrina e jurisprudência francesas não significa o mesmo que hoje se designa sob essa denominação. As palavras, como se sabe, têm significado mundano, mas também técnico-jurídico. Os contornos do direito ao esquecimento em sentido técnico são indissociados do meio digital, que potencializa exponencialmente os danos a direitos de personalidade.

O STF já havia perdido anteriormente a oportunidade de enfrentar o impacto da tecnologia nos direitos do indivíduo ao julgar o tema da proteção de dados e da autodeterminação informativa. Do mesmo modo, perdeu oportunidade de se aproximar da experiência jurídica internacional no tema do direito ao esquecimento, deixando de lado até mesmo as normas vigentes na LGPD (imagem e semelhança do GDPR), em que se trata do direito análogo, porém mais restrito, de apagar dados (excluir ou eliminar na redação do legislador brasileiro). Alguns conceitos acabaram sendo confundidos, ao serem equiparadas a liberdade artística, de misturar fatos e ficção, com a de imprensa e jornalismo. Confundiu censura, com prudência em face de outros direitos fundamentais, pois é certo que a liberdade de publicar não é o único direito constitucional - sendo oportuno lembrar que, recentemente, nas eleições para a presidência do país, viu-se esse mesmo tribunal legitimar atos de controle de conteúdo, determinando sumariamente a remoção de materiais *on line* ou mesmo de programas e canais, sem considerar essa circunstância censura[85].

No caso específico da ação da família Curi, evidencia-se impropriedade e, mais ainda, pouca sensibilidade. Impropriedade do TJRJ afirmar que haveria obrigação de indenizar apenas em situações de uso comercial ou "denegrição"[86] da honra, quando a Constituição não condiciona direitos de personalidade. E pouca sensibilidade ao consignar que a família deve lembrar, ao dizer que "o esquecimento não é o caminho salvador para tudo", sendo "muitas vezes [é] necessário reviver o passado". Não cabe ao tribunal lançar considerações psicológicas. Impropriedade também do STJ, que não apenas confundiu direito à reabilitação com direito ao esquecimento, mas também incluiu o tema do domínio público, que é conceito de direito autoral na discussão e, portanto, alheio ao caso, lançando a derradeira pá de cal ao afirmar simplesmente que sem ilicitude não haveria dever de indenizar, afirmação que, fora do contexto – como ocorre na simples transcrição de ementa -, não corresponde à verdade. No STF, o ministro Nunes Marques sintetizou bem a questão: cabe indenização pelo desprezo da memória da vítima do crime em programa de entretenimento, que renovou o sofrimento da família e violou sua privacidade.

---

85 Trata-se de resolução 23.714, aprovada em 20.10.2022: https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/arquivos/resolucao-desinformacao/@@download/file/TSE%20-%20Resoluc%CC%A7a%CC%83o%20-%20Desinformac%CC%A7a%CC%83o%20-%20aprovada.pdf

Sobre a atuação do STF, validando-a: https://www.conjur.com.br/2022-out-25/stf-maioria-manter-resolucao-tse-fake-news; https://www.cnnbrasil.com.br/politica/stf-tem-placar-a-favor-de-manter-resolucao-do-tse-contra-fake-news/

86 Outra má escolha de palavras, desta feita pelo TJRJ, em tempos em que se discute a possibilidade de um idioma ser mais preconceituoso que o povo que o usa.

Referências bibliográficas

BENNETT, Steven C. The "Right to Be Forgotten": Reconciling EU and US Perspectives, 30 *Berkeley J. Int'l Law*. 161, 2012, p. 161-168.

CACHAPUZ, Maria Claudia. *Intimidade e vida privada no novo Código Civil brasileiro:* uma leitura orientada no Discurso Jurídico. Porto Alegre: Sérgio Antônio Fabris Editor, 2006.

CROCKETT, May. The Internet (Never) Forgets, 19 *SMU Sci. & Tech. L. Rev*. 151 (2016). Disponível em: https://scholar.smu.edu/scitech/vol19/iss2/4

FEITEN WINGERT ODY, Lisiane. *Direito e Arte:* o direito da arte brasileiro sistematizado a partir do paradigma alemão. Madri, Barcelona, B.Aires. SP: Marcial Pons, 2018, v.1.

FEITEN WINGERT ODY, Lisiane. Direito e Linguagem: Direito comparado e línguas estrangeiras – o papel da tradução. *Direito comparado Alemanha-Brasil* vol. II: Temas de Direito privado em estudos originais e traduzidos. Porto Alegre: Faculdade de Direito da UFRGS, 2022.

FEITEN WINGERT ODY, Lisiane. *Direitos autorais e sociedade de informação e conhecimento*: por um direito de uso adaptado à era digital. In: Propriedade Intelectual – Sociedade de Informação – Inteligência Artificial (FERNANDES, Marcia; CALDEIRA, Cristina (org). No prelo.

MURRAY, Andrew. *Information, Technology Law*: the Law & Society. Oxford: OUP, 2019.

Relatório Mundial da UNESCO - Organização das Nações Unidas para a Educação, a Ciência e a Cultura apresenta definição, conteúdo e prognóstico para o futuro das sociedades de conhecimento. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000232575

U.S. Federal Trade Commission Staff. Comments On The European Commission's November 2010 Communication On Personal Data Protection in The European Union 1-2, Jan. 13, 2011 In: http://www.ftc.gov/os/2011/01/111301dataprotectframework.pdf.

VON DIX, Alexander; FRANSSEN, Gregor; KLOEPFER, Michael; SCHAAR, Peter; SCHOCH, Friedrich; VOSSHOFF, Andrea (org.). *Informationsfreiheit und Informationsrecht*. Berlin: Lexxion Verlagsgesellschaft, 2015.

Viés Algorítmico e Discriminação: O Ambiente Regulatório Brasileiro

Allan Carvalho[87]

RESUMO

Com a disseminação de ferramentas de inteligência artificial (IA) cada vez mais sofisticadas e considerando que o Brasil não dispõe de uma política pública especificamente voltada para o fenômeno da discriminação algorítmica, este artigo busca compreender como o direito brasileiro lida com os casos de discriminação causados pelo uso de algoritmos enviesados. O texto inclui uma breve análise do sistema regulatório vigente para identificar eventuais insuficiências normativas, por meio de uma metodologia de caráter exploratório-dedutivo, que inclui a revisão da literatura científica e dos dispositivos institucionais aplicáveis (principalmente a legislação). Por fim, a conclusão indica que a revisão humana de decisões automatizadas é talvez a melhor ferramenta disponível neste momento para prevenir a discriminação algorítmica.

PALAVRAS-CHAVE

LGPD. Aprendizado de máquina, Direito da tecnologia, Direito regulatório, Preconceito.

[87] Allan Carvalho é graduado em Direito pela Universidade Federal do Rio Grande do Sul e em Ciências Sociais pela Universidade Federal do Rio de Janeiro. Seu email de contato é carvalho.apd@gmail.com.

Kelly Lissandra Bruch, é doutora em Direito pela Universidade Federal do Rio Grande do Sul, Professora Adjunta da Universidade Federal do Rio Grande do Sul. Seu e-mail de contato é kelly.bruch@ufrgs.br.

Algorithmic Bias and Discrimination: The Brazilian Regulatory Environment

Allan Carvalho

ABSTRACT

With the propagation of increasingly sophisticated artificial intelligence (AI) tools and considering that Brazil does not have a public policy specifically focused on the phenomenon of algorithmic discrimination, this article aims to understand how Brazilian law deals with cases of discrimination caused by the adoption of biased algorithms. The text includes a brief analysis of the current regulatory landscape to identify possible regulatory shortcomings, through an exploratory-deductive methodology that includes a review of the scientific literature and applicable institutional provisions (legislative, mainly). Finally, the conclusion implies that a human review of automated decisions is perhaps the best tool available at this time to prevent algorithmic discrimination.

KEYWORDS

LGPD, Machine learning, Technology law, Regulatory law, Prejudice.

Introdução

As inovações tecnológicas aceleram a difusão de novas ferramentas que podem apresentar grande utilidade para as pessoas, mas que eventualmente trazem consigo efeitos inesperados e indesejados. O estágio de desenvolvimento tecnológico atual estabelece condições para mudanças sociais profundas, ao oferecer novas formas de interações interpessoais, novos tipos de mobilidade e transporte, ou novas formas de geração de energia, por exemplo. Ainda, pela primeira vez na história a sociedade vem se familiarizando ao convívio com dispositivos (como robôs de limpeza e de atendimento virtual por texto e voz, drones e outras formas de inteligência artificial) que não possuem vida, mas se apresentam cada vez mais autônomos, inteligentes e capazes de aprender por si mesmos.

Entretanto, essas novas aplicações da tecnologia moderna em geral vêm acompanhadas de incertezas no que diz respeito aos seus efeitos de longo prazo. Na medida em que ocorre o desenvolvimento de novas aplicações tecnológicas, também se verificam mudanças na percepção da sociedade a respeito do seu uso e da correspondente resposta regulatória que lhe seria adequada. Diferentes sociedades e seus respectivos cidadãos possuem diversas preferências coletivas e/ou individuais a respeito do grau de incerteza e do tipo de risco que são considerados aceitáveis. Neste contexto, o avanço tecnológico oferece a oportunidade de realizar algumas reflexões relevantes, como, por exemplo, a que diz respeito ao melhor alinhamento possível entre a tecnologia e os valores sociais e humanos considerados universais. Também se pode questionar se neste momento a humanidade realmente tem consciência acerca dos valores mais relevantes que devem ser promovidos (e se há consenso a respeito desses valores), ou ainda como garantir que o mundo digital se torne melhor do que o mundo analógico em relação aos indivíduos, à sociedade e ao planeta. A maneira pela qual a regulação normativa promovida pelo Estado pode atender a esses objetivos sociais diversos e por vezes conflitantes permanece uma questão fundamental da ciência jurídica. Novas tecnologias também levantam questionamentos a respeito dos limites do Direito na medida em que se torna difícil identificar e separar o que é prejudicial do que é benéfico. Também é preciso considerar que a aceitação social das novas tecnologias é essencial para que elas sejam bem-sucedidas.

Como o título sugere, este trabalho trata das respostas regulatórias brasileiras para a questão da discriminação algorítmica. Neste sentido, o problema desta pesquisa aqui é: a ausência de revisão humana das operações automatizadas é prejudicial para se mitigar a discriminação algorítmica? Ou seja, diante da conjuntura apresentada nos parágrafos anteriores, é preciso analisar a capacidade de a discriminação algorítmica no Brasil ser corrigida sem que exista obrigatoriedade de intervenção humana nas decisões automatizadas. Por conseguinte, o objetivo geral desta pesquisa consiste em identificar maneiras de conferir maior eficácia ao texto constitucional brasileiro e garantir a não-discriminação no uso da inteligência artificial. Isto é, este artigo busca estudar se a atual desobrigação legal de revisão humana sobre as decisões automatizadas compromete a eficácia das disposições constitucionais e a proteção aos direitos humanos no Brasil nos casos que envolvem especialmente a discriminação algorítmica em âmbito nacional. Conforme indicado no terceiro capítulo deste

trabalho, no caso da União Europeia (modelo de inspiração para o Brasil nesta área) foi expressamente estabelecida a possibilidade de revisão, por operadores humanos, de decisões automatizadas efetuadas por algoritmos. Uma análise mais profunda poderia avaliar mesmo a capacidade de toda a legislação aplicável ao tema para coibir violações de direitos, em especial direitos fundamentais, causadas por operações automatizadas realizadas por algoritmos enviesados.

A justificativa para esta pesquisa está no fato de que o uso da ciência de dados já atinge patamares que seriam considerados como literatura de ficção há alguns anos.[88] Neste cenário, é imprescindível realizar uma reflexão sobre o uso dos dados que alimentam os algoritmos de inteligência artificial, sobretudo diante de uma crença relativamente comum na suposta infalibilidade da tecnologia. Esse assunto se coloca como um tema de estudos tanto interessante quanto desafiador dentro do Direito, pela dificuldade e atualidade do tema. Por fim, este trabalho tem a intenção de ir além de uma simples reflexão abstrata, procurando analisar fenômenos concretos e contribuir para o desenho de soluções eficazes, em especial considerando a atuação do poder público. Por se tratar de um tema novo para a academia brasileira, não se espera identificar vasta bibliografia específica sobre o objeto desta pesquisa em língua portuguesa, de modo que as fontes consultadas serão em grande medida artigos acadêmicos estrangeiros (de diversas áreas do conhecimento), além da doutrina jurídica brasileira. Assim, é adotado o método dedutivo, com caráter descritivo-exploratório, mediante análise da bibliografia científica publicada sobre o tema para identificar a interseção entre os artigos acadêmicos das áreas de direito e ciência da computação, sobretudo.

Deste modo, ao longo deste artigo, a redação assumirá perspectiva cada vez mais exploratória, na medida em que se busca compreender o fenômeno da discriminação algorítmica e seu tratamento jurídico atual. Isso se deve em grande parte ao fato de que o objeto dessa pesquisa corresponde a uma situação relativamente recente, que há pouco tempo vem recebendo atenção significativa por parte da comunidade acadêmica. Ainda, dada a atualidade deste assunto, também serão analisadas notícias e eventuais discussões legislativas que abordem este tópico.

Este artigo foi organizado em pequenos capítulos que tratam dos objetivos específicos da pesquisa: (1) esta breve introdução, que inclui a apresentação do problema a ser enfrentado, os objetivos gerais e específicos, além da metodologia adotada; (2) a contextualização da pesquisa; (3) a análise dos principais tipos de vieses que originam situações discriminatórias em mecanismos de inteligência artificial, além de tratar do próprio conceito de discriminação; em seguida, há (4) uma avaliação a respeito da aptidão dos mecanismos jurídicos disponíveis no Brasil para lidar com os problemas associados ao viés algorítmico; e finalmente (5) a conclusão, que traz o argumento principal de que a revisão humana de decisões automatizadas talvez seja melhor ferramenta disponível neste momento para combater a discriminação algorítmica.

[88] Como por exemplo, o uso de aplicativos em países como China e Coreia do Sul que monitoram os cidadãos e informam a necessidade de quarentena ou a autorização para circular pela cidade durante o surto de COVID-19 nos primeiros meses de 2020, conforme demonstram os links a seguir: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html; https://coronamap.site/. Acesso em 09 de novembro de 2022.

1. Contexto da pesquisa

Este capítulo tem por objetivo específico realizar breve contextualização a respeito do tema desta pesquisa, com foco nas normas aplicáveis. Em relação ao ordenamento jurídico brasileiro, a Constituição de 1988 resguarda uma série de garantias para que os indivíduos exerçam seus direitos e deveres de modo seguro e previsível, embora seja fundamental que quase sempre a legislação infraconstitucional necessite intervir para detalhar os mandamentos constitucionais e regular, na prática, as disposições da Lei Maior. É por essa via que as diversas instituições estatais podem implementar as políticas públicas previstas em lei para concretizar as metas estabelecidas pelo texto constitucional.

De início, o Marco Civil da Internet (Lei Nº 12.965, de 23 de abril de 2014)[89] representou a mais importante norma voltada especificamente para a regulação da Internet no Brasil, capaz de servir de orientação para futuras políticas públicas a respeito deste tema. Com sua redação de forte caráter principiológico (como a neutralidade da rede, a liberdade de expressão e privacidade dos usuários), o Marco Civil se tornou referência mundial para a regulação da Internet, uma área que permanece em constante transformação. Em seu texto se destacam as disposições que tratam da responsabilidade civil de provedores em relação ao conteúdo criado e/ou publicado por terceiros (incluindo também dispositivos que apresentam relevância para a esfera penal, relacionados a investigações de crimes cibernéticos), além de estimular debates sobre o direito ao esquecimento dentro do ordenamento jurídico brasileiro. O Marco Civil da Internet também serviu inicialmente como um mecanismo geral para a regulação dos dados pessoais, uma vez que até 2018 o Brasil não dispunha de lei especial sobre o assunto. Deste modo, as disposições normativas instituídas pelo Marco Civil "inauguravam o tratamento da tutela de dados no que diz respeito à rede no País", pois "até então se contava apenas com dispositivos ora muito genéricos, como o constante do artigo 21 do Código Civil[90], ora muito setoriais, como o artigo 43 do Código

[89] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 10 de novembro de 2022.

[90] Código Civil, Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

de Defesa do Consumidor[91]", como afirmam os professores Carlos Affonso Souza e Ronaldo Lemos.[92]

É exatamente neste ponto que a entrada em vigor da Lei Geral de Proteção de Dados[93], comumente chamada de "LGPD", representou a mais importante iniciativa brasileira de regulamentação do uso de dados pessoais que consiste na "matéria-prima" fundamental do chamado *big data*, a nova ciência dos dados em massa que possibilita o desenvolvimento de mecanismos cada vez mais complexos de inteligência artificial, como os abordados no capítulo anterior. Aqui o legislador brasileiro em princípio buscou como referência principal o Regulamento Geral Europeu sobre a Proteção de Dados[94] (RGPD), promulgado pelo Parlamento da União Europeia em 2016.

O cenário tecnológico atual aponta para o aumento progressivo no imenso volume de dados que é produzido a partir dos diversos aparelhos eletrônicos interconectados que se tornaram parte da vida cotidiana em quase todos os países nas últimas décadas.[95] Nestas condições, a LGPD terá impacto no cotidiano dos cidadãos brasileiros em inúmeras situações[96], como por exemplo solicitações de crédito junto a

---

[91] Código de Defesa do Consumidor, Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6° Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

[92] SOUZA, Carlos Affonso Pereira de; SILVA JUNIOR, Ronaldo Lemos da. *Marco Civil da Internet:* construção e aplicação. 1. ed. Juiz de Fora: Editar, 2016. v. 1. p. 25. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em 10 de novembro de 2022.

[93] Lei n° 13.709, sancionada em 14 de agosto de 2018 pelo então presidente Michel Temer e vigente desde 18 de setembro de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (acesso em 10 de novembro de 2022).

[94] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e40-1-1. Acesso em 10 de novembro de 2022.

[95] Disponível em: http://www.ihu.unisinos.br/78-noticias/593456-o-big-data-apresenta-uma-multimetodologia- entrevista-com-walter-sosa-escudero. Acesso em 10 de novembro de 2022.

[96] O Direito brasileiro buscou se adequar a essa nova conjuntura social, com o objetivo de estabelecer regras mais específicas para a coleta, armazenamento e uso de informações pessoais por instituições públicas e privadas. Por exemplo, existe a prática comum de solicitar do número do CPF do consumidor na aquisição de produtos e

instituições financeiras ou simples pedidos de refeições, por exemplo, na medida em que se consolida o papel do *big data* na intermediação de praticamente todos os aspectos da vida social contemporânea.

Entretanto, diferentemente da norma europeia, a lei brasileira[97] deixou de prever expressamente a obrigatoriedade de revisão humana sobre uma operação algorítmica. Ou seja, não há obrigação de que o resultado do tratamento automatizado de dados seja analisado por um operador humano, mesmo quando o usuário do serviço se sinta prejudicado. Embora seja bastante improvável que os computadores excedam e mesmo substituam por completo a força de trabalho humana nas próximas décadas, parece inevitável a tendência de que as máquinas continuem ganhando relevância em um número cada vez maior de atividades.

Deste modo, a discussão acadêmica e política em âmbito internacional há alguns anos vem alertando a sociedade para os possíveis efeitos negativos da atividade algorítmica sobre a esfera individual de interesses jurídicos. Neste sentido, este trabalho pretende analisar se a sociedade brasileira dispõe de meios jurídicos suficientes que ofereçam uma resposta institucional à altura dos desafios desta nova realidade, na qual o avanço da ciência de dados representa, simultaneamente, possibilidade de melhorias e fonte de problemas aos usuários.[98]

Conforme mencionado anteriormente, o foco deste artigo está no chamado "viés algorítmico", que trata das decisões tomadas por sistemas de algoritmos que podem estar comprometidas por diversos tipos de vieses, acarretando prejuízos aos indivíduos que se encontram sujeitos aos resultados dessas operações eletrônicas automatizadas. Esse tema se insere em uma conjuntura mais ampla, que trata dos impactos legais causados pelas aplicações da ciência de dados em massa, sobretudo no que diz respeito aos "direitos democráticos e a privacidade".[99]

Este cenário envolve não apenas a relação entre a LGPD (ou outra lei específica) e a discriminação algorítmica[100], mas, considerando seus efeitos na

---

serviços. Para mais detalhes, consultar: https://www.nexojornal.com.br/expresso/2020/02/15/O-que-est%C3%A1-em-jogo-quando-voc%C3%AA-d%C3%A1-seu-CPF-na-hora-da-compra?utm_medium=Social&utm_campaign=Echobox&utm_source=Twitter#Echobox=1582314608. Acesso em 10 de novembro de 2022.

[97] Como é possível constatar a partir da leitura dos artigos 20 e 22 das leis brasileira e europeia, respectivamente.

[98] Disponível em: https://www.conjur.com.br/2019-jul-24/renan-lopergolo-lacunas-lgpd-casos-faceapp. Acesso em 10 de novembro de 2022.

[99] MOLNAR, Adam. *Technology, law, and the formation of (il)liberal democracy?*, Surveillance and society, vol. 15, no. 3/4, 2017, pp. 318-388. Disponível em https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6645. Acesso em 3 de junho de 2020. Aqui o autor chama a atenção para o papel relevante exercido pelos direitos fundamentais elencados na constituição de cada Estado no sentido de resguardar os indivíduos de investidas autoritárias por parte das autoridades públicas devido ao mau uso do *big data*, o que também indica a responsabilidade de juízes e legisladores no sentido de efetivar tais garantias na prática.

[100] O termo "discriminação" aqui é utilizado em um sentido amplo para se referir a impactos prejudiciais descomunais - intencionais ou não – em que o desenho, a implementação e a utilização de sistemas algorítmicos podem causar em determinados grupos sociais ou indivíduos que compartilham certas características. Esta pesquisa não tem por objetivo propor uma conclusão legal sobre a discriminação a partir da

sociedade como um todo, é preciso analisar a capacidade do ordenamento jurídico brasileiro em solucionar os desafios que já estão sendo propostos por essa nova condição. Este caso pode até mesmo gerar um debate envolvendo confitos de direitos fundamentais. Por exemplo, a liberdade econômica (das empresas em geral, especialmente as de tecnologia) versus a não-discriminação (igualdade), como alguns dos recentes argumentos utilizados nas discussões legislativas permitem concluir, conforme se demonstra adiante.

Neste sentido, cabe avaliar se os dispositivos existentes na legislação (como exemplifica o Artigo 20[101] da LGPD), são suficientes para oferecer uma solução satisfatória ao problema da discriminação algorítmica[102] e garantir o cumprimento das normas constitucionais que protegem os direitos fundamentais dos cidadãos, o que deve se tornar um desafio ainda mais presente na medida em que se intensifica a mudança de paradigma tecnológico atualmente em curso. Conforme indicado anteriormente, este assunto vem recebendo cada vez mais atenção nas pesquisas acadêmicas feitas na área jurídica em âmbito internacional, e se coloca como um grande debate que precisa ser realizado pela sociedade brasileira nos próximos anos, de modo a evitar eventuais prejuízos à garantia dos direitos humanos de nossa população.

Como se demonstra adiante, este tema é tão complexo quanto urgente para o Direito, pois a geração massiva de dados torna impossível seu manejo sem a utilização das próprias ferramentas proporcionadas pelo *big data*. Este assunto merece ainda mais atenção por parte de todos os agentes sociais na medida em que tecnologias nascentes (como a conexão de alta velocidade 5G e a chamada Internet das

---

legislação penal ou de qualquer outra. Alguns casos de discriminação podem ser não intencionais e até imprevistos, outros podem ser o resultado de uma decisão política deliberada de concentrar serviços ou assistência naqueles que mais necessitam, como no caso das ações afirmativas. Outros ainda podem criar consequências adversas para populações específicas que criam ou exacerbam a desigualdade de oportunidades para segmentos sociais ou cidadãos que já estão em desvantagem. É neste último caso que o trabalho se concentra, especificamente.

[101] Lei nº 13.709/2018, Art. 20: O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

[102] Especificamente sobre a LGPD, existem diversas questões que mereceriam uma investigação própria, como os efeitos do Art. 20 da LGPD no tratamento automatizado de dados pessoais ou ainda se seria possível que falta de revisão humana por si já representasse um prejuízo em potencial para os usuários.

Coisas[103]) se tornarem a nova realidade mundial nos próximos anos[104], trazendo consigo outras mudanças significativas para nosso modo de vida atual, e com isso diversas questões para quais a sociedade certamente esperará respostas do direito.

Considerando o caso brasileiro, o texto constitucional promulgado em 1988 dispôs em seu artigo 3[105] que um dos objetivos fundamentais da República é combater a discriminação em suas diversas formas. Trata-se de uma meta com força vinculante que deve ser aplicada em todas as decisões e atividades desenvolvidas por cada integrante do Estado brasileiro, inclusive durante o exercício de fiscalização da sociedade civil. Entretanto, assim como ocorre com as demais metas constitucionais, é quase sempre necessário que uma política pública específica seja formulada pelo legislador infraconstitucional e executada pelo poder executivo para que as previsões da Constituição sejam efetivadas na prática.

Neste sentido, a atuação positiva do poder público para combater a discriminação é imprescindível, de acordo com Philip Gil França, "ao desenvolvimento intersubjetivo dos partícipes do sistema constitucional", isto é, "quando o mínimo possível de viabilidade deste desiderato é sentido na vida daqueles que estão sob a égide de sua regulação".[106] Na visão do professor, a política pública pode ser definida como "a organização de esforços estatais para alcançar um claro objetivo predeterminado, mediante um planejado caminho, a partir da demonstração objetiva de realização de um interesse público constitucionalmente previsto".[107]

Deste modo, conforme mencionado acima, o Marco Civil da Internet constituiu a primeira tentativa do legislador de balizar as futuras políticas públicas para regular o mundo digital. Embora não trate apenas do uso de dados pessoais nem estabeleça regras específicas de funcionamento para algoritmos e sistemas de informação, sua redação teve o mérito especial de aproximar a sociedade das discussões sobre a regulação da Internet, além de sedimentar o alcance da responsabilidade civil para os provedores de Internet (positivando o entendimento jurisprudencial de tribunais nacionais e estrangeiros no sentido de não responsabilizar o provedor da conexão pelas

---

[103] Mais detalhes sobre a tecnologia 5G e a Internet das Coisas disponíveis em https://agenciabrasil.ebc.com.br/geral/noticia/2020-03/agencia-brasil-explica-o-que-e-tecnologia-5g. Acesso em 10 de novembro de 2022.

[104] A implementação da tecnologia 5G ao redor do mundo já tem contribuído para acirrar a disputa geopolítica entre Estados Unidos e China. Washington vem seguidamente acusando o país asiático de obter vantagens indevidas incluindo a possibilidade de controle sobre a comunicação internacional caso a infraestrutura implantada seja desenvolvida pela empresa chinesa Huawei, o que é negado por Pequim. A notícia a seguir (em inglês) exemplifica a proporção que esta controvérsia pode tomar: https://www.theguardian.com/technology/2020/jun/02/us-senator-huawei-5g-is-like-soviets-building-wests-submarines. Acesso em 10 de novembro de 2022.

[105] CRFB/88, Art. 3º: Constituem objetivos fundamentais da República Federativa do Brasil: (...) IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

[106] FRANÇA, Phillip Gil. *Objetivos Fundamentais da República, Escolhas Públicas e Políticas Públicas*: Caminhos de Concretização dos Benefícios Sociais Constitucionais. Direitos sociais e políticas públicas I. 1ed. Curitiba: Clássica Editora, 2014, v. 25, p. 230-244.

[107] FRANÇA, Phillip Gil. Idem, ibidem. p. 236.

condutas de seus usuários).[108] Por outro lado, como não poderia deixar de ser em uma democracia, existem críticas[109] ao fato desta lei privilegiar fortemente a liberdade de expressão a ponto de ser preciso recorrer ao Judiciário para retirar de circulação eventual conteúdo que viole por exemplo a intimidade, privacidade ou a proteção ao consumidor. De todo modo, o Marco Civil não será analisado nesta pesquisa por não reger especificamente os casos envolvendo violações de direitos causados por vieses algorítmicos, ainda que seja válida a discussão sobre o papel que o Marco Civil possa desempenhar enquanto marco regulatório geral para o funcionamento da Internet brasileira, o que pode ser um tema de investigação interessante em pesquisas futuras.

Já o Art. 20 da LGPD possibilita ao interessado solicitar a revisão de decisões tomadas exclusivamente por algoritmos (sem intervenção humana). Sobre este ponto houve uma iniciativa política do senador Styvenson Valentim (vinculado ao partido político Podemos, do Rio Grande do Norte), que apresentou o Projeto de Lei 4.496/2019 com o objetivo de alterar a LGPD no que diz respeito à definição da expressão "decisão automatizada". Segundo o autor, este projeto partiu da perspectiva de existirem diversas maneiras de realizar as "decisões automatizadas" previstas na LGPD, sendo necessário indicar expressamente os mecanismos de aprendizado de máquina e inteligência artificial no texto da lei. Essa ação serviria para garantir transparência aos cidadãos, na medida em que facilitaria o acesso a "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada", conforme previsão do §1° do Art. 20 da LGPD. Segundo o senador, "os responsáveis pelo tratamento de dados não fornecem esclarecimentos apropriados para decisões baseadas em técnicas de inteligência artificial ou de outras igualmente complexas".[110]

Como indicado anteriormente, a lei brasileira se inspirou no modelo adotado pela União Europeia para regular este tema. Entretanto, o texto da norma editada pelo parlamento europeu contém explicitamente a possibilidade de revisão humana como uma alternativa aos interessados na reavaliação das referidas decisões[111], o que foi

---

[108] SOUZA, Carlos Affonso Pereira de; SILVA JUNIOR, Ronaldo Lemos da. Idem, ibidem. p. 98.

[109] CARVALHO, P. H.. *O Marco Civil da Internet: Uma análise sobre a constitucionalidade do artigo 19*. Revista da Faculdade de Direito do Sul de Minas. Pouso Alegre, 2017, v. 33, p. 228-244. Disponível em: https://www.fdsm.edu.br/adm/artigos/6917c36392274c9b6393c7f7a7bddbd1.pdf. Acesso em 10 de novembro de 2022.

[110] Maiores detalhes disponíveis em: https://www25.senado.leg.br/web/atividade/materias/-/materia/138136 Acesso em 10 de novembro de 2022.

[111] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Artigo 22: Decisões individuais automatizadas, incluindo definição de perfis 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2. O nº 1 não se aplica se a decisão: a) for necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) for autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. 3. Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos

vetado pela Presidência da República na versão brasileira. Essa possibilidade foi inicialmente adotada pelo legislador brasileiro, contudo após o veto presidencial referente ao parágrafo terceiro do diploma legal, a eventual nova análise que seja solicitada pelo interessado não será obrigatoriamente realizada por um ser humano.

As razões do veto presidencial alegaram a inviabilização dos modelos de negócios de empresas privadas, o que pode parecer algo questionável quando se observa que a economia europeia é bastante dependente do setor de serviços (característica que compartilha com a economia brasileira) e ainda assim determinou a intervenção humana neste cenário. Em especial, a norma brasileira pode se tornar problemática sobretudo por condicionar a preservação de direitos fundamentais[112] a interesses econômicos privados. Entretanto, até o momento não há evidências de que a regulação europeia tenha resultado na inviabilização de negócios ou prejuízos econômicos para as empresas que atuam nos países que integram a União Europeia. A mensagem da Presidência da República nº 288/2019, dirigida à Presidência do Senado Federal, afirma que

> a propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das *startups*, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária.

Assim, a redação final da lei dificultou que decisões automatizadas (isto é, tomadas por algoritmos) sejam corrigidas por meio da intervenção humana e deixou de ser ferramenta valiosa no combate a práticas discriminatórias (que são abordadas adiante), como, por exemplo, eventual decisão que recuse a oferta de crédito a cliente de instituição financeira (ou que considere que o risco do mútuo seja elevado tornando a taxa de juros mais onerosa, consequentemente) em decorrência de características raciais e/ou étnicas do solicitante ou de seu endereço residencial, mesmo sob prova documental que comprove aptidão financeira. Neste caso, não se discute que a

---

interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. 4. As decisões a que se refere o nº 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, nº 1, a não ser que o nº 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

112 A liberdade empresarial é um direito fundamental (resguardado no inciso IV do Art. 1º da Constituição de 1988), de modo que o veto presidencial à obrigatoriedade de revisão humana em decisões automatizadas poderia talvez ser compreendido como um exemplo que enseja uma colisão entre direitos fundamentais. Esta colisão "deve ser enfrentada somente no momento da possível justificação de uma intervenção estatal(...) porque um direito fundamental de outro titular de direito pode estar limitando o exercício do direito fundamental atingido pela medida ou omissão estatal." DIMOULIS, Dimitri.; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 169.

concessão de crédito é inerente à liberdade negocial das instituições financeiras, entretanto a falta de transparência no tratamento automatizado dos dados impede a verificação de possíveis critérios discriminatórios na operação do algoritmo. Novamente, o legislador não inseriu padrões no texto da LGPD para balizar objetivamente o tratamento de dados e garantir segurança jurídica a todas as partes. Entretanto, no âmbito judicial o artigo 7º da Resolução 332/2020 do Conselho Nacional de Justiça tomou por base a LGPD para estabelecer medidas de combate à discriminação no uso de ferramentas de inteligência artificial pelo Poder Judiciário.[113] Membros da academia[114] também tem defendido que a proteção aos direitos individuais consagrados pela LGPD não representa óbice à livre iniciativa empresarial; pelo contrário, possibilitaria maior segurança jurídica e engajamento social capaz de fomentar o ambiente econômico.

Diante deste cenário em que se identificam inúmeros desafios representados pelo avanço na utilização de sistemas de inteligência artificial e suas consequências sociais e jurídicas, é possível levantar a hipótese de que a discriminação promovida por algoritmos não encontra resposta específica por parte da legislação brasileira, o que representa uma lacuna regulatória sobretudo em perspectiva do Art. 3º da Constituição brasileira.

No âmbito da LGPD, por exemplo, a redação atual poderá ser insuficiente para coibir práticas discriminatórias por não prever a obrigatoriedade de intervenção humana na revisão de decisões automatizadas. Também cabe refletir sobre as condições da Autoridade Nacional de Proteção de Dados quanto à resposta, de modo solitário, de todas as demandas em potencial envolvendo casos de discriminação algorítmica. Embora existam outros dispositivos legais (sem falar na própria aplicação direta das normas constitucionais[115]) que protejam os indivíduos de situações

---

113 Res. 332/2020 CNJ, 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. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3429. Acesso em 10 de novembro de 2022.

114 Autores como como Giovana Carlonni, vinculada ao Centre for Information Policy Leadership (CIPL), Carlos Affonso Souza, membro do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio) e Bruno Ricardo Bioni, integrante da organização *think tank* Data Privacy Brasil, que participaram de um debate virtual a respeito das implicações das medidas de combate à pandemia de Covid-19 em face da LGPD. A íntegra está disponível no seguinte endereço eletrônico: https://youtu.be/oBjQAfaf-xc. Acesso em 10 de novembro de 2022.

115 Seguindo a classificação tripartite proposta por José Afonso da Silva, as normas constitucionais de eficácia plena podem constituir a principal garantia nos casos envolvendo a discriminação algorítmica, como será abordado adiante. A doutrina inclui o Art. 3º, CRFB/88 entre as normas de eficácia limitada (de princípio programático), que tem por objetivo vincular a atuação do legislador quando da elaboração de uma

discriminatórias, a LGPD poderia representar a principal inciativa do poder público no que diz respeito à proteção dos direitos individuais e coletivos no cenário socioeconômico atual, onde as operações automatizadas efetuadas por algoritmos têm um impacto cada vez maior na esfera de interesses jurídicos dos cidadãos.

Assim, este capítulo teve por objetivo específico expor o contexto tecnológico e jurídico que abrange esta pesquisa, considerando as normas aplicáveis e o debate legislativo sobre o tema. No próximo capítulo, o foco consiste em apresentar e analisar alguns dos diversos tipos de vieses que podem ocorrer no funcionamento "normal" dos algoritmos, e que podem alimentar e ampliar diversas situações discriminatórias.

2. Viés algorítmico e discriminação

Conforme indicado anteriormente, toda inovação científica traz consigo o potencial de servir ao ser humano de modo a facilitar a execução de alguma tarefa ou resolver determinado problema. Novas ferramentas tecnológicas, neste sentido, podem trazer benefícios ou riscos para a sociedade, dependendo da forma como são utilizadas. Um exemplo clássico é a energia nuclear, que pode fornecer eletricidade de maneira menos nociva ao meio ambiente (sobretudo em comparação aos combustíveis fósseis), mas que também pode representar enorme potencial destrutivo quando utilizada para fins bélicos. Cabe à sociedade decidir o modo pelo qual a nova tecnologia será empregada.

Na medida em que as ferramentas de inteligência artificial são adotadas progressivamente pela sociedade, torna-se perceptível algumas consequências indesejadas. Sobretudo, a aplicação de sistemas de inteligência artificial para tomar decisões em substituição a agentes humanos e instituições leva a preocupações sobre como garantir justiça, imparcialidade e responsabilidade nos resultados dessas operações automatizadas. Concretamente, a inteligência artificial utilizada para controlar equipamentos do mundo real causa preocupações com a segurança, especialmente porque os sistemas estão expostos a toda a complexidade do ambiente humano.[116] Mitigar esses riscos requer o reconhecimento de que a solução deve incorporar os aspectos jurídicos e técnicos (da própria computação), considerando que justiça e segurança estão relacionadas. Como se demonstrará no próximo capítulo, a abordagem deve ser interdisciplinar, tanto por parte de empresas quanto do poder público, no esforço de evitar a discriminação algorítmica intencional, evitando resultados prejudiciais indesejados e gerando as evidências necessárias para dar às partes interessadas a confiança fundamentada de que as falhas não intencionais são

norma infraconstitucional. DUTRA, Luciano. *Direito Constitucional Essencial*. Rio de Janeiro: Forense. 2ªed. 2016. p.48.

[116] Um exemplo grave diz respeito aos carros autônomos que apresentam dificuldade de reconhecer as pessoas com tons de pele escuros como seres humanos, o que coloca esses indivíduos sob maior risco de acidentes. Embora carros autônomos sejam uma realidade ainda distante para a maioria das pessoas, essa falha poderia gerar acidentes graves nos casos dos mecanismos de freio emergencial que estão sendo adotados nos modelos mais recentes de automóveis. Para mais detalhes sobre viés racial em carros autônomos, consultar: WILSON, Benjamin; HOFFMAN, Judy; MORGENSTERN, Jamie. *Predictive Inequity in Object Detection*. arXiv preprint arXiv:1902.11097, 2019. Disponível em: https://arxiv.org/pdf/1902.11097.pdf. Acesso em 20 de novembro de 2022.

raras e improváveis, ou seja, de que o uso da ferramenta de inteligência artificial proposta é seguro.

Neste momento, entretanto, o objetivo específico desta seção é apresentar e analisar os principais tipos de vieses que originam situações discriminatórias em mecanismos de inteligência artificial, além de realizar breve exposição do próprio conceito jurídico de discriminação. Assim, este capítulo realiza uma exposição sobre o viés algorítmico e suas formas mais comuns. Em seguida, o texto trata da discriminação algorítmica propriamente dita.

2.1 Viés algorítmico

Nos últimos anos surgiram evidências de que, no caso dos algoritmos aplicados em sistemas de inteligência artificial, existe o risco (sobretudo não intencional) de ampliar condições discriminatórias[117] a partir do funcionamento "técnico" do algoritmo. O viés em algoritmos pode estar relacionado à sua autoria (a respeito do quão diversa é a equipe que elaborou o código de programação envolvido), pois a relativa homogeneidade de perfil socioeconômico entre os programadores tende a reverberar em seu trabalho, do qual se originam algoritmos menos aptos a lidar com a diversidade de pessoas e situações que existem na sociedade. Também é uma causa relevante a maneira pela qual o algoritmo foi programado, pois é preciso que se leve em consideração o teor de equidade que o trabalho deve preservar. O propósito por trás da criação do algoritmo é igualmente relevante, pois embora suas diversas aplicações possam render enormes resultados financeiros aos seus criadores, é preciso observar que a inovação científica deve se comprometer com impactos positivos na sociedade, sem ampliar condições antijurídicas nem fortalecer retrocessos sociais.[118]

Conforme mencionado anteriormente, a ciência de dados[119] é a principal forma de alimentação e desenvolvimento das ferramentas atuais de inteligência artificial. Logo, não é surpreendente que muitos tipos de vieses causadores da discriminação algorítmica envolvam de uma maneira ou de outra o uso dos dados pelo sistema. O governo federal dos Estados Unidos, que há alguns anos vem elaborando estudos científicos para subsidiar sua política nacional de inteligência artificial, optou por agrupar os diferentes tipos de vieses em duas categorias principais[120], que serão

---

117 Os exemplos mais comuns de viés que os algoritmos apresentam em geral se relacionam a questões étnicas e raciais, ou de gênero e orientação sexual, como se demonstrará adiante.

118 Essas são algumas das observações feitas por Joy Buolamwini, cientista da computação e pesquisadora vinculada ao Massachusetts Institute of Technology, nos Estados Unidos. Buolamwini fundou a Algorithmic Justice League, uma iniciativa para identificar e corrigir viés em algoritmos. Mais detalhes disponíveis em: https://www.ajlunited.org/ Acesso em 20 de novembro de 2022.

119 A ciência de dados, por exemplo, permite utilizar algoritmos de aprendizado de máquina para possibilitar aos humanos identificar e compreender padrões em um conjunto de dados não estruturados (como textos, vídeos e imagens) que não haviam sido descobertos ou mesmo imaginados pelos próprios cientistas. Esta é, na verdade, uma das formas mais comuns da chamada análise preditiva, que tem provocado muito dos avanços recentes na área da inteligência artificial.

120 THE WHITE HOUSE. *Big Data: A Report on Algorithmic Systems,. Opportunity, and Civil Rights*. Executive Office of the President, 2016. pp. 6 – 10. Disponível em:

abordadas a seguir: a primeira relacionada aos dados de entrada (*inputs*) em um algoritmo e a segunda abrangendo o funcionamento interno do algoritmo em si. É preciso observar, também, que existem diversas denominações para cada tipo de viés, mas como aparentemente (ainda) não há uniformidade ou padronização a respeito da sua nomenclatura, aqui será indicada somente sua conceituação, deixando de lado toda a diversidade de nomes que poderiam receber.

Em relação à primeira categoria, o viés se apresenta na medida em que o algoritmo precisa decidir quais dados serão utilizados pelo sistema, em detrimento de outros. Essa é uma ação corriqueira em todos os softwares que utilizam técnicas de inteligência artificial. Por exemplo, sua aplicação é comum em programas de navegação por satélite presentes em aparelhos (celulares) de telefonia móvel, nos quais os dados de velocidade de cada usuário permitem ao sistema conhecer a rota mais rápida para chegar ao destino escolhido. A situação descrita neste caso é benigna, mas sua análise permite compreender de modo simplificado as principais maneiras pelas quais o resultado da operação algorítmica pode resultar em práticas discriminatórias. Os vieses aqui podem ser causados por deficiências na inclusão e tratamento dos dados, isto é, quando algumas informações são consideradas como mais ou menos importantes para a decisão do algoritmo. No caso do exemplo apresentado, o sistema de navegação poderia não incluir a opção de realizar o trajeto por meio de bicicletas ou a pé, deixando em desvantagem as pessoas que não possuem carros.

Um outro tipo de viés muito frequente ocorre quando os dados apresentam algum erro ou estão desatualizados/incompletos. No caso do trajeto descrito, ainda que o sistema oferecesse a rota utilizando o transporte público, de nada adiantaria se as informações de horários não estivessem atualizadas, novamente prejudicando usuários que não utilizam carros.

Há ainda uma terceira categoria de viés algorítmico, relacionado aos dados de entrada, que compreende o viés de seleção (que talvez seja o mais frequente na prática), ocorrendo quando os dados inseridos no sistema não correspondem à realidade. No exemplo escolhido acima, se os dados forem majoritariamente obtidos a partir de telefones de última geração, é provável que a precisão do sistema seja prejudicada nas áreas mais pobres da região, que receberiam um serviço de menor qualidade, já que essa população de menor poder aquisitivo não participaria do serviço da mesma forma.

Por fim, um último tipo de viés que também é muito comum envolve a perpetuação de vieses históricos, por meio de *feedback loops*, isto é, nas situações em que um viés é replicado indefinidamente devido à capacidade da inteligência artificial de aprender com os padrões detectados. Se o modelo de aprendizado está enviesado, os resultados estarão igualmente enviesados, replicando o formato equivocado que foi aprendido. Um exemplo comum são algoritmos de seleção de trabalhadores, que podem desconsiderar um candidato apto à uma vaga de emprego apenas por diferir da faixa etária normalmente contratada pela empresa que publicou a vaga.

Esses tipos de vieses devem ser considerados no desenvolvimento e aplicação de sistemas de inteligência artificial envolvidos na prestação de serviços, para que

https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf. Acesso em 20 de novembro de 2022.

sejam preservados os critérios de eficiência, equidade e ética dispensados aos consumidores e/ou cidadãos em geral, em situações que envolvem tanto as instituições públicas quanto as privadas, como por exemplo concessão de crédito, licitações, alocação de recursos para programas de benefícios sociais e contratações de novos trabalhadores. Ainda não existem parâmetros oficiais nem consenso a respeito da melhor estratégia a ser adotada para mitigar os vieses em algoritmos. Contudo, medidas que promovam transparência e clareza de informação na escolha e tratamento dos dados são um ponto de partida importante para garantir que os dados inseridos em qualquer sistema algorítmico sejam precisos e adequados.

Prosseguindo a análise dos vieses algorítmicos em relação ao segundo ponto indicado anteriormente, que diz respeito ao funcionamento interno do algoritmo, é necessário lidar ainda com a dificuldade de que sua operação está distante da realidade de um usuário médio. Em regra, os códigos que compõem os sistemas algorítmicos são considerados confidenciais ou de propriedade das organizações que os desenvolveram e/ou naquelas onde são utilizados. Esta situação gera processos de tomada de decisão que apresentam diferentes graus de automação, mas que tem a característica comum de não apresentar transparência quanto à elaboração do resultado, o que deixa os usuários afetados com capacidade limitada para identificar os critérios pelos quais tais decisões foram tomadas. Logo, também se restringe suas opções de detectar e procurar corrigir quaisquer eventuais prejuízos ou erros gerados por algoritmos enviesados.

Esses vieses podem até mesmo significar que certos indivíduos serão excluídos inteiramente de determinadas oportunidades. Por exemplo, ao consultar páginas de busca na Internet essas pessoas podem (não) ter acesso a diferentes anúncios específicos de oportunidades profissionais, ou ofertas de mercadorias e serviços em geral, entretanto sem jamais suspeitar que essas oportunidades foram retiradas dos resultados de sua pesquisa a partir do funcionamento automático do algoritmo em uso pelo sistema de buscas. E se torna especialmente difícil para que os usuários tenham consciência do que está ocorrendo nesse tipo de situação, uma vez que se trata de um procedimento complexo, mas que pode se repetir frequentemente em outras interações dos usuários na rede. Novamente, os critérios de transparência e clareza na informação devem nortear a atuação dos mecanismos de inteligência artificial. Sem medidas nesse sentido, as falhas causadas pelo funcionamento interno inadequado de sistemas de algoritmos se tornam mais difíceis de detectar e com maior probabilidade de se intensificar.

Uma forma de viés interno que os algoritmos podem apresentar está justamente relacionado aos sistemas de correspondência (*matching systems*)[121] mal-empregados na busca de informações, recursos ou serviços na rede. Por exemplo, mecanismos de

[121] Existem diversos algoritmos diferentes que podem funcionar como um mecanismo de correspondência, dependendo do tipo de serviço prestado, como aplicativos de transportes ou de relacionamentos. Mas em geral esses sistemas realizam uma espécide de média ponderada que inclui enorme conjunto de dados diferentes, como histórico dos usuários, seu perfil de consumo, disponibilidade do prestador de serviço, etc. Por esta via o algoritmo consegue atingir a resposta que será recomendada a cada usuário de modo individual. Em regra, como acontece com todo sistema de *big data* e na estatística em geral, a precisão do resultado tende a aumentar junto com a quantidade e a qualidade dos dados ao qual se teve acesso. Mais detalhes disponíveis em: https://www.entrepreneur.com/article/338442. Acesso em 20 de novembro de 2022.

pesquisa, plataformas de redes sociais e aplicativos em geral dependem de sistemas de correspondência para determinar os resultados da pesquisa realizada pelos seus usuários, além de decidir quais anúncios exibir e quais empresas recomendar. Tais sistemas de correspondência podem resultar em resultados discriminatórios se a estrutura (*design*) do sistema não for atualizada periodicamente ou ignorar vieses históricos e imprecisões nos dados ou algoritmos usados. Um exemplo disso envolve uma usuária francesa de um aplicativo de relacionamentos, que solicitou seus dados pessoais à empresa responsável e pode constatar como sua rede de relacionamentos afetivos estava sob "curadoria" do algoritmo em questão, que poderia desnecessariamente restringir as suas interações na plataforma.[122]

Outra forma de viés interno envolve os serviços de personalização e recomendação adotados em aplicativos e sistemas de busca que restringem ao invés de alargar as opções do usuário. Aqui, informações detalhadas sobre cada usuário individual são coletadas e analisadas para inferir suas preferências, interesses e crenças. A partir da categorização do usuário em um perfil específico, serão indicadas oportunidades, como novas músicas para baixar, vídeos para assistir, descontos no preço ou produtos para comprar com base no que o sistema entende que está de acordo com a preferência deste perfil. Estudos acadêmicos[123] têm demonstrado que os algoritmos de recomendação deste conteúdo podem inadvertidamente restringir a disponibilidade de informações a determinados grupos sociais, deixando-os sem as mesmas oportunidades de acesso econômico e inclusão em comparação aos demais. Um exemplo é o acesso ao crédito, onde os consumidores que não possuem histórico de contratação de produtos financeiros considerados suficientes pelo algoritmo terão maior probabilidade de ter uma oferta recusada em virtude do seu padrão de consumo. Como se poderia imaginar, esse perfil de consumidor é composto principalmente pelo segmento da população menos privilegiado socioeconomicamente.[124]

A terceira categoria de viés interno abrange os mecanismos de tomada de decisão que pressupõem equivocadamente que a correlação estatística necessariamente implica causalidade[125]. Isto é, um programador (humano) ou o próprio

---

[122] A empresa alega que desde então alterou sua maneira de utilizar os dados pessoais de seus usuários, mas de forma geral se mantém no mercado esta lógica de funcionamento com base nos dados coletados a partir da atividade do usuário. Detalhes acerca do caso citado estão disponíveis no seguinte endereço eletrônico: https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold. Acesso em 20 de novembro de 2022.

[123] SWEENEY, L. *Discrimination in Online Ad Delivery*. Harvard University. January 28, 2013 http://ssrn.com/abstract=2208240; DATTA, A., TSCHANTZ, M. C., *Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination*. In Proceedings on Privacy Enhancing Technologies (PoPETs). 2015. https://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf Acesso em 20 de novembro de 2022.

[124] THE WHITE HOUSE. Idem, ibidem. p 11. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf Acesso em 20 de novembro de 2022.

[125] A estatística inferencial faz uso da análise descritiva dos dados de uma amostra para chegar a conclusões sobre um grupo maior, ao qual não se teve acesso. O objetivo é determinar a probabilidade com que o resultado da análise da amostra se aplica a toda a universalidade dos dados disponíveis. Isto é, criar um modelo que permite prever tendências e comportamentos dos dados que compõem aquele conjunto

sistema algorítmico pode analisar dois fatores que frequentemente ocorrem juntos (por exemplo, pertencer a determinado grupo étnico e ter um certo nível de renda), e presumir que há necessariamente algum nexo de causalidade entre os dois. Logo, criar uma relação causal quando há somente correlação entre os dados pode levar à discriminação de usuários específicos. Um exemplo ocorre em análises demográficas promovidas por seguros de saúde feita nos Estados Unidos: dentro de uma mesma classificação de risco de adoecer, pacientes negros já apresentavam condições de saúde mais agravadas do que os pacientes brancos. Essa diferença ocorre porque os negros em geral possuem uma renda menor e, portanto, tem menos acesso aos serviços de saúde (privados) naquele país.[126] Uma das consequências é que os médicos podem utilizar essa classificação de risco enviesada para formular o tratamento mais adequada para cada paciente, o que no caso dos negros pode estar aquém da sua real necessidade. Embora o estudo seja estrangeiro, considerando as condições socioeconômicas do Brasil provavelmente as mesmas conclusões poderiam ser aplicadas por aqui.

Finalmente, há também uma quarta categoria de viés interno, que ocorre quando o sistema trabalha com conjuntos de dados que não correspondem à realidade daquilo que está sendo representado, isto é, quando as informações estão incompletas ou representam desproporcionalmente certos estratos da população. Neste cenário, o resultado da operação algorítmica será distorcido, sedimentando de modo eficaz a discriminação devido à falha dos dados de entrada iniciais. Considerando que a disponibilidade de dados, o acesso à tecnologia e a participação nas ferramentas digitais estão distribuídos de maneira desigual na sociedade, é necessário que os algoritmos sejam elaborados de modo a lidar com essa diversidade. Do contrário, barreiras econômicas, linguísticas, estruturais ou socioeconômicas podem ser ampliadas pelos mecanismos de inteligência artificial. Sem ajuste adequado, essa característica pode se tornar uma falha sistêmica que reforça os padrões existentes de discriminação por meio de uma descrição estatística pouco representativa que será utilizada pelo algoritmo, gerando tratamento desigual para as pessoas envolvidas. No Reino Unido, por exemplo, o algoritmo utilizado na seleção de candidatos ao visto de imigração teve seu uso descontinuado, no que se tornou talvez o primeiro desafio bem-sucedido a um sistema de tomada de decisão de inteligência artificial naquele país. As críticas se concentraram no fato de que o software estaria reproduzindo as práticas

---

determinado em estudo. A relação de causalidade pode ser demonstrada, por exemplo, por meio de experimentos aleatórios e controlados. Este é um assunto complexo e que envolve frequentemente grande risco de erro, mas em regra as análises demonstram que duas variáveis associadas nem sempre apresentam relação de causa e efeito entre si, e que quaisquer conclusões a esse respeito devem ser feitas com cautela. Para mais detalhes sobre análise de causalidade em estatística consultar: PEARL, Judea. *Causality: Models, Reasoning, and Inference*. Cambridge: Cambridge University Press, 2000. Disponível em: http://bayes.cs.ucla.edu/BOOK-99/book-toc.html. Acesso em 20 de novembro de 2022.

[126] OBERMEYER, Ziad; POWERS, Brian; VOGELI, Christine; MULLAINATHAN, Sendhil. *Dissecting racial bias in an algorithm used to manage the health of populations*. Science nº 366, 2019. pp. 447-453. Disponível em: https://www.ehidc.org/sites/default/files/resources/files/Dissecting%20racial%20bias%20in%20an%20algorithm%20used%20to%20manage%20the%20health%20of%20populations.pdf. Acesso em 20 de novembro de 2022.

racistas que foram institucionalizadas em parte do século passado quanto à origem nacional dos imigrantes.[127] Um episódio em particular, conhecido como *Windrush scandal* (escândalo de Windrush), foi a grande motivação para o governo britânico alterar sua política imigratória.[128]

Esses tipos de vieses podem representar grandes problemas para os usuários, considerando a disseminação cada vez maior das técnicas de inteligência artificial. No caso do aprendizado de máquina, por exemplo, os códigos de programação são complexos e geram resultados por vezes incompreensíveis até mesmo para seus programadores. Não obstante, essa ferramenta é cada vez mais usada em situações do cotidiano, como análise de crédito, empréstimos e contratação de novos trabalhadores, conforme indicado anteriormente. Como esses algoritmos se tornam cada vez mais sofisticados, também ficamais difícil preservar a transparência e explicar com clareza o método pelo qual as máquinas tomam decisões autônomas. Assim, programadores e cientistas de dados podem inadvertidamente ou inconscientemente projetar, treinar ou implantar sistemas de *big data* enviesados, o que é uma consequência inevitável de sua própria cultura e histórico de vida, como acontece com qualquer ser humano.

Os vieses dos algoritmos estão muito associados aos vieses cognitivos que os seres humanos apresentam frequentemente em seu próprio raciocínio, e que são transferidos ao código de programação pelo trabalho do programador ou pelos dados que alimentarão o funcionamento do algoritmo. Os vieses cognitivos atuam como atalhos ou desvios no processo racional do pensamento humano, consistindo em um caminho "mais curto" do qual o cérebro se vale para simplificar a realidade e resolver determinado problema com menos esforço, atingindo a resposta mais rápida, que nem sempre é a correta. Em relação à inteligência artificial, isso poderia ser mitigado pela transparência do código de programação, o que dificilmente ocorre por razões de propriedade intelectual.[129] Por isso a mitigação de vieses deve ser uma preocupação desde a fase de projeto do software, para que os usuários se sintam seguros e confiantes, sabendo que sistemas algorítmicos enviesados são a exceção, e não a regra geral.

Deste modo, já que o uso da inteligência artificial deve se tornar cada vez mais presente na vida cotidiana das pessoas, será necessário dedicar mais atenção para

---

[127] Mais detalhes disponíveis em: https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants. Acesso em 20 de novembro de 2022.

[128] Neste caso houve a prisão e deportação ilegal de cidadãos britânicos negros, devido à interpretação equivocada da legislação vigente nas décadas de 1960 e 1970, que apresentava critérios hoje considerados racistas. Mais detalhes sobre este episódio disponíveis na avaliação independente que foi promovida pelo governo, disponível no seguinte endereço eletrônico:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876336/6.5577_HO_Windrush_Lessons_Learned_Review_LoResFinal.pdf. Acesso em 20 de novembro de 2022.

[129] Sobre este ponto, consultar: STEFFENS, Luana. *A influência dos vieses cognitivos na tomada de decisão pela inteligência artificial: um estudo baseado nas evidências no caso norte-americano COMPAS*. In: Fabio da Silva Veiga; Denise Pires Fincato. (Org.). Estudos de Direito, Desenvolvimento e novas Tecnologias. 1ed. Porto Alegre: Instituto Iberoamericano de Estudos Jurídicos, 2020, v. 1, p. 1-419.

compreender a maneira de operação desses sistemas, avaliando continuamente os dados que alimentam o algoritmo e seu mecanismo de atuação, bem como os resultados produzidos. Inclusive, ainda é comum a crença de que os números seriam "naturalmente" neutros e imparciais, e que representariam sempre a mesma realidade objetiva, o que traz sérias dificuldades e contribui para ofuscar situações discriminatórias que afetam negativamente a vida das pessoas.[130] Assim, os desafios relacionados a essa nova realidade tecnológica incluem sobretudo os resultados das operações automatizadas, que devem sempre garantir que as informações sobre lugares, pessoas, comportamentos, etc. sejam usados de forma adequada, ética e na promoção de princípios democráticos, como a não-discriminação e igualdade de oportunidades.

2.2 Discriminação algorítmica

É claro que as tecnologias que fazem uso da ciência de dados também podem apresentar o potencial de aprimorar a capacidade de detecção e prevenção de discriminação em geral. Existem perspectivas que inclusive defendem o uso de algoritmos para ajudar os seres humanos em seu processo de tomada de decisão, com o objetivo de preservar critérios de equidade e objetividade[131], ou que até mesmo não recomendam a possibilidade da revisão humana de decisões automatizadas, o que será abordado adiante. Porém, o problema desta pesquisa diz respeito aos algoritmos que não funcionam tão bem na prática e podem ampliar situações discriminatórias numa escala maior na medida que em os mecanismos de inteligência artificial são adotados pela sociedade em diversas situações.

Assim, quando essas aplicações tecnológicas não são implementadas de modo adequado, a inteligência artificial pode contribuir na prática para perpetuar, exacerbar ou mascarar situações discriminatórias, conforme já indicado. Nos últimos anos a questão do viés na operação algorítmica vem assumindo uma posição de destaque nas pesquisas acadêmicas e debates legislativos que envolvem o *big data*. Quando se utiliza a ciência de dados para tratar vastas quantidades de dados (alguns dos quais podem nunca se tornar 'informação' de fato), sem que exista interação humana no

---

130 Para o antropólogo Rodrigo Ochigame, o pressuposto de que os números são inerentemente neutros e imparciais serve para ocultar determinadas lutas políticas e reduzir a compreensão do fenômeno da discriminação algorítmica a um critério puramente matemático. Assim, após ajustes no modelo do código de programação utilizado, o algoritmo poderia ser apresentado como uma solução acabada para conflitos de caráter político, como discriminação de minorias. A análise completa de Ochigame pode ser consulta no seguinte endereço eletrônico: https://phenomenalworld.org/analysis/long-history-algorithmic-fairness. Acesso em 20 de novembro de 2022.

131 "There is a large body of research on algorithmic decision making that dates back several decades. And the existing studies on this topic all have a remarkably similar conclusion: Algorithms are less biased and more accurate than the humans they are replacing." O autor Alex P. Miller reconhece que algoritmos podem ser parte da solução, embora seja sempre necessário preservar a transparência e a ética na elaboração do código e no uso dos dados. Artigo disponível em: https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms. Acesso em 20 de novembro de 2022.

processo de tomada de decisão do algoritmo, é preciso se considerar qual será o impacto causado.[132]

Atualmente, há uma percepção entre pesquisadores[133] de que algoritmos podem potencializar diversas espécies de discriminação e promover violações de direitos fundamentais. Existem exemplos[134] na área penal, eleitoral[135], consumerista, etc. que justificam amparo jurídico para sanar as violações originadas pela operação enviesada dos algoritmos. O problema se torna mais sensível na medida em que esses algoritmos são quase sempre desenvolvidos por empresas privadas e que, portanto, detém a sua propriedade[136], de modo que seu mecanismo de funcionamento nem sempre pode ser auditado, como já mencionado.[137] A Tabela 1 a seguir apresenta alguns exemplos de vieses raciais causados por algoritmos.[138]

---

[132] CARRUTHERS, Caroline, JACKSON, Peter.; *The Chief Data Officer's Playbook*. EBSCO Publishing: eBook Collection, 2018.

[133] Esta é a perspectiva de autores abordados ao longo deste artigo, como Cathy O'Neil, Meredith Broussard, Safiya Noble, Tarcízio Silva, dentre outros.

[134] Esses exemplos foram identificados no noticiário eletrônico (brasileiro e estrangeiro), disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; https://www.nexojornal.com.br/externo/2019/11/24/A-parcialidade-dos-algoritmos; https://www.theatlantic.com/technology/archive/2011/04/the-curious-connection-between-apps-for-gay-men-and-sex-offenders/237340; Acesso em 20 de novembro de 2022.

[135] O Provimento nº 71, de 13 de junho de 2018, editado pela Corregedoria Nacional de Justiça inclusive vedou manifestações de magistrados favoráveis ou contrárias a candidatos e partidos políticos que possam ser entendidas como exercício de atividade político-partidária. Esse entendimento foi confirmado pelo Ministro do Supremo Tribunal Federal Roberto Barroso, afirmando que "tais declarações em redes sociais, com a possibilidade de reprodução indeterminada de seu conteúdo e a formação de algoritmos de preferências, contribuem para se alcançar um resultado eleitoral específico, o que é expressamente vedado pela Constituição." (Medida Cautelar em Mandado de Segurança 35793/Distrito Federal, Relator Ministro Roberto Barroso, julgado em 04/09/2018, publicado 06/09/2018).

[136] O Artigo 5º, incisos XXVII, XXVIII e XXIX da Constituição de 1988 juntamente com o Artigo 7º da Lei 9.610 de 1998 (Lei de Direitos Autorais) e a Lei 9.609 de 1998 (Lei do Software) resguardam ao criador o direito de propriedade sobre o código de programação de um algoritmo.

[137] "Se o policiamento preditivo significa que alguns indivíduos terão mais envolvimento policial em suas vidas, é preciso haver um mínimo de transparência", disse em entrevista Adam Schwartz, advogado sênior da Electronic Frontier Foundation. Até que façam isso, o público não deve confiar que os dados inseridos e os algoritmos são uma base sólida para prever qualquer coisa." Tradução livre de "If predictive policing means some individuals are going to have more police involvement in their life, there needs to be a minimum of transparency," Adam Schwartz, a senior staff attorney with the Electronic Frontier Foundation, said in an interview "Until they do that, the public should have no confidence that the inputs and algorithms are a sound basis to predict anything." Disponível em: https://www.mic.com/articles/156286/crime-prediction-tool-pred-pol-only-amplifies-racially-biased-policing-study-shows. Acesso em 20 de novembro de 2022.

[138] A tabela foi retirada (com adaptações) a partir do seguinte artigo: SILVA, Tarcízio. *Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código*. In: Anais do IV Simpósio Internacional LAVITS – Assimetrias e (In)visibilidades: Vigilância, Gênero e Raça. Salvador, Bahia, Brasil, 2019. Disponível em: https://www.researchgate.net/publication/333700308_Racismo_Algoritmico_em_Plataf

Tabela 1 - Exemplos concretos de racismo algorítmico categorizados pelo conteúdo específico de discriminação racial que apresentam

Caso de racismo algorítmico	**Contéudo da discriminação**
Sistema do Google permite empresas exibirem anúncios sobre crime especificamente a afro-americanos	Suposição de criminalidade
Resultados no Google Imagens apresentam hiper-sexualização para buscas como "*garotas negras*"	Exotização; Negação de cidadania
Facebook esconde manifestações contra violência policial racista	Negação de realidades raciais
Google Photos marca fotos de jovens negros com a tag "gorila"	Negação de cidadania
Chatbot da Microsoft torna-se racista em menos de um dia	Diversas
Robôs conversacionais de startups não encontram face de mulher negra; sistemas de visão computacional erram gênero e idade de mulheres negras	Negação de cidadania; exclusão e isolamento
Mecanismos de busca de bancos de imagens invisibilizam famílias e pessoas negras	Negação de realidades raciais
App que transforma selfies equipara beleza à brancura	Exotização; exclusão e isolamento
APIs de visão computacional confundem cabelo negro com perucas	Exotização
Ferramentas de processamento de linguagem natural possuem vieses contra linguagem e temas negros	Patologização de valores culturais
Análise facial de emoções associa categorias negativas a atletas negros	Suposição de criminalidade
Twitter decide não banir discurso de ódio nazista/supremacista branco para não afetar políticos do partido Republicano nos Estados Unidos	Negação de realidades raciais; exclusão

Fonte: Silva, 2019.

ormas Digitais microagressoes e discriminacao em codigo. Acesso em 20 de novembro de 2022.

A sociologia é uma das principais áreas científicas que tem estudado o fenômeno da discriminação. Neste contexto, o trabalho clássico do sociólogo alemão Norbert Elias em uma pequena cidade no interior da Inglaterra contribuiu para estabelecer o conceito de outsider.[139] Sua pesquisa facilitou a compreensão das distinções de valor que os indivíduos acabam por atribuir entre si dentro de um determinado grupo social, em uma espécie de "hierarquia classificatória" (status quo) que apresenta profundas implicações na vida de cada pessoa que compõe esse mesmo grupo. Para Elias, essa estrutura corresponderia a um modelo geral que explicaria (ao menos em parte) a motivação para atitudes discriminatórias dos seres humanos em relação aos indivíduos percebidos como integrantes de um estrato social inferior. Este fato também serve para entender as crescentes tensões sociais e políticas existentes no atual contexto de globalização, pois as pessoas em regra não foram preparadas para a intensificação dos processos de mobilidade social, migrações, mudanças tecnológicas, etc. que vem ocorrendo em todo o mundo.

Mais especificamente sobre a questão envolvendo a discriminação algorítmica, a cientista social norte-americana Safiya Umoja Noble[140] aponta para a falta de consciência por parte da sociedade em geral em relação à atuação silenciosa dos algoritmos enviesados que podem produzir diversos casos de discriminação, como visto acima. Segundo a autora, a atuação discriminatória desses mecanismos de inteligência artificial pode se tornar umas das questões mais relevantes envolvendo os direitos humanos no século XXI.

Embora Noble tenha voltado sua atenção até o momento para o fator humano por detrás da engenharia de software, o principal risco de viés aqui pode ser considerado não-intencional e difícil de detectar, como já demonstrado anteriormente. Ou seja, a análise da autora privilegia a perspectiva de que os vieses inerentes aos programadores humanos (que elaboram os códigos de programação para compor os algoritmos de inteligência artificial) representam uma das principais causas da discriminação algorítmica. Neste sentido, talvez a principal responsabilidade desses profissionais seja a de garantir que esses vieses sejam corrigidos ao longo do desenvolvimento do programa, uma vez que é praticamente impossível treinar seres humanos para não apresentar nenhum tipo de viés. Além disso, ainda que o algoritmo funcione bem, isso não impede que os dados estejam enviesados e comprometam a qualidade da operação ao final, como indicado anteriormente.

De todo modo, Noble também insiste na transparência algorítmica enquanto um meio de fomentar o debate público a respeito de como lidar com os impactos sociais, políticos e econômicos da utilização de mecanismos de inteligência artificial da maneira mais eficaz, por meio de políticas públicas específicas para este tema. A autora também tem o mérito de chamar atenção para o fato de que a tecnologia não deve contribuir para naturalizar a discriminação a qual determinados grupos sociais (sobretudo minorias raciais) estão submetidos historicamente. Essa perspectiva é

---

[139] Em sua pesquisa de campo, Norbert Elias explorou conceitos como superioridade social e moral, autopercepção e reconhecimento, além de pertencimento e exclusão em um grupo social que à primeira vista seria bastante homogêneo. ELIAS, Norbert. *Os estabelecidos e os outsiders: sociologia das relações de poder a partir de uma pequena comunidade*. Rio de Janeiro: Jorge Zahar, 2000.

[140] NOBLE, Safiya Umoja. *Algorithms of oppression: how search engines reinforce racism*. New York: New York University Press, 2018

compartilhada por cientistas de dados como Catherine ("Cathy") O'Neil, que desenvolveu um estudo sobre falhas em modelos matemáticos utilizados pelo big data para compreender (e antecipar) padrões de comportamento humano por meio de algoritmos. Em sua carreira profissional, O'Neil adquiriu progressivamente a percepção de que muitas suposições equivocadas estão disfarçadas nas fórmulas matemáticas e terminam compondo o código de programação sem testagem ou reflexão prévia por parte dos profissionais envolvidos em sua elaboração. Na visão da autora, isso ocorre devido ao fato de que os eventuais prejudicados (pela decisão automatizada enviesada) apresentam dificuldade de comprovar suas suspeitas ao mesmo tempo em que existe certa presunção de tecnicalidade e objetividade em relação aos algoritmos. A principal razão para este desinteresse das empresas estaria associada à perspectiva de que os lucros gerados pelo negócio desestimulam a busca pela revisão ou investigação de eventuais problemas envolvendo a ferramenta de inteligência artificial utilizada.

Neste caso, um dos tipos mais comuns de viés apontados por O'Neil envolve o feedback loop, conforme descrito nas páginas anteriores. Sem contraponto com ao menos parte da realidade, não há como saber se as informações geradas pelo mecanismo estatístico do algoritmo estão na verdade produzindo análises defeituosas e prejudiciais, sem nunca de fato aprender com seus erros. A autora aponta que na prática alguns mecanismos de inteligência artificial acabam por criar uma realidade paralela que será usada para justificar (matematicamente) os seus próprios resultados. Esse tipo de modelo tende a se retroalimentar e se perpetuar enquanto não houver correção dos dados. Nas palavras de O'Neil: [141]

> Como deuses, esses modelos matemáticos eram opacos, seu funcionamento invisível para todos, exceto para os sacerdotes mais elevados em seu domínio: matemáticos e cientistas da computação. Seus veredictos, mesmo quando errados ou prejudiciais, estavam fora de discussão ou apelação. E eles tendiam a punir os pobres e oprimidos em nossa sociedade, enquanto tornavam os ricos mais ricos. (...) Isso ocorre, em parte, porque eles são projetados para avaliar um grande número de pessoas. Eles se especializam em grandes quantidades e são baratos. Isso é parte de seu apelo. Os ricos, em contraste, frequentemente se beneficiam de análises individualizadas. Um escritório de advocacia ou uma escola preparatória exclusiva se apoiarão muito mais em recomendações e entrevistas cara a cara do que uma rede de fast food ou uma rede escolar urbana sem dinheiro. Os privilegiados, veremos repetidamente,

[141] "Like gods, these mathematical models were opaque, their workings invisible to all but the highest priests in their domain: mathematicians and computer scientists. Their verdicts, even when wrong or harmful, were beyond dispute or appeal. And they tended to punish the poor and the oppressed in our society, while making the rich richer. (...) This is, in part, because they are engineered to evaluate large numbers of people. They specialize in bulk, and they're cheap. That's part of their appeal. The wealthy, by contrast, often benefit from personal input. A white-shoe law firm or an exclusive prep school will lean far more on recommendations and face-to-face interviews than will a fast-food chain or a cash-strapped urban school district. The privileged, we'll see time and again, are processed more by people, the masses by machines." O´NEIL, Cathy. *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York: Crown, 2016. pp 10-14.

> recebem tratamento majoritariamente feito por pessoas, as massas por máquinas. (tradução livre)

Ainda, jornalistas como Meredith Broussard[142] chamam a atenção para todas as consequências inesperadas que novas tecnologias trazem consigo, ao relatar um caso onde um *drone* foi alvejado ao sobrevoar a casa de uma pessoa nos Estados Unidos. O dono da casa se sentiu ameaçado e, desconhecendo a origem e propriedade do objeto, atirou no robô aéreo enquanto este sobrevoava sua residência. A polícia foi chamada até o local, mas não soube lidar com o fato, e os agentes decidiram prender o proprietário do imóvel por ser quem estava armado. Por fim, um tribunal posteriormente o inocentou por considerar que exercia seu direito legítimo de defender sua propriedade. Este fato é utilizado pela autora para evidenciar que quase sempre as empresas que introduzem novas tecnologias no mercado não estão conscientes dos riscos envolvidos na utilização de seus produtos, mesmo diante do fato bastante conhecido de que a população norte-americana é uma das mais armadas do mundo.[143]

No caso da discriminação algorítmica, menos inteligível ao público leigo do que o exemplo relatado acima, Broussard afirma que muitos profissionais e empresas possuem uma visão ingênua sobre como as novas tecnologias serão usadas. Sem a cautela necessária, a autora acredita que a novas ferramentas de inteligência artificial podem prestar um serviço incompatível com o interesse público, seguindo o raciocínio exposto nos parágrafos anteriores.

Como se sabe, o ordenamento jurídico brasileiro é refratário a quaisquer formas de preconceito e discriminação, seguindo as determinações constitucionais que promovem a igualdade entre os cidadãos. O que não significa, claro, que toda forma de discriminação seja negativa ou inválida, pois tanto a igualdade formal (isonomia em sentido estrito) quanto a igualdade material (que está associada à ideia de justiça distributiva e social) devem ser atendidas pelo Estado.

Na visão de Luís Roberto Barroso,[144]

> a Constituição Federal de 1988 consagra o princípio da igualdade e condena de forma expressa todas as formas de preconceito e discriminação. A menção a tais valores vem desde o preâmbulo da Carta, que enuncia o propósito de se constituir uma "sociedade fraterna, pluralista e sem preconceitos". O art. 3º renova a intenção e lhe confere inquestionável normatividade, enunciando serem objetivos fundamentais da República "construir uma sociedade livre, justa e solidária" e "promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação". O caput do art. 5º reafirma que "todos são iguais perante a lei, sem distinção de qualquer

142 BROUSSARD, Meredith. *Artificial unintelligence: how computers misunderstand the world*. Cambridge: MIT Press, 2018.

143 BROUSSARD, Meredith. Idem, ibidem. p. 77 – 78.

144 BARROSO, Luís Roberto. *Diferentes, mas iguais: o reconhecimento jurídico das relações homoafetivas no Brasil*. Revista Brasileira de Direito Constitucional, v. 17, p. 105-138, 2011. Disponível em: http://www.luisrobertobarroso.com.br/wp-content/uploads/2017/09/diferentes_mas_iguais_atualizacao_2011.pdf. Acesso em 20 de novembro de 2022.

> natureza". O constituinte incluiu, ainda, menções expressas de rejeição ao racismo e à discriminação contra as mulheres.

Neste ponto, o objeto desta pesquisa trata da questão da igualdade material, que envolve enormes dificuldades teóricas e práticas na sua concretização. Barroso defende que a concreção do direito geral de igualdade envolve três dimensões principais: formal, material e também a igualdade enquanto reconhecimento (dimensão simbólica que impacta na autoestima dos indivíduos).[145] Essas três grandes categorias precisam ser atendidas para que a desigualdade seja reduzida em um país como o Brasil, marcado historicamente por profundas diferenças entre seus cidadãos. De todo modo, na visão de Barroso é necessário haver intervenção estatal para garantir a efetividade dos mandamentos constitucionais em âmbito público e privado, pois[146]

> onde não exista um motivo relevante e legítimo que justifique diferença no tratamento, a equiparação deve ser a conduta de todos os órgãos e agentes públicos e, dentro de certa medida, deve ser imposta até mesmo aos particulares.

Portanto, promover a igualdade material requer políticas públicas de caráter universalista, conduzidas pelo Estado, como é o caso das ações afirmativas, por exemplo. A atuação do poder público é essencial para mitigar situações históricas de discriminação contra determinados grupos sociais. Além disso, a garantia da igualdade em todas as suas dimensões é algo que compõe o próprio conceito de democracia, ao assegurar igualdade de oportunidades. Ela também possibilita o livre desenvolvimento da personalidade de todos os cidadãos e favorece o crescimento do indivíduo, inserido em uma sociedade plural e diversificada.

Assim, em síntese, este capítulo abordou alguns dos principais tipos de vieses que originam situações discriminatórias em mecanismos de inteligência artificial. Prosseguindo com o raciocínio exposto acima, a análise agora se volta para a regulação da inteligência artificial enquanto possível estratégia para oferecer condições que possam neutralizar a discriminação algorítmica.

3. O ambiente regulatório brasileiro

Até este ponto, foi apresentado de modo breve o funcionamento de algumas das principais ferramentas de inteligência artificial e dos eventuais vieses que podem apresentar. Neste capítulo final o objetivo específico consiste em investigar se os mecanismos jurídicos disponíveis são suficientes para lidar com os problemas associados ao viés algorítmico.

Conforme mencionado ao longo do texto, a Constituição atual tem como um de seus objetivos fundamentais garantir a não-discriminação entre os indivíduos no Brasil. Porém, como se sabe, a mera disposição da Lei Maior nem sempre é suficiente para garantir sua eficácia. Assim, deste ponto em diante o texto busca identificar o método mais eficaz de concretizar o mandamento citado. Considerando que o Brasil não dispõe de uma política pública especificamente voltada para o tema do viés algorítmico, surge a preocupação de como conferir eficácia ao texto constitucional e

[145] Conforme voto proferido no julgamento da Ação Declaratória de Constitucionalidade 41, julgada pelo Plenário do STF em 08 de junho de 2017.

[146] BARROSO, Luís Roberto. Idem, ibidem.

garantir a não-discriminação no uso da inteligência artificial. Ao longo das próximas páginas, a abordagem desta pesquisa se volta especialmente para a questão da revisão humana de decisões automatizadas, entendida aqui como um método possível de mitigação dos prejuízos causados pelos algoritmos enviesados e que ficou de fora da redação final da LGPD, conforme já mencionado.

Neste contexto, o argumento principal deste trabalho diz respeito à necessidade de uma política pública específica que esteja apta a concretizar a respectiva disposição constitucional de garantia da não-discriminação. Isto requer uma atuação positiva por parte do legislador para garantir a efetividade deste mandamento, por se tratar de norma que não possui eficácia direta e imediata.

Como visto anteriormente, o Marco Civil da Internet não tem incidência específica sobre a questão da discriminação algorítmica. A LGPD, por sua vez, deixou de oferecer a obrigatoriedade de revisão humana de decisões automatizadas como um recurso para remediar administrativamente eventuais prejuízos aos indivíduos afetados. Deste modo, este capítulo analisa inicialmente a capacidade do próprio setor privado de se adequar voluntariamente ao arcabouço previsto pela Constituição, sobretudo por meio das políticas internas de ética das grandes empresas de tecnologia. Após, a atenção é dedicada ao sistema regulatório vigente propriamente dito, para identificar eventuais insuficiências normativas. É desnecessário insistir, entretanto, que os direitos fundamentais previstos no ordenamento jurídico brasileiro permanecem como o principal meio para proteger as pessoas de situações discriminatórias.

3.1 A dimensão ética

No campo filosófico, a ética tem difícil definição, embora esteja presente em todas os aspectos da vida humana. Isto ocorre porque o ser humano possui capacidade de reflexão sobre os seus próprios atos, o que lhe confere a possibilidade de escolha, de modo consciente. Essa liberdade de agência é um dos fundamentos da ética na medida em que trabalha com a operação sobre alternativas, ou seja, qualquer tomada de decisão requer um grau mínimo de consciência da opção escolhida. A faculdade de escolher, então, consiste em uma obrigação imposta ao indivíduo, já que o processo decisório em geral apresenta uma multiplicidade de caminhos onde é necessário avaliar e decidir por qual deles seguir.

Deste modo, a tomada de decisão humana supõe a avaliação dos múltiplos fatores que perfazem uma situação complexa, perpassada por valores morais, estéticos, religiosos, de utilidade, dentre outros. Na visão de Eduardo Bittar, atualmente as relações econômicas e de reprodução social da vida material humana constituem uma das principais determinantes das possibilidades éticas. O autor argumenta que "uma palavra em desuso como esta – ética –, apesar de seu valor, tem sido considerada simplesmente um obstáculo a mais a atravancar o andamento das facilidades do pragmatismo consumista e comercial."[147]

Como acontece em todos os segmentos econômicos e ramos profissionais, a preocupação com princípios éticos a respeito do trabalho desenvolvido é essencial para garantir resultados compatíveis com o interesse público. Em relação ao *big data*, a ética

[147] BITTAR, Eduardo Carlos Bianca. *Curso de ética jurídica: ética geral e profissional*. 13ª ed. São Paulo: Saraiva, 2016. p. 18.

desempenha um papel fundamental para assegurar que sua utilização esteja de acordo com valores positivos para a sociedade, uma vez que a automação do processo de análise e tomada de decisões pode trazer amplas consequências para as pessoas envolvidas, conforme demonstrado no capítulo anterior. A responsabilidade e o compromisso ético da ciência de dados nesse ponto é ainda maior:[148]

> Cometer erros éticos pode ter um grande impacto no futuro de como tratamos os dados. Se errarmos, a percepção do público pode mudar muito rapidamente e ter um impacto muito negativo sobre o que podemos fazer; as leis podem mudar e exigir conformidade, mas à medida que o uso de dados evolui tão rapidamente, as leis que o regem terão abrangência sobre o que os dados precisam que elas cubram? De certa forma, já estamos tentando lidar com isso no nível legislativo, mas estamos abordando os problemas centrais que tentamos resolver ou estamos nos restringindo demais? E é esse o preço que pagamos por não levar esta área e sua segurança a sério o suficiente? No entanto, temos que progredir, isso é inevitável; a estagnação não serve para nada, então como podemos inovar com responsabilidade? (...) O primeiro passo é entender o papel que desempenhamos em tudo isso e assumir a responsabilidade por isso. Pense nas consequências tanto quanto possível, tanto as diretas quanto as não intencionais, e monitore a reação a elas. Procurar coisas desconhecidas é uma posição realmente difícil de se estar, mas se você não olhar, provavelmente nunca as verá. Pelo menos monitorar o que está acontecendo lhe dá essa chance de lutar. Em última análise, você tem que agir. Este é um campo em evolução, não tenha medo de admitir se as coisas não saírem do jeito que você queria e precisar corrigir a trajetória. (tradução livre)

De certa forma, é perceptível que as considerações éticas venham se tornando uma preocupação cada vez mais relevante na atuação das empresas em geral, e não apenas por razões de imagem para conquistar boa aceitação de seus produtos e serviços no mercado.[149] Somente no ano de 2020, por exemplo, diversos fatores em

---

148 "Making ethical mistakes can have a big impact on the future of how we treat data. If we get it wrong public perception can change really quickly and have a very negative impact on what we can do; laws can change and enforce compliance but as the use of data evolves at such a pace, will the laws that legislate it cover what the data needs them to cover? In some ways we are already trying to deal with this at the legislative level, but are we addressing the core problems we are trying to fix or are we constraining ourselves too much? And is this the price we are paying for not taking this area and its security seriously enough? Yet we have to progress, that is inevitable; stagnation serves no purpose, so how do we innovate responsibly? (…) The first step is to understand the role we play in all of this and to take responsibility for it. Think through the consequences as much as possible, both the direct and the unintended ones, then monitor for the reaction to it. Looking for your unknown unknowns is a really difficult position to be in but if you don't look you will probably never see them. At least monitoring what is happening gives you that fighting chance. Ultimately you have to take action. This is an evolving field, don't be afraid to admit it if things didn't go the way you wanted them to and you need to course-correct." CARRUTHERS, Caroline, JACKSON, Peter. Idem, ibidem. p. 139.

149 Além das próprias vítimas diretas da discriminação algorítmica, qualquer descuido em relação ao uso ético da tecnologia pode rapidamente causar enormes estragos à imagem pública da empresa envolvida, prejudicando relações com clientes e entidades reguladoras, e reduzindo seus ganhos econômicos. Revelações recentes da

âmbito internacional contribuíram para colocar a ética entre as prioridades das empresas de maneira inédita. A pandemia de Covid-19, as frequentes manifestações populares por justiça e equidade social, a aceleração da transformação digital em curso e a crescente tomada de consciência a respeito da discriminação e da exclusão de oportunidades para alguns segmentos da população intensificaram as demandas para que as organizações adotem certas medidas como resposta, que vão desde o apoio a causas sociais ao anúncio de incentivos para a promoção da diversidade. No mercado consumidor, por exemplo, uma pesquisa recente nos Estados Unidos revelou que a maioria significativa (68%) do público vê a sustentabilidade como sendo muito importante ao adquirir algum produto ou serviço, e percentual relativamente alto (49%) pagariam até mesmo a mais por produtos sustentáveis.[150] Esses dados são ainda mais significativos quando se considera as faixas etárias mais jovens. Os nascidos a partir da década de 1980 estão entre as pessoas que mais demonstram preocupação a respeito das consequências éticas da adoção de tecnologias envolvendo inteligência artificial em seus locais de trabalho.[151]

Em relação ao viés algorítmico especificamente, em pesquisa recente[152] entre profissionais de cargo gerencial em empresas da área de tecnologia, constatou-se que uma proporção bastante alta (94% nos Estados Unidos e 86% no Reino Unido) tinha a intenção de aumentar o investimento em medidas preventivas contra mecanismos de inteligência artificial enviesados no ano de 2020. Esse cenário se repete para outras categorias de trabalhadores da área de tecnologia. Um estudo[153] no Reino Unido identificou que 28% dos entrevistados presenciaram decisões de tecnologia eticamente questionáveis, e que 18% inclusive deixaram as organizações em que atuavam por conta deste fator.

O compromisso com padrões éticos mínimos demonstrado pelas empresas de tecnologia e seus profissionais se torna mais relevante em um cenário como o brasileiro, onde não há um sistema regulatório específico para lidar com o problema da

---

Microsoft e do Google para grupos de investidores advertiram sobre o dano em potencial que uma inteligência artificial utilizada de modo indevido pode causar em suas respectivas marcas. Mais detalhes estão disponíveis em: https://www.theverge.com/2019/2/11/18220050/google-microsoft-ai-brand-damage-investors-10-k-filing.

Acesso em 20 de novembro de 2022.

150 A pesquisa foi realizada pela empresa de tecnologia norte-americana CGS, e está disponível no seguinte endereço eletrônico: https://www.cgsinc.com/en/infographics/CGS-Survey-Reveals-Sustainability-Is-Driving-Demand-and-Customer-Loyalty. Acesso em 20 de novembro de 2022.

151 Conforme pesquisa realizada pela organização norte-americana Genesys em seis países de economia avançada. Detalhes disponíveis em: https://www.prnewswire.com/news-releases/new-workplace-survey-finds-nearly-80-of-employers-arent-worried-about-unethical-use-of-ai--but-maybe-they-should-be-300911214.html. Acesso em 20 de novembro de 2022.

152 Maiores detalhes disponíveis em: https://www.computerweekly.com/news/252474408/IT-chiefs-recognise-the-risks-of-artificial-intelligence-bias. Acesso em 20 de novembro de 2022.

153 O estudo da organização britânica Doteveryone pode ser consultado no seguinte endereço eletrônico: https://www.doteveryone.org.uk/report/workersview/. Acesso em 20 de novembro de 2022.

discriminação algorítmica. Além disso, grande parte da população nacional poderia não estar apta para utilizar os serviços tecnológicos de última geração, estando em posição vulnerável diante de quaisquer efeitos negativos que o uso das tecnologias mais recentes podem apresentar. Em países menos desenvolvidos (como o Brasil), a dependência dos usuários em relação às principais empresas de tecnologia pode estar bastante acentuada, sobretudo no que diz respeito às redes sociais.[154] Este fato provavelmente contribui para que determinados vieses nessas plataformas sejam amplificados.[155]

Como este trabalho apresentou ao longo das páginas anteriores, existe uma série de desafios no uso ético de qualquer tecnologia, que deve ser administrada e monitorada tão ativamente quanto qualquer outro aspecto da instituição que faz uso da ferramenta em questão. No âmbito empresarial, as políticas internas de promoção de princípios éticos podem constituir o principal método para atingir esse objetivo e gerar resultados positivos para seus clientes e controladores.[156]

Na medida em que os mecanismos de inteligência artificial se desenvolvem e ganham maior complexidade, se torna mais difícil para qualquer organização avaliar se o seu funcionamento ocorre do modo pretendido. Este ponto é especialmente delicado em relação às áreas mais sensíveis, como assistência à saúde, justiça criminal e acesso a serviços financeiros. Em muitos casos pode mesmo ser difícil determinar qual medida seria apropriada diante de um dilema ético ou conflito de direitos fundamentais, o que torna ainda mais necessária a existência de uma resposta normativa para esse assunto. É neste ponto que a regulação jurídica propriamente dita pode desempenhar um papel complementar e bastante necessário para ir além das políticas internas organizacionais, como se demonstra a seguir. Até mesmo porque a proteção aos direitos fundamentais não deve estar subordinada ao voluntarismo de quaisquer agentes do setor privado, devendo ser garantida pelo Estado por todos os meios disponíveis. Nenhuma reivindicação de conduta "ética" empresarial ou profissional pode ser considerada apta a substituir a urgência de restrições legalmente aplicáveis à implantação de tecnologias que detém o potencial de violar as garantias básicas previstas no ordenamento jurídico brasileiro.

---

154 Detalhes acerca da pesquisa estão disponíveis na página eletrônica a seguir: https://qz.com/333313/milliions- of-facebook-users-have-no-idea-theyre-using-the-internet/. Acesso em 20 de novembro de 2022.

155 Em 2018 o Facebook foi inclusive acusado pela ONU de negligência no caso do genocídio da minoria étnica Rohingya em Myanmar, no sudeste asiático. Detalhes em: https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1GO2PN. Acesso em 20 de novembro de 2022.

156 Sobre este ponto, existem algumas propostas de princípios éticos gerais, como a formulada pela Comissão Europeia, disponível no seguinte endereço eletrônico: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Há também outra proposta, de caráter similar, do Berkman Klein Center for Internet and Society da Universidade de Harvard, que está disponível aqui: https://cyber.harvard.edu/topics/ethics-and-governance-ai. Acesso em 20 de novembro de 2022.

3.2 Regulação jurídica

O conceito de regulação pode apresentar diversos significados dependendo do contexto. Na economia, por exemplo, uma das definições mais conhecidas é a do professor norte- americano Nicholas Gregory Mankiw, que afirma se tratar de uma intervenção estatal destinada a promover a eficiência e a equidade econômicas, isto é, resolver falhas de mercado em prol da competividade e realizar justiça social.[157]

Para o direito brasileiro há também uma variedade conceitual grande, onde algumas análises privilegiam um ou outro aspecto para caracterizar e classificar a regulação. Essa discussão doutrinária não será abordada aqui em virtude dos limites e propósitos deste artigo. Entretanto, como se sabe, a noção jurídica não pode se limitar à simples reprodução de teorias políticas ou econômicas, ainda que de fato possua fundamentos políticos e econômicos. Sob o ponto de vista do direito administrativo especificamente, a regulação é exercida pelo Estado por meio da edição de normas jurídicas em sentido amplo, ou seja, todas aquelas emitidas pelo Estado no exercício regular de suas funções legislativa, administrativa e jurisdicional. Neste sentido, de acordo com José dos Santos Carvalho Filho[158], o poder público poderia atuar de duas maneiras na ordem econômica: enquanto "Estado Regulador" e "Estado Executor". Nesta última hipótese haveria uma intervenção estatal específica para atuar diretamente na atividade econômica como se fizesse parte da iniciativa privada. Já a primeira categoria diz respeito ao poder de reger e fiscalizar a economia tal como é organizada pelos agentes econômicos privados, e é neste sentido que se analisa o papel do Estado ao longo desta pesquisa.

No caso brasileiro, a atividade reguladora do Estado está disciplinada entre os artigos 170 e 181 da Constituição de 1988. O artigo 170[159] estebelece as finalidades constitucionais da regulação, enquanto que o artigo 174[160] trata dos meios pelos quais ela é realizada: fiscalização, incentivo e planejamento[161]. A partir destes dois dispositivos

---

[157] MANKIW, Nicholas Gregory. *Principles of Economics*. 5ª ed. South-Western Cengage Learning, 2007. p. 74.

[158] CARVALHO FILHO, José dos Santos. *Manual de Direito Administrativo*. 30ª ed. São Paulo: Atlas, 2016. p. 967.

[159] CRFB/88, Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: I - soberania nacional; II - propriedade privada; III - função social da propriedade; IV - livre concorrência; V - defesa do consumidor; VI - defesa do meio ambiente, inclusive mediante tratamento diferenciado conforme o impacto ambiental dos produtos e serviços e de seus processos de elaboração e prestação; VII - redução das desigualdades regionais e sociais; VIII - busca do pleno emprego; IX - tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no País. Parágrafo único. É assegurado a todos o livre exercício de qualquer atividade econômica, independentemente de autorização de órgãos públicos, salvo nos casos previstos em lei.

[160] CRFB/88, Art. 174. Como agente normativo e regulador da atividade econômica, o Estado exercerá, na forma da lei, as funções de fiscalização, incentivo e planejamento, sendo este determinante para o setor público e indicativo para o setor privado.

[161] A Lei nº 13.874/2019, conhecida como Lei da Liberdade Econômica não incluiu o direito do consumidor entre os ramos do direito abarcados por suas disposições, de modo que sua redação parece não trazer nenhuma determinação específica com consequências para os casos de discriminação algorítmica, em primeira análise.

é possível compreender que o Estado tem o poder-dever de agir positivamente para atingir os objetivos estabelecidos no texto constitucional no que tange à supervisão da ordem econômica, por meio do poder de polícia do qual dispõe. Deste modo, por exemplo, o poder público deve conciliar a manutenção da livre iniciativa com a proteção aos consumidores e a redução das desigualdades sociais, o que pode ser feito por meio do regramento e inspeção específicos para cada atividade econômica. Neste sentido, o atual estágio tecnológico demanda ainda mais atenção e velocidade do legislador, considerando a complexidade dos "aspectos decorrentes da inovação na vida das pessoas e das empresas, desde os direitos de personalidade e intimidade, até aqueles pertinentes ao âmbito do direito do consumidor, tributário, dos contratos, criminal, propriedade imaterial e outros."[162]

Se no Brasil ainda não há política regulatória específica, no direito estrangeiro a União Europeia tem sido o principal fórum de discussão política e de regulação do *big data*.[163] Conforme indicado na parte inicial deste texto, o RGPD prevê especificamente a revisão humana de decisões automatizadas como um direito dos indivíduos. Mas ainda permanecem desafios, e o Parlamento Europeu deve seguir implementando novas normas que regulem a área de tecnologia em seus diferentes aspectos.[164]

Na visão de Marietje Schaake,[165] que atuou como deputada no Parlamento Europeu na última década, a União Europeia seria a única reguladora de fato das grandes empresas transnacionais de tecnologia sediadas principalmente no Vale do Silício (no estado norte- americano da Califórnia). Seu principal argumento é de que a tecnologia só pode ser democrática quando submetida a um debate público envolvendo os cidadãos e seus representantes políticos, de modo que a tributação e a regulação dessa área econômica não significam um ataque às empresas de

---

[162] DOMINGUES, Paulo Sérgio. *Legislativo 4.0: o desafio da criação de novas leis para um mundo em mutação*. In: Cadernos Adenauer XXI, nº1. A quarta revolução industrial: inovações, desafios e oportunidades. Rio de Janeiro: Fundação Konrad Adenauer, 2020. p. 56. Disponível em: https://www.kas.de/pt/web/brasilien/einzeltitel/-/content/cadernos-adenauer-1-2020-1. Acesso em 21 de novembro de 2022.

[163] Nos Estados Unidos a *California Consumer Privacy Act* é a principal lei que regula o uso dos dados, enquanto não é editada norma federal que trate do assunto. Sobre este assunto: HARTZOG , Woodrow; RICHARDS, Neil. *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. Rev. 1687 (2020). Disponível em: https://lawdigitalcommons.bc.edu/bclr/vol61/iss5/3. Acesso em 21 de novembro de 2022.

[164] No cenário internacional as organizações sem fins lucrativos Anistia Internacional e Access Now formularam a "Declaração de Toronto", um documento que tem por objetivo estabelecer parâmetros para a operação de algoritmos de aprendizado de máquina, e convidando Estados e empresas de tecnologia a garantir que os algoritmos respeitem os princípios básicos de igualdade e não-discriminação. O documento pode ser acessado aqui: https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf.

Acesso em 21 de novembro de 2022.

[165] Conforme entrevistas disponibilizadas nos seguintes endereços eletrônicos: https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm; https://www.newyorker.com/tech/annals-of-technology/what-can-america-learn-from-europe-about-regulating-big-tech?utm_source=twitter&utm_medium=social&utm_campaign=onsite-share&utm_brand=the-new-yorker&utm_social-type=earned. Acesso em 21 de novembro de 2021.

informática nem aos seus produtos. O objetivo da regulação consiste em garantir que os produtos sejam seguros e estejam em conformidade comas leis e os valores das sociedades em que operam, observando em especial os critérios de transparência e privacidade.[166]

Segundo Schaake, os segredos comerciais e os acordos de confidencialidade muitas vezes impedem que as informações sobre o funcionamento das grandes empresas privadas de tecnologia sejam divulgadas ao público. Essas proteções jurídicas dificultam a resposta estatal em relação aos riscos que já existem e também impedem pesquisas independentes sobre os efeitos pretendidos e não intencionais dos produtos dessas organizações. O resultado é o bloqueio do debate público bem informado sobre digitalização e segurança, inibindo a formulação de políticas com base em evidências. Para Schaake, o Estado tem o dever de regular esta seara para garantir o acesso às informações de interesse público, lembrando que a iniciativa privada deve atuar em consonância com os princípios universais dos direitos humanos, o que precisa ser exigido das lideranças políticas internacionais.

Conforme indicado, no âmbito europeu o RGPD disciplinou a tomada de decisão automatizada na era do *big data* e estabeleceu a revisão humana como um meio de garantir a transparência de tais decisões. Além disso, no caso de decisões automatizadas envolvendo dados pessoais, o RGPD obriga o responsável pelo tratamento a fornecer ao titular dos dados "informações significativas sobre a lógica envolvida", conforme se depreende da leitura do artigo 13, inciso 2, alínea f e artigo 14, inciso 2, alínea g.[167] Neste ponto, existe um debate a respeito do direito do usuário de obter explicações sobre a decisão automatizada que afete seus interesses jurídicos. Embora esse direito em princípio se encaixe bem na intenção mais ampla do RGPD de promover um alto nível de transparência, ele também levanta algumas questões, como o que exatamente precisaria ser revelado ao titular dos dados e o que se entende por explicação de uma decisão automatizada baseada em algoritmos. Além de obstáculos técnicos, também existem questões relacionadas à propriedade intelectual que não podem ser negligenciadas.[168] Nos próximos anos, o Parlamento Europeu deverá

[166] Em relação à privacidade, o professor norte-americano Daniel J. Solove argumenta que é mais eficaz criar mecanismos regulatórios com foco no acesso, uso, armazenamento e transferência de dados do que instituir direitos (e responsabilidades) aos usuários (detentores destes dados). SOLOVE, Daniel J., *The Myth of the Privacy Paradox*. George Washington Law Review, Vol. 89, 2021. p. 40. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265. Acesso em 21 de novembro de 2022.

[167] RGPD, artigo 13: informações a facultar quando os dados pessoais são recolhidos junto do titular: (...) 2. Para além das informações referidas no nº 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente: (...) f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, nºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.; O artigo 14 possui idêntica determinação, porém incidindo em relação aos casos em que as informações não são recolhidas junto ao seu titular.

[168] Na dinâmica do atual desenvolvimento tecnológico é válido refletir sobre certa limitação nos direitos de propriedade industrial, tomando por base a teoria da função social da propriedade. Essa medida pode inclusive auxiliar o desenvolvimento dos países menos desenvolvidos como o Brasil diante dos atuais desafios trazidos pela

enfrentar o desafio de buscar encontrar formas de conciliar a exigência de transparência com os interesses das empresas de tecnologia.

O debate se torna ainda mais complexo na medida em que há posições contrárias ao direito de revisão humana das decisões automatizadas. Existem pesquisadores[169] que defendem que a intervenção humana em um processo automatizado e o direito à informação a respeito de como a decisão foi tomada pelo algoritmo dificilmente serão remédios jurídicos suficientes para eventuais danos causados pela inteligência artificial, como a discriminação algorítmica. Nesse raciocínio, por exemplo, no caso do RGPD ainda não haveria clareza a respeito dos institutos elencados em seu texto; tampouco existiria uma definição precisa sobre o tipo de informação a respeito do funcionamento da tecnologia que deve ser disponibilizada ao usuário. Neste caso, a solução estaria em outros dispositivos trazidos pelo próprio RGPD, como o direito ao esquecimento e a portabilidade de dados pessoais, bem como processos de avaliação e certificação dos sistemas algorítmicos por instituições credenciadas.

Assim, a regulação jurídica da inteligência artificial deve ter o objetivo de proteger os usuários de eventuais danos e manter o mercado livre para a competição econômica, ou seja, preservar o interesse público e proteger o desenvolvimento tecnológico. Qualquer regulamento nesse sentido deve sopesar os riscos e os benefícios que a adoção da inteligência artificial pode trazer para a sociedade. Inclusive, as leis já existentes deverão ser adaptadas a essa nova realidade, em que a tecnologia se torna cada vez mais relevante para o atual modelo econômico global. Além disso, os reguladores devem ter em mente que seu trabalho não pode restringir a inovação tecnológica benéfica em virtude do aumento exagerado dos custos de conformidade com as normas e parâmetros estabelecidos. O governo federal norte-americano apontou que a regulação da inteligência artificial poderia inclusive ser pensada caso a caso, sendo inserida nas normas que já regem determinado produto no momento em que o mesmo seja atualizado para incluir alguma ferramenta inteligente (como por exemplo no caso da indústria automobilística em relação aos carros autônomos).[170]

---

globalização. Sobre este assunto, consultar: BRUCH, Kelly Lissandra; HOFF, Debora Nayar; DEWES, Homero. *A função social do direito de propriedade industrial como alternativa de governabilidade aos países em desenvolvimento: um estudo sobre a propriedade industrial de plantas*. Direito, Estado e Sociedade, v. 32, 2008. p. 149. Disponível em: https://www.researchgate.net/publication/236897426_Funcao_social_do_direito_de_propriedade_industrial_como_alternativa_de_governabilidade_aos_paises_em_desenvolvimento_um_estudo_sobre_a_propriedade_industrial_de_plantas. Acesso em 21 de novembro de 2022.

169 Sobre este assunto, consultar: EDWARDS, Lilian; VEALE, Michael. *Slave to the Algorithm? Why a Right to Explanation is Probably Not the Remedy You are Looking for*. SSRN Electronic Journal, 2017. Disponível em: https://www.researchgate.net/publication/318003528_Slave_to_the_Algorithm_Why_a_Right_to_Explanationn_is_Probably_Not_the_Remedy_You_are_Looking_for. Acesso em 21 de novembro de 2022.

170 THE WHITE HOUSE. *Preparing for the Future of Artificial Intelligence*. Executive Office of the President, 2016. pp. 17. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf. Acesso em 21 de novembro de 2022.

Como se sabe, a regulamentação eficaz de qualquer tecnologia complexa pressupõe uma assesssoria técnica especializada para ajudar a orientar a tomada de decisão dos representantes políticos em seu trabalho legislativo, além de supervisionar todas as fases do processo regulatório. Esse é um desafio ainda maior para países em desenvolvimento como o Brasil, onde provavelmente será necessário desenvolver pesquisas e produzir conhecimento a respeito das particularidades da realidade nacional diante das potencialidades e riscos que a inteligência artificial pode representar. O trabalho científico realizado por profissionais de diferentes perspectivas e qualificações, a participação pública e a troca de conhecimento entre o governo federal e os governos estaduais e municipais, universidades, centros de pesquisa, dentre outras organizações pode contribuir para que o melhor modelo regulatório seja alcançado.

Talvez o principal objetivo da regulação seja fomentar a criação de melhores mecanismos de inteligência artificial desde o princípio, para que não seja preciso se dedicar tanto à salvaguarda de direitos individuais de cada usuário. Além disso, o fortalecimento de agências reguladores e organizações da sociedade civil pode ajudar na supervisão e análise dos critérios de precisão, imparcialidade e integridade que se espera das novas tecnologias.

Em síntese, este capítulo abordou a ética e a regulação como maneiras de mitigar os efeitos da discriminação algorítmica, tarefa que deve ser interdisciplinar e envolver as empresas de tecnologia (e outras organizações da sociedade civil) e o poder público. Como indicado ao longo do texto, este é um desafio significativo. Porém, o esforço de evitar a discriminação algorítmica e proteger os indivíduos de seus resultados prejudiciais indesejados é uma medida que pode gerar a confiança de que a utilização da inteligência artificial é segura e fomentar ainda mais o desenvolvimento dessa modalidade tecnológica.

4 Conclusão

A motivação para esta pesquisa se deve ao fato de que a discussão sobre os impactos sociais e jurídicos das novas ferramentas tecnológicas disponíveis atualmente são fundamentais para que o Direito consiga contribuir com as soluções adequadas que a sociedade espera. É preciso evitar que os operadores do Direito não apenas venham a chancelar narrativas de determinadas áreas ou sujeitos e possam, ao contrário, permitir maior diversidade de perspectivas que atendam aos anseios plurais de uma democracia. Como a aplicação da legislação e da jurisprudência depende do intéprete e a hermenêutica exerce grande influência no Direito, talvez seja válida a analogia em relação à revisão humana de decisões automatizadas, enquanto proposta apta para mitigar eventuais vieses em sistemas de inteligência artificial. Entretanto, ainda não há consenso científico a respeito da capacidade dessa medida de resolver os problemas gerados pela discriminação algorítmica.

Conforme demonstrado ao longo deste artigo, os algoritmos em sistemas de *big data* são treinados e alimentados por um conjunto gigantesco de dados, estando muito além do que o ser humano conseguiria lidar de modo solitário. Porém, caso esses dados sejam tendenciosos ou intencionalmente distorcidos os algoritmos acabarão por se

tornar parciais em sua operação. Apesar de processarem uma grande quantidade de informações com muita velocidade, esses sistemas eletrônicos não são infalíveis nem se encontram livres da influência humana.

Não se trata aqui de negar que a inteligência artificial já trouxe grandes benefícios para a sociedade. Existe a crença inclusive de que seu uso torne o mundo mais justo e igualitário, conforme demonstrado ao longo do texto. A regulação jurídica tampouco deve travar o avanço científico ou dificultar a inovação. Seu propósito é apenas garantir que os direitos fundamentais não sejam colocados em segundo plano em favor de determinada agenda econômica. A dificuldade reside na velocidade das mudanças tecnológicas em curso, o que requer trabalho e atenção constante por parte do poder público. Promover critérios de transparência pode ajudar no controle democrático da tecnologia, conforme visto. Mas somente será possível obter a abordagem multissetorial, multidisciplinar e conjunta que esta questão requer mediante a dedicação de especialistas em diversas áreas, como direito, ciência da computação e ética, além de instituições como órgãos públicos, academia, sociedade civil e empresas privadas.

Os conceitos abordados no texto mostram interseção cada vez maior entre as áreas do direito e da ciência da computação. Neste sentido, a pesquisa realizou breve exposição a respeito dos principais tipos de vieses que mecanismos de inteligência artificial podem apresentar. Na falta de solução mais adequada para este problema, a pergunta deste trabalho abrange a revisão humana das operações algorítmicas como um meio de correção dos eventuais resultados enviesados que forem entregues por sistemas automatizados. Ao deixar de prever a revisão humana expressamente, a legislação brasileira é percebida aqui como insuficiente para lidar com esta situação. Acredita-se que a regulação deveria ser capaz de fomentar o desenvolvimento tecnológico com atenção aos direitos fundamentais e conquistas sociais. Este pode ser o cenário mais favorável para que a tecnologia de fato consiga contribuir com a melhoria das condições de vida ao longo deste século.

É inevitável que uma pesquisa realizada sobre algoritmos de inteligência artificial já esteja desatualizada no momento de sua publicação, em decorrência do desenvolvimento bastante rápido que essas ferramentas apresentam atualmente. Entretanto, é de se esperar que os desafios abordados ao longo deste trabalho continuem existindo por mais algum tempo. O principal propósito do texto permanece como um convite ao debate sobre alguns dos efeitos indesejáveis que o desenvolvimento tecnológico pode trazer aos indivíduos, para que em seguida seja possível encontrar soluções eficazes. No Brasil, em especial, a História demonstra que as profundas desigualdades sociais não desaparecerão sem que exista engajamento e resistência por parte da sociedade.

Este artigo se encerra como uma reflexão a respeito das alterações relevantes que os algoritmos e suas aplicações tem causado nas relações sociais, políticas e econômicas contemporâneas, para as quais se acredita que a sociedade brasileira estaria melhor amparada se houvesse uma política pública especialmente elaborada para lidar com este tema. Essa poderia ser uma resposta efetiva para conciliar eventual conflito de direitos fundamentais envolvidos nessa questão, como liberdade econômica

e igualdade. O desafio principal da regulação jurídica aqui é encontrar a melhor maneira de proteger a inovação e os direitos humanos, não só no Brasil como no restante do mundo

Referências

ABE, Jair Minoro; SCALZITTI, Alexandre; SILVA FILHO, João Inácio. *Introdução à lógica para a ciência da computação*. São Paulo: Arte e Ciência, 2002.

ARANHA, Maria Lúcia de Arruda; MARTINS, Maria Helena Pires. *Filosofando :* Introdução à Filosofia. São Paulo : Moderna, 1986.

BATES, Madeleine. *Models of natural language understanding*. Proceedings of the National Academy of Sciences, v. 92, n. 22, 1995. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC40721/pdf/pnas01500-0075.pdf Acesso em 21 de novembro de 2022.

BARROSO, Luís Roberto. *Diferentes, mas iguais: o reconhecimento jurídico das relações homoafetivas no Brasil*. Revista Brasileira de Direito Constitucional, v. 17, p. 105-138, 2011. Disponível em: http://www.luisrobertobarroso.com.br/wp-content/uploads/2017/09/diferentes_mas_iguais_atualizacao_2011.pdf. Acesso em 21 de novembro de 2022.

BITTAR, Eduardo Carlos Bianca. *Curso de ética jurídica: ética geral e profissional*. 13ª ed. São Paulo: Saraiva, 2016.

BRASIL. Constituição da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 de novembro de 2022.

_____. Lei nº 9.609 , de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em 21 de novembro de 2022.

_____. Lei n.º 9.610, de 16 de fevereiro de 1996. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em 30 de outubro de 2020.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 21 de novembro de 2022.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 21 de novembro de 2022.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 21 de novembro de 2022.

_____. Lei nº 13.874, de 20 de setembro de 2019. Institui a Declaração de Direitos de Liberdade Econômica; estabelece garantias de livre mercado; altera as Leis nos 10.406, de 10 de janeiro de 2002 (Código Civil), 6.404, de 15 de dezembro de 1976, 11.598, de 3 de dezembro de 2007, 12.682, de 9 de julho de 2012, 6.015, de 31 de dezembro de 1973, 10.522, de 19 de julho de 2002, 8.934, de 18 de novembro 1994, o Decreto-Lei nº 9.760, de 5 de setembro de 1946 e a Consolidação das Leis do Trabalho,

aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943; revoga a Lei Delegada nº 4, de 26 de setembro de 1962, a Lei nº 11.887, de 24 de dezembro de 2008, e dispositivos do Decreto-Lei nº 73, de 21 de novembro de 1966; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm. Acesso em 21 de novembro de 2022.

_____. Provimento nº 71 da Corregedoria Nacional de Justiça, de 13 de junho de 2018. Disponível em: https://atos.cnj.jus.br/atos/detalhar/2608. Acesso em 21 de novembro de 2022.

_____. Projeto de Lei nº 4496, de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), para definir a expressão "decisão automatizada". Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/138136. Acesso em 21 de novembro de 2022.

_____. Resolução nº 332/2020 do Conselho Nacional de Justiça. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3429. Acesso em 21 de novembro de 2022.

BROUSSARD, Meredith. *Artificial unintelligence: how computers misunderstand the world*. Cambridge: MIT Press, 2018.

BRUCE, Andrew; BRUCE, Peter. *Practical Statistics for Data Scientists*. Sebastopol: O'Reilly, 2017.

BRUCH, Kelly Lissandra; HOFF, Debora Nayar; DEWES, Homero. *A função social do direito de propriedade industrial como alternativa de governabilidade aos países em desenvolvimento: um estudo sobre a propriedade industrial de plantas*. Direito, Estado e Sociedade, v. 32, 2008. Disponível em:

https://www.researchgate.net/publication/236897426_Funcao_social_do_direito_de_propriedade_industrial_como_alternativa_de_governabilidade_aos_paises_em_desenvolvimento_um_estudo_sobre_a_propriedade_industrial_de_plantas. Acesso em 21 de novembro de 2022.

CARRUTHERS, Caroline, JACKSON, Peter.; *The Chief Data Officer's Playbook*. EBSCO Publishing : eBook Collection, 2018.

CARVALHO FILHO, José dos Santos. *Manual de Direito Administrativo*. 30ª ed. São Paulo: Atlas, 2016.

CARVALHO, Patrícia Heloisa de. *O Marco Civil da Internet:* Uma análise sobre a constitucionalidade do artigo 19. Revista da Faculdade de Direito do Sul de Minas. Pouso Alegre, 2017, v. 33, p. 228-244. Disponível m: https://www.fdsm.edu.br/adm/artigos/6917c36392274c9b6393c7f7a7bddbd1.pdf. Acesso em 21 de novembro de 2022.

COPELAND, B. Jack, *The Modern History of Computing*. The Stanford Encyclopedia of Philosophy (Winter 2017 Edition), Edward N. Zalta (ed.). Disponível em: https://plato.stanford.edu/entries/computing-history/. Acesso em 21 de novembro de 2022.

DATTA, A., TSCHANTZ, M. C., *Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination*. In Proceedings on Privacy Enhancing Technologies (PoPETs). 2015. https://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf. Acesso em 21 de novembro de 2022.

DIMOULIS, Dimitri; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais* – 5. ed. rev., atual. e ampl. – São Paulo: Atlas, 2014.

DOMINGUES, Paulo Sérgio. *Legislativo 4.0: o desafio da criação de novas leis para um mundo em mutação*. In: Cadernos Adenauer XXI, nº1. A quarta revolução industrial: inovações, desafios e oportunidades. Rio de Janeiro: Fundação Konrad Adenauer, 2020. Disponível em: https://www.kas.de/pt/web/brasilien/einzeltitel/-/content/cadernos-adenauer-1-2020-1. Acesso em 21 de novembro de 2022.

DUTRA, Luciano. *Direito Constitucional Essencial*. Rio de Janeiro: Forense. 2ªed. 2016.

EDWARDS, Lilian; VEALE, Michael. *Slave to the Algorithm? Why a Right to Explanation is Probably Not the Remedy You are Looking for*. SSRN Electronic Journal, 2017. Disponível em: https://www.researchgate.net/publication/318003528_Slave_to_the_Algorithm_Why_a_Right_to_Explanationn_is_Probably_Not_the_Remedy_You_are_Looking_for. Acesso em 21 de novembro de 2022.

ELIAS, Norbert. *Os estabelecidos e os outsiders: sociologia das relações de poder a partir de uma pequena comunidade*. Rio de Janeiro: Jorge Zahar, 2000.

FRANÇA, Phillip Gil. *Objetivos Fundamentais da República, Escolhas Públicas e Políticas Públicas*: Caminhos de Concretização dos Benefícios Sociais Constitucionais. Direitos sociais e políticas públicas I. 1ed. Curitiba: Clássica Editora, 2014, v. 25.

HARTZOG , Woodrow; RICHARDS, Neil. *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. Rev. 1687 (2020). Disponível em: https://lawdigitalcommons.bc.edu/bclr/vol61/iss5/3. Acesso em 21 de novembro de 2022.

HASTIE, Trevor; TIBSHIRANI, Robert; FRIEDMAN, J. H. *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. 2ª ed. Nova York: Springer, 2009. Disponível em:

https://link.springer.com/book/10.1007%2F978-0-387-84858-7#authorsandaffiliationsbook. Acesso em 21 de novembro de 2022.

HURWITZ, Judith; KIRSCH, Daniel. *Machine Learning For Dummies*: IBM Limited Edition. Hoboken: John Wiley & Sons Inc., 2018. Disponível em: https://www.ibm.com/downloads/cas/GB8ZMQZ3. Acesso em 21 de novembro de 2022.

LAWRENCE, B. Solum. *Legal Personhood for Artificial Intelligences*. North Carolina Law Review, v. 70, n. 4, 1992. p. 1236. Disponível em: https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=3447&context=nclr. Acesso em 21 de novembro de 2022.

MACHADO, Anderson Fraiha; MENDES, Leilani Dian; GARCEZ, Lucas Nogueira. *Introdução à Arquitetura e Engenharia Jurídica com Lawtex*. São Paulo: Looplex, 2018.

MACHADO, Eduarda Sordi Pinheiro. *Inteligência artificial e direitos autorais:* a proteção de obras criadas por computadores inteligentes. Trabalho de conclusão de curso de graduação. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019.

MANKIW, Nicholas Gregory. *Principles of Economics*. 5ª ed. South-Western Cengage Learning, 2007.

MATTHEWS, P. H. *Linguistics:* a very short introduction. Oxford: Oxford University Press, 2003.

MCCORDUCK, Pamela. *Machines who think: a personal inquiry into the history and prospects of artificial intelligence*. AK Peters Ltd : Natick, 2004

MOLNAR, Adam. *Technology, law, and the formation of (il)liberal democracy?*, Surveillance and society, vol. 15, no. 3/4, 2017, pp. 318-388. Disponível em

https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6645. Acesso em 21 de novembro de 2022.

NOBLE, Safiya Umoja. *Algorithms of oppression: how search engines reinforce racism*. New York: New York University Press, 2018.

OBERMEYER, Ziad; POWERS, Brian; VOGELI, Christine; MULLAINATHAN, Sendhil. *Dissecting racial bias in an algorithm used to manage the health of populations*. Science nº 366, 2019. pp. 447-453. Disponível em: https://www.ehidc.org/sites/default/files/resources/files/Dissecting%20racial%20bias%20in%20an%20algorithm%20used%20to%20manage%20the%20health%20of%20populations.pdf. Acesso em 22 de outubro de 2020.

O'NEIL, Cathy. *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York: Crown Publishers, 2016.

PEARL, Judea. *Causality: Models, Reasoning, and Inference*. Cambridge: Cambridge University Press, 2000. Disponível em: http://bayes.cs.ucla.edu/BOOK-99/book-toc.html. Acesso em 21 de novembro de 2022.

PRESTES, Edson. *Teoria dos grafos*. Porto Alegre: 2011, vol. 4, 2016. Disponível em: http://www.inf.ufrgs.br/~prestes/Courses/Graph%20Theory/Livro/ParteLivroGrafos.pdf. Acesso em 21 de novembro de 2022.

SOLOVE, Daniel J., The Myth of the Privacy Paradox. George Washington Law Review, Vol. 89, 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265. Acesso em 21 de novembro de 2022.

SHANNON, Claude Elwood. *A symbolic analysis of relay and switching circuits*. In Transactions of the American Institute of Electrical Engineers, vol. 57, no. 12, pp. 713-723, Dec. 1938. Disponível em: https://www.cs.virginia.edu/~evans/greatworks/shannon38.pdf. Acesso em 21 de novembro de 2022.

SILVA, Tarcízio. *Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código*. In: Anais do IV Simpósio Internacional LAVITS – Assimetrias e (In)visibilidades: Vigilância, Gênero e Raça. Salvador, Bahia, Brasil, 2019. Disponível em: https://www.researchgate.net/publication/333700308_Racismo_Algoritmico_em_Plataformas_Digitais_microagressoes_e_discriminacao_em_codigo. Acesso em 21 de novembro de 2022.

SOUZA, Carlos Affonso Pereira de; SILVA JUNIOR, Ronaldo Lemos da. *Marco Civil da Internet:* construção e aplicação. 1. ed. Juiz de Fora: Editar, 2016. v. 1. p. 25. Disponível em: < https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf>. Acesso em 21 de novembro de 2022.

STANKOVIĆ; Radomir S.; ASTOLA, Jaakko. *Reprints from the Early Days of Information Sciences: TICSP Series On the Contributions of Akira Nakashima to Switching Theory*. Tampere: Tampere International Center for Signal Processing, 2008. Disponível em: http://ticsp.cs.tut.fi/reports/reprint-nakashima-rr.pdf. Acesso em 21 de novembro de 2022.

STEFFENS, Luana. *A influência dos vieses cognitivos na tomada de decisão pela inteligência artificial: um estudo baseado nas evidências no caso norte-americano COMPAS*. In: Fabio da Silva Veiga; Denise Pires Fincato. (Org.). Estudos de Direito, Desenvolvimento e novas Tecnologias. 1ed. Porto Alegre: Instituto Iberoamericano de Estudos Jurídicos, 2020, v. 1, p. 1- 419.

SURDEN, Harry. *Machine Learning and Law*. Washington Law Review, v. 89, 2014. p. 89. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol89/iss1/5/. Acesso em 21 de novembro de 2022.

SWEENEY, L. *Discrimination in Online Ad Delivery*. Harvard University. January 28, 2013 http://ssrn.com/abstract=2208240. Acesso em 21 de novembro de 2022.

THE WHITE HOUSE. *Big Data: A Report on Algorithmic Systems,. Opportunity, and Civil Rights*. Executive Office of the President, 2016. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf. Acesso em 21 de novembro de 2022.

_____. *Preparing for the Future of Artificial Intelligence*. Executive Office of the President, 2016. pp. 17. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf. Acesso em 21 de novembro de 2022.

TURING, Allan M. *Computing Machinery and Intelligence*. Mind, v. 59, n. 236, 1950. Disponível em: https://academic.oup.com/mind/article-abstract/LIX/236/433/986238. Acesso em 21 de novembro de 2022.

UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e40-1-1. Acesso em 21 de novembro de 2022.

WANG, Yilun.; KOSINSKI, Michal. *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*. Journal of Personality and Social Psychology. American Psychological Association, 2017. Disponível em: <https://osf.io/zn79k/>. Acesso em 21 de novembro de 2022.

WILSON, Benjamin; HOFFMAN, Judy; MORGENSTERN, Jamie. *Predictive Inequity in Object Detection*. arXiv preprint arXiv:1902.11097, 2019. Disponível em: https://arxiv.org/pdf/1902.11097.pdf. Acesso em 21 de novembro de 2022.

WORLD INTELLECTUAL PROPERTY ORGANIZATION. *WIPO Technology Trends 2019:*Artificial Intelligence. Geneva, 2019.

YE, Guixin; TANG, Zhanyong; FANG, Dingyi; ZHU, Zhanxing; FENG, Yansong; XU, Pengfei; CHEN, Xiaojiang; WANG, Zheng. *Yet Another Text Captcha* Solver: A Generative Adversarial Network Based Approach. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18). New York: Association for Computing Machinery, 2018. p. 332–348. Disponível em: https://dl.acm.org/doi/10.1145/3243734.3243754. Acesso em 21 de novembro de 2022.

Outras fontes:

ACCESS NOW. *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems*. Disponível em: https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf. Acesso em 21 de novembro de 2022.

AGÊNCIA BRASIL. *Agência Brasil explica: o que é a tecnologia 5G*. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-03/agencia-brasil-explica-o-que-e-tecnologia-5g. Acesso em 21 de novembro de 2022.

BRAUNER, Daniela F. (via portal Medium). *A semântica de dados é um futuro possível para o aprendizado de máquina?* Disponível em: https://medium.com/@danibrauner/a-sem%C3%A2ntica-de-dados-%C3%A9-um-

futuro-poss%C3%ADvel-para-o-aprendizado-de-m%C3%A1quina-9344661b5db7. Acesso em 21 de novembro de 2022.

CARLONI, Giovanna; BIONI, Bruno Ricardo; SOUZA, Carlos Affonso. *Vigilância digital contra o Covid-19: um mal necessário?* Videoconferência disponível em: https://youtu.be/oBjQAfaf-xc. Acesso em 21 de novembro de 2022.

CGS. *CGS Survey Reveals 'Sustainability' Is Driving Demand and Customer Loyalty*. Disponível em: https://www.cgsinc.com/en/infographics/CGS-Survey-Reveals-Sustainability-Is-Driving-Demand-and-Customer-Loyalty. Acesso em 21 de novembro de 2022.

COMPUTER WEEKLY. *IT chiefs recognise the risks of artificial intelligence bias*. Disponível em: https://www.computerweekly.com/news/252474408/IT-chiefs-recognise-the-risks-of-artificial-intelligence-bias. Acesso em 21 de novembro de 2022.

CONJUR. *As lacunas da Lei Geral de Proteção de Dados em casos como o do FaceApp*. Disponível em: https://www.conjur.com.br/2019-jul-24/renan-lopergolo-lacunas-lgpd-casos-faceapp. Acesso em 21 de novembro de 2022.

DOTEVERYONE. *Workers' View*. https://www.doteveryone.org.uk/report/workersview/. Acesso em 21 de novembro de 2022.

EL PAÍS. *Na verdade, o que [...] é exatamente um algoritmo?* Disponível em: https://brasil.elpais.com/brasil/2018/03/30/tecnologia/1522424604_741609.html. Acesso em 21 de novembro de 2022.

ENTREPRENEUR. *How Startups Develop and Deploy Matching Algorithms.* Disponível em: https://www.entrepreneur.com/article/338442. Acesso em 21 de novembro de 2022.

FOREIGN AFFAIRS. *The Lawless Realm: Countering the Real Cyberthreat*. Disponível em: https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm. Acesso em 21 de novembro de 2022.

HARVARD BUSINESS REVIEW. *Want Less-Biased Decisions? Use Algorithms*. Disponível em: https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms. Acesso em 21 de novembro de 2022.

INSTITUTO HUMANITAS. *"O big data apresenta uma multimetodologia". Entrevista com Walter Sosa Escudero*. Disponível em: http://www.ihu.unisinos.br/78-noticias/593456-o-big-data-apresenta-uma-multimetodologia-entrevista-com-walter-sosa-escudero. Acesso em 21 de novembro de 2022.

MIC. *Crime-prediction tool PredPol amplifies racially biased policing, study shows*. Disponível em: https://www.mic.com/articles/156286/crime-prediction-tool-pred-pol-only-amplifies-racially-biased-policing-study-shows. Acesso em 21 de novembro de 2022.

NEXO. *O que está em jogo quando você dá seu CPF na hora da compra*. Disponível em: https://www.nexojornal.com.br/expresso/2020/02/15/O-que-est%C3%A1-em-jogo-quando-voc%C3%AA-d%C3%A1-seu-CPF-na-hora-da-compra?utm_medium=Social&utm_campaign=Echobox&utm_source=Twitter#Echobox=1582314608. Acesso em 21 de novembro de 2022.

_____. *A parcialidade dos algoritmos*. Disponível em: https://www.nexojornal.com.br/externo/2019/11/24/A-parcialidade-dos-algoritmos. Acesso em 21 de novembro de 2022.

PHENOMENAL WORLD. *The Long History of Algorithmic Fairness*. Disponível em: https://phenomenalworld.org/analysis/long-history-algorithmic-fairness. Acesso em 21 de novembro de 2022.

PR NEWSWIRE. *New Workplace Survey Finds Nearly 80% of Employers Aren't Worried About Unethical Use of AI -- But Maybe They Should Be*. Disponível em: https://www.prnewswire.com/news-releases/new-workplace-survey-finds-nearly-80-of-employers-arent-worried-about-unethical-use-of-ai--but-maybe-they-should-be-300911214.html. Acesso em 21 de novembro de 2022.

PROPUBLICA. *Machine Bias - There's software used across the country to predict future criminals. And it's biased against blacks.* Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em 21 de novembro de 2022.

QUARTZ. *Millions of Facebook users have no idea they're using the internet*. Disponível em: https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/. Acesso em 21 de novembro de 2022.

REINO UNIDO. *Windrush Lessons Learned Review*. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876336/6.5577_HO_Windrush_Lessons_Learned_Review_LoResFinal.pdf. Acesso em21 de novembro de 2022.

REUTERS. *U.N. investigators cite Facebook role in Myanmar crisis.* Disponível em: https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1GO2PN. Acesso em 21 de novembro de 2022.

Site oficial do Instituto Charles Babbage. Disponível em: http://www.cbi.umn.edu/about/babbage.html. Acesso em 21 de novembro de 2022.

Site oficial do projeto Algorithmic Justice League. Disponível em: https://www.ajlunited.org/. Acesso em 21 de novembro de 2022.

Site oficial do projeto Coronamap. Disponível em: https://coronamap.site/. Acesso em 21 de novembro de 2022.

Site oficial do projeto GPT-3. Disponível em: https://openai.com/blog/openai-api/. Acesso em 21 de novembro de 2022.

Site oficial do projeto Iamus. Detalhes disponíveis em: http://www.geb.uma.es/melomics/melomics.html. Acesso em 21 de novembro de 2022.

THE ATLANTIC. *The Curious Connection Between Apps for Gay Men and Sex Offenders*. Disponível em: https://www.theatlantic.com/technology/archive/2011/04/the-curious-connection-between-apps-for-gay-men-and-sex-offenders/237340; Acesso em 21 de novembro de 2022.

THE GUARDIAN. *Home Office to scrap 'racist algorithm' for UK visa applicants*. Disponível em: https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants. Acesso em 21 de novembro de 2022.

_____. *I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets*. Disponível em: https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold. Acesso em 21 de novembro de 2022.

_____. *US senator: Huawei 5G is like Soviets building west's submarines*. Disponível em: https://www.theguardian.com/technology/2020/jun/02/us-senator-huawei-5g-is-like-soviets-building-wests-submarines. Acesso em 21 de novembro de 2022.

THE NEW YORKER. *What Can America Learn from Europe About Regulating Big Tech?* Disponível em: https://www.newyorker.com/tech/annals-of-technology/what-can-america-learn-from-europe-about-regulating-big-

tech?utm_source=twitter&utm_medium=social&utm_campaign=onsite-share&utm_brand=the-new-yorker&utm_social-type=earned. Acesso em 21 de novembro de 2022.

THE NEW YORK TIMES. *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em 21 de novembro de 2022.

THE VERGE. *Google and Microsoft warn investors that bad AI could harm their brand*. Disponível em: https://www.theverge.com/2019/2/11/18220050/google-microsoft-ai-brand-damage-investors-10-k-filing. Acesso em 21 de novembro de 2022.

UNIÃO EUROPEIA. *Ethics guidelines for trustworthy AI*. Disponível em: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Acesso em 21 de novembro de 2022.

UNIVERSIDADE DE HARVARD. Berkman Klein Center for Internet & Society. *Ethics and Governance of AI*. Disponível em: https://cyber.harvard.edu/topics/ethics-and-governance-ai. Acesso em 21 de novembro de 2022.

De Regresso à Borda D'Água: O Propósito dos Limites Entre os Dados Pessoais e os Dados Não Pessoais nos Regulamentos da União Europeia[171]

Manuel David Masseno[172]

RESUMO

O Direito da União Europeia sobre proteção de dados não se aplica aos dados não pessoais. Porém, os limites legais entre dados pessoais e dados não pessoais são instáveis, assentando no desenvolvimento de tecnologias de anonimização e de personalização potenciadas pela Inteligência Artificial, com riscos crescentes para os responsáveis pelo tratamento e os subcontratantes. Este texto pretende identificar os riscos mencionados e as respostas possíveis, de acordo com o Regulamento Geral de Proteção de Dados da União Europeia, tendo também em consideração os Regulamentos que se lhe seguiram.

PALAVRAS-CHAVE:

Anonimização, Certificação, Dados não pessoais, Dados pessoais, Risco, União Europeia.

---

[171] Em atenção ao curtíssimo prazo de resposta ao pedido de um contributo para esta Obra, optei por disponibilizar uma nova versão em Língua Portuguesa da Comunicação, exposta como "On the Waterfront: 'Personal' and 'Non-Personal' Data at Both EU Regulations", na *Nordic Conference on Legal Informatics 2019 - Digital Rights, Digital Lawyers, Digital Courts*, realizada na *Lapin yliopisto* (Universidade da Lapónia, Finlândia) dia 14 de novembro de 2019, a qual fora publicada, em Portugal, na revista *Cyberlaw by CIJIC* (ISSN 2183-7295) n.º 9, 2020, pp. 25-43, como "Na borda: dados pessoais e não pessoais nos dois Regulamentos da União Europeia", também com referências bibliográficas em espanhol, italiano e, sobretudo, em português. Consequentemente, limitei-me a acrescentar algumas considerações muito breves a propósito das implicações específicas da *Nova Geração* de Regulamentos, bem como os contributos doutrinários entretanto publicados em acesso aberto, mantendo a orientação assumida na versão original, mas limitadamente a Autores nacionais, por força das referidas limitações temporais.

[172] Professor Adjunto do IPBeja - Instituto Politécnico de Beja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, sendo ainda o seu Encarregado da Proteção de Dados.

De Regresso à Borda D'Água: O Propósito dos Limites Entre os Dados Pessoais e os Dados Não Pessoais nos Regulamentos da União Europeia[173]

Manuel David Masseno

ABSTRACT

European Union Law on data protection does not apply to non-personal data. However, the legal limits between personal and non-personal data are unstable, relying on the development of anonymization and personalization Artificial Intelligence enhanced technologies, with increasing risks to be handled by controllers and processors. This paper intends to identify the mentioned risks and the possible remedies, according to the General Data Protection Regulation of the European Union, also taking into consideration the Regulations that followed it.

KEYWORDS:

Anonymization; Certification; Non-personal data; Personal data; Risk

[173] Em atenção ao curtíssimo prazo de resposta ao pedido de um contributo para esta Obra, optei por disponibilizar uma nova versão em Língua Portuguesa da Comunicação, exposta como "On the Waterfront: 'Personal' and 'Non-Personal' Data at Both EU Regulations", na *Nordic Conference on Legal Informatics 2019 - Digital Rights, Digital Lawyers, Digital Courts*, realizada na *Lapin yliopisto* (Universidade da Lapónia, Finlândia) dia 14 de novembro de 2019, a qual fora publicada, em Portugal, na revista *Cyberlaw by CIJIC* (ISSN 2183-7295) n.º 9, 2020, pp. 25-43, como "Na borda: dados pessoais e não pessoais nos dois Regulamentos da União Europeia", também com referências bibliográficas em espanhol, italiano e, sobretudo, em português. Consequentemente, limitei-me a acrescentar algumas considerações muito breves a propósito das implicações específicas da *Nova Geração* de Regulamentos, bem como os contributos doutrinários entretanto publicados em acesso aberto, mantendo a orientação assumida na versão original, mas limitadamente a Autores nacionais, por força das referidas limitações temporais.

> "Assistimos a uma nova revolução industrial induzida pelos dados digitais, a informática e a automatização. As atividades humanas, os processos industriais e a investigação conduzem, todos eles, à recolha e ao tratamento de dados numa escala sem precedentes, favorecendo o surgimento de novos produtos e serviços, assim como de novos processos empresariais e metodologias científicas [e] Desde que as regras relativas à proteção dos dados pessoais, quando aplicáveis, sejam cumpridas, os dados, uma vez registados, podem ser reutilizados muitas vezes sem perda de fidelidade. Esta geração de valor agregado está no cerne do conceito de cadeia de valor dos dados. [tendo sempre presente que] O direito fundamental à proteção dos dados pessoais aplica-se aos grandes volumes de dados no caso de se tratar de dados pessoais: o seu tratamento tem de respeitar todas as regras aplicáveis em matéria de proteção de dados."[174]

1 – As referências

Antes de mais, é necessário ter presente que, uma vez operada a constitucionalização da Proteção de Dados operada em 2009 com a entrada em vigor do Tratado de Lisboa, com a inclusão da mesma no Tratado sobre o Funcionamento da União Europeia (Art.º 16.º) e com a receção da Carta dos Direitos Fundamentais (Art.º 8.º) no Direito Primário da União (Ex vi, Art.º 6.º do Tratado da União Europeia), o respetivo microssistema ficou consolidado, ainda que não completo, com a adoção do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho 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 que revoga a Diretiva 95/46/C (Regulamento Geral sobre a Proteção de Dados) – o RGPD[175].

Ao mesmo tempo e enquanto ainda decorria o processo legislativo correspondente ao RGPD, a Comissão [presidida por Jean-Claude] Juncker avançou com a "Estratégia para o Mercado Único Digital na Europa" (COM/2015/192 final, de 6 de maio), dando continuidade a orientações que vinham da Comissão [presidida por José Manuel Durão] Barroso e constavam da Comunicação "Para uma economia dos dados próspera", de 2014, referida em proémio[176].

---

[174] Comunicação da Comissão "Para uma economia dos dados próspera" (COM/2014/0442 final, de 2 de julho).

[175] Os estudo sobre o RGPD são hoje multidão. Mas, sempre podemos referir os estudos de Angelina TEIXEIRA (2016), de Alfonso ORTEGA JIMÉNEZ e Juan José Gonzalo DOMENECH (2018) e ainda de Chris HOOFNAGLE, Bart van der SLOOT e Fredrik ZUIDERVEEN BORGESIUS (2019).

[176] Aliás, na sua "Estratégia para o Mercado Único Digital na Europa" a Comissão acentua que "As empresas e os consumidores continuam a não se sentirem suficientemente confiantes para adotar serviços de computação em nuvem transfronteiras para fins de armazenamento ou processamento de dados, devido a preocupações relacionadas com a segurança, o respeito dos direitos fundamentais e a proteção de dados em termos mais gerais. A adoção do Pacote Reforma da Proteção de Dados assegurará que o tratamento de dados pessoais seja regido por regras atualizadas e uniformes em toda a União. No entanto, frequentemente os contratos excluem, ou limitam de forma significativa, a responsabilidade contratual do prestador de serviços de computação em nuvem caso os dados deixem de estar disponíveis ou fiquem inutilizáveis, ou dificultam a rescisão do contrato. Isso significa que não existe, de facto, uma portabilidade dos dados. No domínio da proteção de dados, tanto o atual

O que foi explicitado através de uma sua nova Comunicação, "Construir uma Economia Europeia dos Dados" (COM/2017/9 final, de 10 de janeiro), agora centrada na necessidade de avançar com disciplinas para os "dados em bruto", com um especial ênfase na sua portabilidade em todo o Mercado Interno da União[177]. Daí que a Comissão tenha avançado com a Proposta (COM/2017/0495 final, de 13 de setembro) do que veio a ser o Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho de 14 de novembro de 2018 relativo a um regime para o livre fluxo de dados não pessoais na União Europeia – o Regulamento LFD[178].

No entanto e entre outras, voltou a ser colocada questão a necessitar de respostas jurídicas tão robustas quanto possível, a de existir uma borda, mutável de acordo com a evolução das tecnologias, entre os âmbitos de aplicação material de ambos os Regulamentos, isto é, entre os dados pessoais e os dados não pessoais. A determinação dessa borda, e um breve esboço do que fazer, constitui o objeto desta intervenção.

2 – até mesmo nos limites

Para começar, temos que o RGPD "aplica-se ao tratamento de dados pessoais" (Art.º 2.º n.º 1), não só a uma "pessoa singular [física] identificada", mas também a uma que

como o futuro quadro legislativo impede as restrições à livre circulação de dados pessoais na União. As restrições à livre circulação de dados por outros motivos não são abordadas. [Pelo que] A Comissão irá propor em 2016 a Iniciativa Europeia «Livre Circulação de Dados» que aborda a questão das restrições à livre circulação de dados por motivos não relacionados com a proteção de dados pessoais na UE e das restrições injustificadas sobre a localização de dados para fins de armazenamento ou de tratamento. A iniciativa abordará as questões emergentes de propriedade, interoperabilidade, usabilidade e acesso aos dados nomeadamente em situações entre empresas, entre empresas e consumidores e dados gerados por máquinas e máquina-a-máquina. Incentivará o acesso aos dados públicos a fim de contribuir para dinamizar a inovação."

177 Sobre estes Documentos e em termos gerais sobre o Mercado Único Digital e por todo, é de atender aos testudos de Fernanda Ferreira DIAS (2016) e de Joana Covelo de ABREU (2017).

178 Para uma perspetiva geral do *Regulamento LFD*, embora tratando essencialmente de outras questões, Pedro DE MIGUEL ASENSIO (2019), assim como o meu texto sobre a apropriabilidade dos dados não pessoais (2021).

venha a ser "identificável", em termos potenciais e através de meios técnicos, incluindo os indiretos[179-180].

Consequentemente, do RGPD resulta que: "[…] Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação." (Considerando 26 in fine)

Por sua vez, o Regulamento LFD veio esclarecer que o mesmo "aplica-se ao tratamento de dados eletrónicos que não sejam dados pessoais" (Art.º 2.º n.º 1), entendendo estes "na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679 [o RGPD]" (Art.º 3.º n.º 1)[181].

Assim, ao Regulamento Geral sobre Proteção de Dados é conferida uma vis atractiva, sempre que não seja possível identificar os dados em presença como, exclusivamente, não pessoais. Pelo que, "No caso de um conjunto de dados compostos por dados pessoais e não pessoais, o presente regulamento aplica-se aos dados não pessoais do conjunto de dados. Caso os dados pessoais e não pessoais de um conjunto

---

[179] Ou seja "[…] 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;" (Art.º 4.º 1). O que incluí os quase-identificadores e os metadados, ao ser certo que, "As pessoas singulares podem ser associadas a identificadores por via eletrónica […] tais como endereços IP (protocolo internet) ou testemunhos de conexão (*cookie*) ou outros identificadores como as etiquetas de identificação por radiofrequência." (*Considerando* 30). Diversamente, a propósito da reindentificação de dados pseudonimizados, o *RGPD* acrescenta que "[…] importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica." (*Considerando* 26).

[180] Neste particular, há ainda que atender ao conteúdo do Parecer 4/2007 sobre o conceito de dados pessoais, de 20 de junho de 2007, do *Grupo de Trabalho do* 29.º [o qual antecedeu o CEPD – Comité Europeu para a Proteção de Dados], assim como à Jurisprudência do Tribunal de Justiça da União Europeia, a qual culminou no Acórdão proferido no Processo C-582/14, *Patrick Breyer*, de 19 de outubro de 2016. Quanto a estas referências, são de atender os estudos, complementares entre si, de Rossana DUCATO (2016), de Nadezhda PURTOVA (2018), de A. Barreto MENEZES CORDEIRO (2018) e ainda de Lorenzo dalla CORTE (2019), inclusive quanto a referências bibliográficas adicionais.

[181] Isto, porque "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, os dados relativos à agricultura de precisão que podem ajudar a controlar e a otimizar a utilização de pesticidas e de água ou ainda dados sobre as necessidades de manutenção de máquinas industriais." (*Considerando* 9).

de dados estejam indissociavelmente ligados, o presente regulamento não prejudica a aplicação do Regulamento (UE) 2016/679" (Art.º 2.º n.º 2 do Regulamento LFD).

3 – mas, afinal, nada é para sempre

No que concerne a distinção que nos ocupa, temos que a Diretiva 95/46/CE, que precedeu o Regulamento sobre Proteção de Dados, assentara numa fictio iuris, ao abstrair-se da evolução da técnica, ainda que previsível. Daí, na mesma constar que "[…] os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável [os quais são, também] conservados sob uma forma que já não permita a identificação da pessoa em causa." (Considerando 26).

O que já não ocorre com o RGPD, ao ser assumido que "As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos [e também que] Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares." (Considerando 30).

Por sua vez, o Regulamento LFD é transparente, ao explicitar que "Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade" (Considerando 9 in fine), o mesmo valendo para os dados originariamente anónimos, por identidade de razão.

Porém, é necessário ter presente que não estamos face a algo verdadeiramente novo. Aliás, as Instituições da União Europeia foram ficando cientes desta realidade, como mostram os Pareceres do Grupo de Trabalho do Art.º 29.º.

Assim e num primeiro momento, tal ocorreu a propósito dos riscos para a proteção dos dados dos administrados que poderiam advir da transposição da Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de Novembro de 2003, relativa à reutilização de informações do sector público, designadamente, o Parecer n.º 7/2003 sobre a reutilização de informações do setor público e a proteção dos dados pessoais, de 12 de dezembro. A que se seguiu o Parecer n.º 6/2013 sobre dados abertos e reutilização de informações do setor público (ISP), de 5 de junho, suscitado pela adoção da Diretiva 2013/37/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público[182]. E ainda o Parecer n.º 5/2018, de 10 de julho, da Autoridade Europeia para a Proteção de Dados, agora tendo por referência a Proposta que levou à Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público (reformulação) (Diretiva Dados Abertos).

Mas, uma análise detalhada desta questões, tanto desde o ponto de vista técnico quanto numa perspetiva jurídica, constituiu o objeto do Parecer n.º 5/2014 sobre técnicas de anonimização, de 10 de abril[183].

---

[182] Sobre esta tensão entre as políticas de dados abertos e a proteção de dados, criticamente, temos também o artigo de Katleen JANSSEN e Sara HUGELIER (2013).

[183] No qual é afirmado, precisamente, que "A anonimização de dados pessoais pode ser uma boa estratégia para manter os benefícios e atenuar os riscos. Quando um

Por isso mesmo, algumas autoridades nacionais avançaram com orientações destinadas a mostrar padrões aos respetivos responsáveis pelo tratamento de dados, como no Reino Unido com a ICO - Information Commissioner's Office, que aprovou o Anonymisation: managing data protection risk code of practice, em novembro de 2012, ou com a Agencia Española de Protección de Datos, com as suas Orientaciones y garantías en los procedimientos de anonimización de datos personales, de outubro de 2016.

Entretanto e a propósito da entrada em vigor do Regulamento LFD, a Comissão Europeia publicou as suas Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia (COM/2019/250 final, de 29 de maio), com referências específicas e desenvolvidas quanto a esta questão184, concluindo que "[…] se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais. [e, do mesmo modo] Aplicam-se as mesmas regras [as relativas ao tratamento de dados pessoais] quando a evolução da tecnologia e da análise de dados torna possível a conversão de dados anonimizados em dados pessoais."

Acrescente-se que preocupações idênticas, em especial motivadas pela disponibilização de informações do Setor Público destinadas à sua reutilização por privados num contexto tecnológico de acesso generalizado às analíticas de Big Data,

---

conjunto de dados se encontra verdadeiramente anonimizado e as pessoas deixam de ser identificáveis, a legislação europeia de proteção de dados deixa de ser aplicável.

No entanto, estudos de casos e publicações de investigação evidenciam que criar um conjunto de dados verdadeiramente anónimo a partir de um conjunto substancial de dados pessoais mantendo, simultaneamente, as informações subjacentes exigidas para a tarefa não é um desafio simples. Por exemplo, um conjunto de dados considerado anónimo pode ser combinado com outro conjunto de dados de modo a que uma ou mais pessoas sejam passíveis de ser identificadas."

184 "Todos os dados que não sejam «dados pessoais», na aceção do Regulamento Geral sobre a Proteção de Dados, são dados não pessoais. Os dados não pessoais podem ser classificados segundo a origem:

· Desde o início - dados originalmente não relacionados com uma pessoa singular identificada ou identificável, tais como dados sobre as condições meteorológicas gerados por sensores instalados em turbinas eólicas ou dados sobre as necessidades de manutenção de máquinas industriais.

· Em segunda fase - dados inicialmente pessoais, mas posteriormente anonimizados. A «anonimização» de dados pessoais é diferente da pseudonimização (ver supra), uma vez que os dados devidamente anonimizados não podem ser atribuídos a uma determinada pessoa, nem sequer pela utilização de dados adicionais, pelo que se tratam de dados não pessoais.

Aferir da correta anonimização dos dados depende de circunstâncias específicas e únicas de cada caso. Os vários exemplos detetados de reidentificação de conjuntos de dados supostamente anonimizados demonstraram que essa avaliação pode ser exigente. Para determinar se uma pessoa é identificável, é necessário ter em conta todos os meios suscetíveis de serem razoavelmente utilizados por um responsável pelo tratamento ou qualquer outra pessoa para identificar uma pessoa direta ou indiretamente.

No entanto, se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais."

enformaram o Anexo II do Relatório de 24 de novembro de 2016 (A/HRC/31/64) do Relator Especial para a Privacidade do Conselho dos Direitos Humanos das Nações Unidas, Joseph A. Cannataci, logo no seu primeiro Relatório.

Adicionalmente e como resulta também dos Documentos antes referidos, diversos estudos académicos foram mostrando as dificuldades de manter distinções claras, consistentes e, mais ainda, irreversíveis entre dados pessoais e dados não pessoais. O que se concretiza na explicitação dos limites das técnicas de anonimização disponíveis em cada momento, assim como nas possibilidades de personalização de dados anónimos ou anonimizados.

A título exemplificativo, logo em 2010 e desde uma perspetiva jurídica, Paul OHM expôs as insuficiências das técnicas então disponíveis. Entretanto, em julho último, seguindo uma metodologia de natureza matemática, Luc ROCHER, Julien M. HENDRICKX e Yves-Alexandre de MONTJOYE demonstraram como a reidentificação de dados anónimos ou anonimizados pode ser alcançada, com níveis muito altos de eficácia e uma relativa facilidade técnica[185-186].

4 – e "que fazer?" ...antes do tratamento de dados, pessoais e não pessoais

Atendendo a este contexto técnico e regulatório, também resultante do Princípio da responsabilidade proativa (Accountability)[187] e por força da aplicação dos Princípios e regras constantes do RGPD, o responsável pelo tratamento deverá promover a realização de análises de risco, previamente à anonimização de dados pessoais ou aos

---

[185] Depois das conclusões de Paul OHM, a questão continuou a sem debatida na Doutrina de ambas margens do Atlântico, procurando uma compatibilização, porventura impossível, entre uma tecnologia crescentemente mais poderosa no sentido de viabilizar a repersonalização de dados anonimizados e as regras pressupondo a correspondente irreversibilidade, sobretudo durante o processo legislativo que culminou na adoção do *Regulamento Geral sobre Proteção de Dados*, ou logo após, como ocorreu com Paul SCHWARTZ e Daniel SOLOVE (2011), Samson Y. ESAYAS (2015) ou ainda com Sophie STALLA-BOURDILLON e Alison KNIGHT (2017), ainda sobre esta questão, têm um especial interesse as reflexões críticas de Augusto Cesar TORBAY (2020) e de Joana Diniz de FIGUEIREDO (2022).

[186] Quanto à utilização de analíticas de *Big Data* para a "definição de perfis" (isto é, uma "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações", Art.º 4.º 4) do *RGPD*) e para a personalização, também a partir de dados anónimos ou anonimizados, são de referir os estudos de Benjamin HABEGGER *et al*. (2014), de Alessandro MANTELERO (2016) e de Elena GIL (2016, *maxime* pp. 86-110) ou, desde uma perspetiva técnica de, Nils GRUSCHKA *et al*. (2018) e ainda o meu trabalho (2019) e com Cristiana Teixeira SANTOS (2019), tal como as reflexões críticas de Lorenzo COTINO HUESO (2017), ainda, as mais recentes e específicas de Luís Manuel PICA (2021) e de Tamára CHELES (2022), além das referências de Ana Sofia CARVALHO e Isabel Restier POÇAS (2020).

[187] Havendo sido objeto do Parecer 3/2010 sobre o princípio da responsabilidade, adotado em 13 de julho de 2010 pelo *Grupo de Trabalho do Art.º 29*, o mesmo ficou explicitado n.º 2 do Art.º 5.º do *RGPD*, em cujos termos, "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 [, isto é, pelo cumprimento dos "Princípios relativos ao tratamento de dados pessoais] e tem de poder comprová-lo", sobre o mesmo, além das considerações de Teresa Vale LOPES (2018) e de Emanuele LUCCHINI GUASTALLA (2018), tem ainda muito interesse o estudo de Lachlan URQUHART, Tom LODGE e Andy CRABTREE (2019).

tratamento de dados não pessoais[188]. O que o afastará de incorrer em qualquer uma das responsabilidades previstas nas tipologias constantes do RGPD em resultado da personalização de dados, mesmo se apenas potencial ou realizada por terceiros[189].

Aliás, embora se nos afigure evidente, deve ficar claro que a anonimização de dados pessoais pressupõe a presença dos inerentes requisitos no que respeita à "Licitude do tratamento" (Art.ºs 6.º a 11.º), assim como a observância dos "Princípios relativos ao tratamento de dados pessoais" (Art.º 5.º). O mesmo valendo para a personalização, ou a repersonalização, de dados anónimos ou anonimizados.

Especificamente, deverão ser seguidos os critérios indicados no RGPD a propósito tanto da "Proteção de dados desde a conceção e por defeito [omissão…]" (Art.º 25), em particular no que se refere à "Segurança do tratamento" (Art.º 32.º), ou seja, "Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas […]."[190].

E ainda, se isso resultar da análise de risco ou for necessário por a mesma ser obrigatória para tratamentos de dados pessoais análogos aos pretendidos (Art.º 35.º n.º 3)[191], deverá também ser efetuada uma "Avaliação de impacto sobre a proteção de dados", com especial ênfase no acompanhamento da evolução das técnicas de personalização ou de repersonalização de dados anónimos ou anonimizados, isto é,

---

[188] Isto, porque "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica." (*Considerando* 26 do *RGPD*). A propósito das análises de risco neste contexto, em termos gerais, são de referir os estudos de Niels van DIJK, Raphaël GELLERT e Kjetil ROMMETVEIT (2016), de Alessandro MANTELERO (2017), assim como as considerações de Teresa Vale LOPES (2018).

[189] Como ocorre com o "direito de indemnização e responsabilidade", objetiva e solidária (Art.º 82.º), com as "coimas" [sanções administrativas], que podem atingir montantes muito elevados (Art.ºs 58.º n.º 1 i) e 83.º), e, sendo o caso, com outras "sanções", designadamente de ordem penal (Art.º 84.º). Para uma melhor compreensão destes preceito e por todos, atente-se no estudo Brendan Van ALSENOY, (2017) e na síntese de Pedro Miguel FREITAS (2018).

[190] Quanto ao conteúdo e ao sentido destas previsões, são sobretudo os estudos encomendados pela ENISA – agora, Agência da União Europeia para a Cibersegurança, antes da adopção do *RGPD*, a George DANESIS *et al*. (2014) e a Giuseppe D'ACQUISTO *et al*. (2015), e, depois, a Marit HANSEN e Konstantinos LIMNIOTIS (2018), sendo ainda de considerar os contributos de Simone CALZOLAIO (2017), de Lee A. BYGRAVE (2017), de Irene KAMARA (2017), este centrado na definição e aplicação de normas técnicas neste domínio, assim como de Teresa Vale LOPES (2018).

[191] Especificamente, "a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º; ou c) Controlo sistemático de zonas acessíveis ao público em grande escala."

"Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares […]." (Art.º 35.º n.º 1)[192].

Por outras palavras, essas Avaliações devem realizar-se periodicamente ou sempre que se verifique a emergência de novas técnicas neste domínio, não apenas para a anonimização mas também para a personalização[193].

Adicionalmente, o enquadramento de tais tratamentos de dados no âmbito de "um procedimento de certificação aprovado nos termos do artigo 42.º" (tal como referido no Art.º 25.º n.º 3 a propósito da "proteção de dados desde a conceção e por defeito" e no Art.º 32.º n.º 2 no que se refere à "segurança do tratamento") poderá assumir uma grande importância para evitar males maiores no que se refere às várias responsabilidades nas quais os responsáveis pelos tratamentos podem incorrer, embora não as afastem, pelo menos por inteiro[194].

Neste mesmo sentido, a aprovação de "critérios de certificação", contendo parâmetros objetivos e detalhados quanto às técnicas de anonimização mais robustas, pelo Comité Europeu para a Proteção de Dados, conduzindo a um "Selo Europeu de Proteção de Dados", reveste-se da maior relevância (Art.ºs 42.º n.º 5 e 70.º n.º 1 p)[195].

Sempre a propósito da certificação das técnicas de anonimização e do tratamento de dados anónimos ou anonimizados, ferramentas complementares poderiam resultar do novel "sistema europeu de certificação da cibersegurança", tal como previsto no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança)[196]. O que teria consequências, pelo menos no que se refere à segurança no tratamento dos

---

[192] A este propósito e em geral, são de assinalar as referências breves de Luís PICA (2018) e as considerações de Teresa Vale LOPES (2018), bem como e sobretudo os estudos de Niels van DIJK, Raphaël GELLERT e Kjetil ROMMETVEIT (2016), de Bruno PEREIRA e João ORVALHO (2019) e, sobretudo, de Eliseu Pinto LOPES (2022).

[193] Para tanto, cumprirá seguir as Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 (Revistas e adotadas pela última vez em 4 de outubro de 2017), do Comité Europeu para a Proteção de Dados.

[194] No que se refere a este regime, atente-se nos estudos de Giovanni Maria RICCIO e Federica PEZZA, (2018) e de Jorge A. VIGURI CORDERO (2018), assim como nos apontamentos de Luís PICA (2018) e de Teresa Vale LOPES (2018).

[195] Aliás, essa mesma preocupação já consta, ainda que como referências muitos sintéticas, das Orientações 1/2018 relativas à certificação e à definição de critérios de certificação de acordo com os artigos 42.º e 43.º do Regulamento (Versão 3.0, de 4 de junho de 2019), adotadas pelo CEPD.

[196] A propósito destas questões, em termos gerais, é de atender aos estudos de Helena CARRAPIÇO e André BARRINHA (2017) e de Alexandre L. Dias Pereira (2018), na expetativa de uma próxima publicação de trabalhos específicos, embora estas questões não sejam novas, como mostra o estudo de Roksana MOORE (2013), por exemplo. Além de continuarem a ser ignoradas pela nossa Doutrina, como ocorreu com Jorge Bacelar GOUVEIA (2021) e com Diogo Lopes ALVES (2021).

dados, sobretudo perante uma "violação de dados pessoais"[197], com implicações quanto à presença e conteúdo do dever de notificação da mesma aos titulares dos dados (Art.º 34.º do RGPD).

Em especial, estaria em causa uma certificação facultando um 'nível de garantia' 'substancial'[198] ou, até mesmo, um 'alto'[199] (Art.º 52), relativamente a ameaças por parte de terceiros, no sentido de afastar no tempo os riscos resultantes da evolução das tecnologias e da redução dos respetivos custos, pelo menos.

5 – e para prevenir responsabilidades, pelo menos em parte

Como acabámos de ver, a minimização dos riscos de incumprimento do *RGPD* resultantes de personalizações futura de dados anónimos ou anonimizados, de forma a manter até aos limites do possível a liberdade de tratamento dos mesmo, incluindo a respetiva negociação, implica acompanhar de perto a evolução do estado da técnica, assim como da ações das autoridades, de proteção de dados ou de cibersegurança, no que se refere às certificações de ferramentas ou de procedimentos. Porém, os riscos de incumprimento estarão sempre presentes, apenas podendo ser contidos.

No entanto, o procedimento mais eficaz para afastar tais riscos, ainda que inviável em muitos casos, pela própria *natureza das coisas*, passaria pela aplicação da disciplina constante do *RGPD* a todos os tratamentos de dados, pessoais e não pessoais, pelo menos quando fossem empregues tecnologias como as inerentes à "internet das coisas, a inteligência artificial e a aprendizagem automática" (*Considerando* 9 do

---

[197] Por "«Violação de dados pessoais», [entende-se] uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;" (Art.º 4.º 12) do *RGPD*). No que se refere a esta matéria, é de atender ao conteúdo do artigo de Stephanie von MALTZAN (2019) e do nosso com Guilherme Magalhães MARTINS e José FALEIROS Júnior (2020), assim como às considerações de Digo Lopes ALVES (2021).

[198] "6. Um certificado europeu de cibersegurança que ateste um nível de garantia «substancial» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos conhecidos para a cibersegurança e do risco de incidentes e ciberataques levados a cabo por autores com competências e recursos limitados. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público e a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias."

[199] "7. Um certificado europeu de cibersegurança que ateste um nível de garantia «elevado» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos de ciberataques sofisticados levados a cabo por autores com competências e recursos significativos. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público, a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias, ao nível tecnológico mais avançado, e uma avaliação da sua resistência a atacantes competentes através de ensaios de penetração. […]"

Regulamento LFD)[200]. Designadamente e pelo menos, com a cifragem de tais massas de dados, de modo a prevenir as consequências e responsabilidades resultantes de eventuais "violações de dados"[201].

6 – entretanto…

Procurando dar resposta aos desenvolvimentos tecnológicos e à crescente concorrência norte-americana e chinesa, mas mantendo firmes os Valores constitucionais subjacentes à Construção Europeia, a Comissão apresentou a sua "Visão e objetivos" na sua Comunicação "Construir o futuro digital da Europa" (COM/2020/67 final, de 19 de fevereiro). Na mesma e designadamente, previa a apresentação de propostas legislativas orientadas à regulação da governação dos dados, pessoais e não pessoais, assim como à clarificação dos regimes de acesso aos próprios dados[202]; em paralelo, propunha-se avançar com propostas relativas à disciplina da concorrência e dos serviços nos mercados digitais, atendendo à necessidade de enquadrar as "plataformas de grande dimensão" (*Gatekeepers*) pelo poder efetivo que as mesmas foram adquirindo em tais mercados.

Até por corresponder a uma continuidade das iniciativas que haviam levado à adoção do *RGPD* e, sobretudo, do Regulamento *RFD* e da *Diretiva Dados Abertos*, a primeira foi logo consubstanciada na Comunicação "Uma estratégia europeia para os dados" (COM/2020/66 final), apresentada em simultâneo, tendo conduzido ao Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (*Regulamento Governação de Dados*)[203], bem como à mais recente Proposta de Regulamento relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (*Regulamento Dados*) (COM/(2022/68 final), de 23 de fevereiro.

Em termos muito sintéticos, o *Regulamento Governação de Dados*, determina que o "acesso para fins de reutilização de dados só deve ser concedido se o organismo do setor público ou o organismo competente, na sequência de um pedido de reutilização, tiver assegurado que os dados: i) foram anonimizados, no caso dos dados

---

[200] Em síntese, trata-se de observar os "Princípios relativos ao tratamento de dados pessoais" - em especial no que se refere à "limitação das finalidades", à "minimização dos dados" e à sua "integridade e confidencialidade" (Art.º 5.º n.º 1 b) e c) e n.º 2), de acatar os requisitos de licitude que couberem (Art.ºs 6.º a 11.º), de respeitar pelos "direitos dos titulares dos dados" (Art.ºs 12.º a 22.º), bem como cumprir as obrigações impostas aos responsáveis pelo tratamento (Art.ºs 24.º a 39.º), em especial formulando e seguindo políticas de privacidade (Art.º 24.º n.º 2), metodicamente. A este propósito, vejam-se as considerações breves de Lurdes Alves DIAS (2018), os artigos de Dag Wiese SCHARTUM (2017) e de Filippo A. RASO (2018), os estudos temáticos realizados por mim e por Cristiana Teixeira SANTOS (2018) e (2019), e ainda as reflexões críticas de Miguel MORENO MÚÑOZ (2017).

[201] No que se refere à utilização desta técnica no âmbito do *RGPD*, é de referir o trabalho de Gerald SPINDLER e Philipp SCHMECHEL (2016), sendo ainda de muito interesse as reflexões contextuais de Samson Y. ESAYAS (2015).

[202] A propósito dos regimes então vigente, permito-me remeter para o meu texto (2021), até pela ausência de outros contributos nacionais.

[203] Aliás, confirmando a prioridade, a respetiva Proposta (COM/2020/767 final) foi apresentada ainda em 2020, a 25 de novembro.

pessoais; […] e, adicionalmente, "Os atos legislativos específicos da União podem estabelecer que determinadas categorias de dados não pessoais detidos por organismos do setor público são consideradas altamente sensíveis para efeitos do presente artigo, caso a sua transferência para países terceiros possa comprometer objetivos de política pública da União, como a segurança e a saúde pública, ou possa acarretar riscos de reidentificação de dados não pessoais anonimizados." ((Art.º 5.º n.º 3 a) e n.º 13)[204]. Aliás, no respetivo Parecer conjunto 3/2021 do CEPD e da AEPD sobre a proposta de Regulamento do Parlamento Europeu e do Conselho relativo à governação de dados (Regulamento Governação de Dados), de 9 de junho de 2021, estas preocupações ficaram em evidência.

Por seu turno, a Proposta de *Regulamento Dados*, limita-se a esclarecer que "Caso seja estritamente necessário incluir dados pessoais nos dados disponibilizados a um organismo do setor público ou a uma instituição, agência ou organismo da União, devem ser respeitadas as regras aplicáveis em matéria de proteção de dados pessoais, devendo a disponibilização dos dados e a sua subsequente utilização ser acompanhadas de garantias relativas aos direitos e interesses das pessoas a quem esses dados dizem respeito. O organismo que solicita os dados deve demonstrar a estrita necessidade e as finalidades específicas e limitadas do tratamento. Antes de disponibilizar os dados, o detentor dos dados deve envidar esforços razoáveis para os anonimizar ou, caso essa anonimização se revele impossível, aplicar meios tecnológicos como a pseudonimização e a agregação" (*Considerando* 64), o que mereceu reservas no Parecer conjunto 2/2022 do CEPD e da AEPD sobre a proposta de Regulamento o relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (Regulamento Dados), de 4 de maio, nomeadamente quanto ao tratamento de dados por um «produto» da Internet das Coisas.

A outra linha conduziu à adoção do Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (*Regulamento dos Mercados Digitais*) – *Regulamento DMA*, e do Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (*Regulamento dos Serviços Digitais*) – *Regulamento DSA*, embora o segundo não tenha uma incidência significativa neste domínio[205], partindo o primeiro do então

[204] Especificamente, o *Considerando* 8 recorda que "Em conformidade com o Regulamento (UE) 2016/679, os princípios da proteção de dados não deverão aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável, nem a dados pessoais tornados de tal modo anónimos que o titular dos dados não possa, ou já não possa ser, identificado. A reidentificação dos titulares dos dados a partir de conjuntos de dados anonimizados deverá ser proibida. Tal proibição deverá aplicar-se sem prejuízo da possibilidade de realizar investigação sobre técnicas de anonimização, em especial para garantir a segurança da informação, melhorar as técnicas de anonimização existentes e contribuir para a robustez geral da anonimização, em conformidade com o Regulamento (UE) 2016/679.".

[205] Embora ainda sobre as duas *Propostas* de Regulamento, são de atender as reflexões breves de Beatriz Macedo VITORINO e de João Pinto RAMOS (2021), assim como de Pedro Madeira FROUFE (2021), de Miguel PEREIRA (2021) e de Nuno Sousa e SILVA (2021), apesar de as mesmas não atenderem às questões em análise específica.

muito recente Regulamento (UE) 2019/1150 do Parlamento Europeu e do Conselho de 20 de junho de 2019, relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha.

Assim, no *Regulamento DMA*, inclusive na sequência das considerações constantes do Parecer 2/2021, da AEPD, de 10 de fevereiro, e da Declaração sobre o Pacote dos Serviços Digitais e a Estratégia para os Dados, do CEPD, de 18 de novembro de 2021, ficaram estabelecidas regras impondo aos *Gatekeepers*[206] anonimização de dados pessoais antes de os facultar a «utilizadores profissionais» (Art.º 7.º n.º 11 e 13.º n.º 5), consequentemente "Ao proporcionar acesso aos seus dados sobre pesquisas, o controlador de acesso deverá assegurar a proteção dos dados pessoais dos utilizadores finais, nomeadamente contra eventuais riscos de reidentificação, pelos meios adequados, como a anonimização de tais dados pessoais, sem diminuir substancialmente a qualidade ou a utilidade dos dados. Os dados pertinentes são anonimizados se os dados pessoais forem irreversivelmente alterados de tal modo que as informações não digam respeito a uma pessoa singular identificada ou identificável ou sempre que os dados pessoais sejam anonimizados de tal forma que o seu titular não seja identificável ou já não possa ser identificado" (*Considerando* 61).

[206] A propósito das respetiva responsabilidades, em termos gerais e ainda tendo por referência a *Proposta*, tem bastante interesse o texto de Margarida Melo SANTOS (2022).

Bibliografia

ABREU, Joana Covelo de (2017). "O Mercado Único Digital e o seu desígnio político-constitucional: o impacto da Agenda Eletrónica Europeia nas soluções de interoperabilidade". *UNIO - EU Law Review*, Vol. 3 n. 1;

ALSENOY, Brendan Van (2017), "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation", *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. n. 7;

ALVES, Diogo Lopes (2021), "O papel fundamental da Cibersegurança na Proteção de Dados Pessoais", *Anuário da Proteção de Dados - 2021*, pp. 121-154;

BYGRAVE, Lee A. (2017), "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements", *Oslo Law Review*, Vol 4. n. 2, pp. 105-120;

CALZOLAIO, Simone (2017), "*Privacy by design*. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679", *Federalismi.it – Rivista di diritto pubblico italiano, comparator e europeo*, n. 24, pp. 2-21;

CARRAPIÇO, Helena; BARRINHA, André (2018), "European Union cyber security as an emerging research and policy field", *European Politics and Society*, Vol. 19, n. 3, pp. 299-303;

CARVALHO, Ana Sofia; POÇAS, Isabel Restier (2020), "Big data e o regulamento geral de proteção de dados da União Europeia". *Revista Ibérica do Direito*, Vol. 1, n.º 2(1);

CHELES, Tamára (2021), "Os Desafios dos Consumidores na Era de *Big Data*", *Anuário da Proteção de Dados - 2021*, pp. 155-176;

CORDEIRO. A. Barreto Menezes (2018), "Dados pessoais: conceito, extensão e limites", *Revista de Direito Civil*, A. 3 n. 2, pp. 297-321;

CORTE, Lorenzo dalla (2019), "Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law", *European Journal of Law and Technology*, Vol. 10 n. 1;

COTINO HUESO, Lorenzo (2017), "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata – Revista internacional de éticas aplicadas*, n. 24, pp. 131-150;

DANESIS, George *et al*. (2014). *Privacy and Data Protection by Design – from policy to engineering*, ENISA - Agência da União Europeia para a Cibersegurança;

D'ACQUISTO, Giuseppe *et al*. (2015). *Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics*, ENISA - Agência da União Europeia para a Cibersegurança;

DE MIGUEL ASENSIO, Pedro A. (2019), "Servicios de almacenamiento y tratamiento de datos: el Reglamento (UE) 2018/1807 sobre libre circulación de datos no personales", *La Ley Unión Europea*, n. 66, pp. 1-6;

DIAS, Lurdes Alves (2018), "RPGD: Principais Dificuldades e Dúvidas das Organizações e dos Titulares de Dados Pessoais na Adaptação ao Atual Regime", *Cyberlaw by CIJIC*, n. 6;

DIAS, Fernanda Ferreira (2016), "O Mercado Único Digital Europeu", *Análise Europeia - Revista da Associação Portuguesa de Estudos Europeus*, n. 2, pp. 16-41;

DIJK, Niels van; GELLERT, Raphaël; ROMMETVEIT, Kjetil (2016), "A risk to a right? Beyond data protection risk assessments", *Computer Law & Security Review*, Vol. 32 n. 2, pp. 286-306;

DUCATO, Rossana (2016), "La crisi della definizione di dato personale nell'era del web 3.0", *Quaderni della Facoltà di Giusrisprudenza dell'Università di Trento*, n. 26, pp. 143-178;

ESAYAS, Samson Yoseph (2015), "The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach", *European Journal of Law and Technology*, Vol. 6 n. 2;

FIGUEIREDO, Joana Diniz de (2022), "As Smart Cities e a Privacidade: o critério legal para a anonimização de dados agregados", *Anuário da Proteção de Dados 2022*, pp. 217-253;

FREITAS, Pedro Miguel (2018), "Regulamento Geral de Proteção de Dados: uma visão portuguesa sobre o regime sancionatório". *UNIO - EU Law Review*, Vol. 4 n. 2;

FROUFE, Pedro Madeira (2021). "Cinco notas introdutórias à Lei dos Serviços Digitais: construindo o futuro digital da Europa (*Another brick in the wall*)". ABREU, Joana Covelo de; COELHO, Larissa; CABRAL, Tiago Sérgio (Ed.) *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)* - Volume II. Braga: Pensamento Sábio - Associação para o conhecimento e inovação da Universidade do Minho / Escola de Direito, pp. 23-28;

GIL, Elena (2016), *Big data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos / Boletín Oficial del Estado;

GOUVEIA, Jorge Bacelar (2021). "*CyberLaw and CyberSecurity*". *Revista Jurídica Portucalense*, n.º 29;

GRUSCHKA, Nils *et al*. (2018), "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR", *Proceedings of the 2018 IEEE International Conference on Big Data*, Seattle;

HABEGGER, Benjamin *et al*. (2014), "Personalization vs. Privacy in Big Data Analysis", *International Journal of Big Data*, n. 1, pp. 25-35;

HANSEN, Marit; LIMNIOTIS, Konstantinos (2018), *Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default*, ENISA – Agência da União Europeia para a Cibersegurança;

HOOFNAGLE, Chris J.; SLOOT, Bart van der; ZUIDERVEEN BORGESIUS, Frederik (2019), "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law*, Vol. 28 n. 1, pp. 65-98;

JANSSEN, Katleen; HUGELIER, Sara (2013), "Open data as the standard for Europe? A critical analysis of the European Commission's proposal to amend the PSI Directive", *European Journal of Law and Technology*, Vol. 4 n. 3;

KAMARA, Irene (2017), "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'", *European Journal of Law and Technology*, Vol. 8 n. 1;

LOPES, Eliseu Pinto (2022), "Avaliação de impacto sobre a proteção de dados", *Privacy and Data Protection Magazine*, n.º 5, pp. 101-142;

LOPES, Teresa Vale (2018), "Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados", *Anuário da Proteção de Dados - 2018*, pp. 45-69;

LUCCHINI GUASTALLA, Emanuele (2018), "Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori", *Contratto e Impresa*, n. 1, pp. 106-125;

MALTZAN, Stephanie von (2019), "No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protection Compliant Incident Response System", *European Journal of Law and Technology*, Vol. 10 n. 1;

MANTELERO, Alessandro (2016), "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", *Computer Law & Security Review*, Vol. 22 n. 2, pp. 238-255;

IDEM (2017), "Responsabilità e rischio nel Reg. UE 2016/679", *Le nuove leggi civili commentate*, Vol. XL n. 1, pp. 144-164;

MASSENO, Manuel David (2019), "Como a União Europeia procura proteger os cidadãos-consumidores em tempos de *Big Data*", *Revista Eletrônica do Curso de Direito da UFSM*, Vol. 14 n.º 3;

MASSENO, Manuel David (2021), "Nas Fronteiras da Propriedade Intelectual: os direitos patrimoniais sobre dados, uma perspetiva europeia", *Privacy and Data Protection Magazine*, n.º 1, pp. 212-221;

MASSENO, Manuel David; SANTOS; Cristiana Teixeira (2018), "Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations", *MediaLaws – Rivista di diritto dei media*, n. 2, pp. 251-266;

IDEM (2019), "Personalization and profiling of tourists in smart tourism destinations - a data protection perspective", *International Journal of Information Systems and Tourism*, Vol. 4 n. 2, pp. 7-23;

MASSENO, Manuel David; MARTINS, Guilherme Magalhães; FALEIROS Júnior, José (2020), "A segurança na proteção de dados: entre o RGPD europeu e a LGPD brasileira", *Revista do CEJUR / Tribunal de Justiça de Santa Catarina - Prestação Jurisdicional*, Vol. 8 n.º 1;

MORENO MUÑOZ, Miguel (2017), "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", *Dilemata – Revista internacional de éticas aplicadas*, n. 24, pp. 1-23;

MOORE, Roksana (2013), "The Case for Regulating Quality within Computer Security Applications". *European Journal of Law and Technology*, Vol. 4 n. 3;

ORTEGA JÍMENEZ, Alfonso; GONZALO DOMENECH, Juan José (2018), "Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea", *Revista de la Faculdad de Derecho de la Universidad de la República*, n. 44;

PEREIRA, Alexandre L. Días (2018). "A Proteção de Dados Pessoais e o Direito à Segurança Informática no Comércio Eletrónico". *Banca, Bolsa e Seguros*, n.º 3, pp. 303-329;

PEREIRA, Bruno; ORVALHO, João (2019), "Avaliação de Impacto sobre a Protecção de Dados", *Cyberlaw by CIJIC*, n.º 7;

PEREIRA, Miguel (2021), "Taming Europe's digital landscape? Brief notes on the proposal for a Digital Services Act". *UNIO - EU Law Review*, Vol. 7 n. 2;

PICA, Luís (2018). "As Avaliações de Impacto, o Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais", *Cyberlaw by CIJIC*, n.º 5;

IDEM (2021). "A definição de perfis no direito tributário e a tutela dos dados pessoais dos obrigados tributários no direito português", *Revista de la Facultad de Derecho de la Universidad de la República*, n.º 51;

PURTOVA, Nadezhda (2018), "The law of everything. Broad concept of personal data and future of EU data protection law", *Law, Innovation and Technology*, Vol. 10 n. 1, pp. 40-81;

RASO, Filippo A. (2018), "Innovating in Uncertainty: Effective Compliance and the GDPR", *Harvard Journal of Law & Technology Digest*;

RICCIO, Giovanni Maria; PEZZA, Federica (2018), "Certification Mechanism as a Tool for the Unification of the Data Protection European Law", *MediaLaws – Rivista di diritto dei media*, n.º 1, pp. 249-260;

SANTOS, Margarida Melo (2022). "Plataformas digitais – que preocupações regulatórias?". RIBEIRO, João César; ABREU, Joana Covelo de; AMORIM, Carlos Abreu (Ed.) *Democracia e Comunicação Social – um debate introdutório para a era digital*. Braga: UMinho Editora, pp. 29-33;

SCHARTUM, Dag Wiese (2017), "Intelligible Data Protection Legislation: A Procedural Approach", *Oslo Law Review*, Vol 4. n. 1, pp. 48-59;

SCHWARTZ, Paul; SOLOVE, Daniel (2011), "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *New York University Law Review*, Vol. 86, pp. 1814-1894;

SILVA, Nuno Sousa e (2021), "Novas regras para a Internet: notas breves sobre iniciativas europeias de regulação de plataformas digitais", *Revista de Direito Intelectual*, n.º 1, pp. 75-102;

SPINDLER, Gerald; SCHMECHEL, Philipp (2016), "Personal Data and Encryption in the European General Data Protection Regulation", *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 7;

STALLA-BOURDILLON, Sophie; KNIGHT, Alison (2017), "Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data", *Wisconsin International Law Journal*, Vol. 34 n. 2, pp. 285-322;

TEIXEIRA, Angelina (2016), "A Chave para a Regulamentação da Protecção de Dados (Das pessoas singulares)", *Data Venia - Revista Jurídica Digital*, n.º 6, pp. 6-32;

TORBAY, Augusto Cesar (2020), "A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia", *Anuário da Proteção de Dados – 2020*, pp. 49-78;

URQUHART, Lachlan; LODGE, Tom; CRABTREE, Andy (2019), "Demonstrably doing accountability in the Internet of Things", *International Journal of Law and Information Technology*, Vol. 27 n. 1, pp. 1-27;

VIGURI CORDERO, Jorge A. (2018), "La Certificación en el Nuevo Reglamento Europeo de Protección de Datos y Anteproyecto de Ley Orgánica de Protección de Datos", *El Tiempo de los Derechos*, n. 11;

VITORINO, Beatriz Macedo; RAMOS, João Pinto (2021). "Introdução à Proposta do Regulamento dos Mercados Digitais". *Revista de Direito e Tecnologia*, Vol. 3 n.º 1, pp. 105-139.

II_Outros Estudos

Criptoarte, Direitos Autorais e Consumo Conspícuo: O Conceito de Obra Original no Uso de Tokens Não Fungíveis (Non-Fungible Tokens - NFT) no Mercado de Arte Digital[207]

Renato Dolabella Melo[208]

INTRODUÇÃO

Recentemente, uma nova forma de comercialização de obras de arte começou a se popularizar: a venda de obras digitais certificadas por um *non-fungible token* (NFT)[209] que atesta que aquele material se trata de um objeto único. Somente em 2021 já foram noticiados vários negócios milionários executados por meio desse novo modelo. No Brasil, podemos destacar, entre outros casos, o uso de NFTs em cards esportivos no formato digital. Já há exemplos que demonstram que o arquivo certificado como único por meio do token obtém uma valorização maior entre colecionadores, se comparado aos cartões que, embora apresentem também imagens de jogadores, não tenham esse atestado de singularidade[210].

Tais fatos chamam atenção, não apenas pelo valor, mas também pela novidade desse tipo de operação. No caso, a exclusividade adquirida pelo comprador se baseia em uma declaração do artista sobre o caráter "único" de uma obra que, a princípio, poderia tecnicamente ser reproduzida de forma absolutamente idêntica, dada sua natureza digital. Assim, trata-se de situação distinta da venda tradicional de obras de artes plásticas, na qual há uma tela, escultura ou suporte físico similar contendo a manifestação artística. O adquirente não mais mantém sob sua posse um objeto tangível, mas sim um *certificado único de autenticidade* validado por meio de *blockchain (non-fungible token – NFT)*.

Nesse contexto, percebe-se um novo comportamento do consumidor e deve-se investigar os motivos que o levam a investir grandes quantias na aquisição de algo

[207] *Projeto de Pesquisa apresentado à Faculdade de Direito da Universidade Federal de Minas Gerais, como requisito para conclusão de residência de Pós-Doutorado.*

[208] Advogado, pós-doutoramento na Faculdade de Direito da Universidade Federal de Minas Gerais.

[209] Os NFTs são códigos digitais que usam a tecnologia *blockchain* para atestar que cada arquivo é único. Com isso, são elementos não fungíveis, uma vez que não existem dois NFTs iguais.

[210] https://ge.globo.com/futebol/times/atletico-mg/noticia/atletico-mg-se-surpreende-com-resultados-iniciais-do-projeto-nft-nao-so-se-paga-ja-da-lucro.ghtml

que não é sequer uma obra concreta (no sentido de obra tangível, corpórea)[211]. Além disso, há várias disposições na legislação de direitos autorais (Lei 9.610/98) que se baseiam no conceito tradicional de "obra original", não havendo previsão legal sobre a sua aplicação (ou não) no caso dos novos negócios efetivados via NFTs. Assim, é importante o estudo das questões jurídicas envolvendo o tema.

Dessa forma, a pesquisa se justifica tanto pelos altos valores pecuniários envolvidos nas alienações das obras digitais com NFT, quanto pela novidade do tema e inexistência de referências sobre o assunto na legislação de direitos autorais. De fato, a Lei 9.610 é do ano de 1998, de modo que qualquer questão envolvendo modelos de negócios digitais não encontra respostas prontas nessa norma. Como a venda das obras com NFTs é um fenômeno extremamente recente, o tema ainda não foi tratado amplamente na doutrina jurídica ou na jurisprudência, especialmente no que diz respeito ao enquadramento (ou não) das criações como originais para fins jurídicos.

Deve-se ainda destacar que essa lacuna conceitual sobre a originalidade tem consequências práticas muito relevantes para os envolvidos nas vendas das obras. A Lei 9.610/98, por exemplo, prevê o direito de sequência em favor do autor, de modo que este tem o direito de perceber pelo menos 5% do lucro em uma eventual revenda de sua criação. Considerando que o uso recente dos NFTs na arte já rendeu negócios milionários, é possível que essas mesmas obras sejam novamente negociadas no futuro pelos seus atuais proprietários. E tais transações têm o potencial de gerar outras movimentações financeiras relevantes. Assim, eventual entendimento de que se trata de obras originais forçosamente implicaria a obrigatoriedade de repasse ao autor de parte do lucro obtido na revenda.

Na mesma linha, a ausência de um suporte físico que represente a posse física da obra pode gerar uma confusão entre a sua aquisição e a transferência dos seus direitos autorais. No caso de objetos tangíveis/corpóreos, a Lei 9.610/98 é clara ao diferenciar essas situações e indicar que a compra do original não implica automaticamente a obtenção dos direitos autorais de exclusividade. Dada a natureza particular das obras certificadas com NFTs, essa é outra questão que demanda investigação científica.

Assim, a novidade do tema e os relevantes impactos que a discussão pode gerar justificam a pesquisa. Nesse sentido, passaremos a analisar o conceito de blockchain/NFTs, motivações para a aquisição das obras digitais nesse novo modelo e questões de impacto prático para o tema no âmbito dos direitos autorais, como direito de sequência e a diferença entre cessão e aquisição de original.

---

[211] "People value and surround themselves with objects to which they attach their lives and experiences. Keychains and tee-shirts memorialize family vacations. Mint condition vinyl records represent years of memories and collecting. Humans innately seek to store value from their life in these objects. Consistent with the digital shift, the way we do that has changed dramatically. As an example: ask someone in two different decades what they would save from their house if it were burning down. In the 1950s someone might say a photo album. In the 2010s, someone is much more likely to say their phone or laptop. All the sentimental and personal value that people used to store in the objects around them is now stored inside of digital devices or in the cloud. Photo albums become photo apps. Letter exchanges become text messages". (FAIRFIELD, 2021, p. 6 e 7)

1. Blockchain e NFT

Para compreender adequadamente o blockchain e como ele funciona no âmbito dos NFTs, inicialmente é preciso entender alguns conceitos técnicos que envolvem essa tecnologia. O primeiro deles é a hash function. Esta é uma função computacional que converte informações em um código de tamanho fixo, chamado hash[212]. É importante destacar que duas entradas idênticas sempre vão gerar o mesmo resultado na saída. Porém, conteúdos com pequenas diferenças, ao serem processados por uma hash function, implicam códigos totalmente distintos:

> A hash function is an algorithm that converts data of any size into a fixed length data string. One of the most used hash functions is the Secure Hash Algorithm 256 or SHA256, which generates a string of 256 bits. If the data are a video larger than a Gigabyte, a multi-megabyte picture or a text message of only a few bytes, the output is always a constant 256 bits. For the sake of convenience, the 256 bit-string is normally represented with 64 hexadecimal characters in the hash output (Table 1). For any algorithm, an identical input generates the same result. So, in the hashing case, the same input data always generates the same hash output value. However, there is one essential difference with other algorithms. While in many algorithms a minor change of the input value results in nearby output values, at least in predictable orders of magnitude, the slightest change in the input data of a secure hash algorithm results in an entirely different hash value, even if it the change is only a single colour value of a pixel in an image, a comma or space in a text document or the third digit after the comma in a number, as is demonstrated in Table 1.

[212] "A hash is a one-way mathematical relationship whereby an input generates a unique alphanumeric string of limited length. Anything can be hashed: a picture, the entire text of the Encyclopedia Britannica, or in the case of blockchains, a list of transactions showing who owns what. The key element to a hash is that if any part of the input is changed, the hash changes, revealing that a fraudster has attempted to alter some piece of data". (FAIRFIELD, 2021, p. 17)

Table 1. Transformation of a string using the SHA-256 hash function.

Input	SHA-256 output (256-bit binary format)	64-symbol hex representation[4]
Hello World	10100101100100011010011011 01010000001011111101000010 00000100000001001010000000 01000101110011001111001111 10110111101100011001000011 01011000101100011001011011 11110000101111001101101000 11001010110101011110110010 01110111110110011010110110 01111100010100011101110	a591a6d40bf420404a011 733cfb7b190d62c65bf0bc da32b57b277d9ad9f146e
Hello, World	00000011011001110101101011 00010100111111111110011100 11010001010100110101110011 00110001111101111111001101 11111010001011000100010110 00110001010010000110000011 01110001111101000001100011 01110000010011011011110010 11010001100110101100000111 11101111101000101100101	03675ac53ff9cd1535ccc7 dfcd- fa2c458c5218371f418dc1 36f2d19ac1fbe8a5

Source: Banking Concepts.

This characteristic results in two consequences:

- Applying the same hash function to the same input data, e.g., a data file, makes it possible to verify whether the input data has been altered.

- For a secure hash algorithm, it is impossible to predict the exact hash value or a range of hash values for a given change in the input data. (BRAUN-DUBLER, *et ali,* 2020, p. 46 a 48)

Isso tem implicações relevantes no que diz respeito à integridade do arquivo e à capacidade de verificar eventuais alterações nele, o que será extremamente importante para a dinâmica do blockchain, como se verá a seguir. Além disso, vale destacar que o algoritmo indicado acima (SHA256)[213] pode gerar uma quantidade gigantesca de códigos diferentes, suficiente para identificar individualmente cada átomo do universo conhecido:

> Cryptography operates through probabilities. Relying on probabilities, even when low, often causes uneasiness if the associated risks cannot be translated into our everyday life. To illustrate the power of big numbers in cryptography, we take the SHA256 algorithm described above and calculate how many combinations can be built from a 256-bit string. $2256 \approx 1.16 * 10^{77}$ = 115 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 Since this number is so large that it is abstract to our understanding, we approximate it with real-world examples based on atoms. The human body

[213] "SHA-256 is a hashing algorithm created by the NSA, which is considered particularly secure. It always generates a 32-byte hash value, notwithstanding the size of the original data" (FINCK, 2018, p. 5).

> consists mostly of water with approximately 10^{19} atoms. Most of the earth consists of iron and, taking this as a base, the earth has about 10^{49} atoms. There exist an estimated 10^{11} to 10^{12} stars in our galaxy and 10^{23} stars in the universe. The number of atoms in the known universe containing billions of galaxies is estimated between 10^{78} and 10^{82}. So, as a rough approximation, a 256-bit string is enough to identify every atom in the known universe uniquely. (BRAUN-DUBLER, *et ali,* 2020, p. 49)

É importante destacar que há mais de uma versão do algoritmo SHA, que diferem basicamente na sua capacidade de compressão de dados e o nível de segurança decorrente disso. Quanto maior for essa capacidade, menor é a chance de colisão entre os resultados processados pelo algoritmo e maior é o seu nível de segurança:

> In the absence of analytical attacks, the maximum collision resistance of SHA0 and SHA-1 is about 2^{80}, which is not a good fit if they are used in protocols together with algorithms such as AES, which has a security level of 128–256 bits. Similarly, most public-key schemes can offer higher security levels, for instance, elliptic curves can have security levels of 128 bits if 256 bits curves are used. Thus, in 2001 NIST introduced three more variants of SHA-1: SHA-256, SHA-384 and SHA-512, with message digest lengths of 256, 384 and 512 bits, respectively. A further modification, SHA-224, was introduced in 2004 in order to fit the security level of 3DES. These four hash functions are often referred to as SHA-2. [...] If a collision search attack is applied to the hash function — an attack that due to the birthday paradox is in principle always feasible as we recall from Section 12.2.3 of Understanding Cryptography [11] — SHA-3 with 256, 384 and 512 bit output shows an attack complexity of approximately 2^{128}, 2^{192} and 2^{256}, respectively. This is an exact match for the cryptographic strength that the three key lengths of AES provide against brute-force attacks (cf. [11, Chapter 6.2.4]). Similarly, 3DES has a cryptographic strength of 2^{112}, and SHA-3 with 224 bit output shows the same resistance against collision attacks. (PAAR e PELZL, 2010, p. 2 e 4)

Tecnicamente, qualquer coisa pode passar por uma hash function e gerar uma hash, nos moldes explicados acima. Porém, é importante notar que normalmente o código não contém o conteúdo em si, mas uma indicação apontando o local onde o

conteúdo está arquivado[214,215]. Há questões relacionadas a custos[216] e apenas arquivos muito pequenos poderiam ser armazenados dentro da blockchain, o que limita bastante essa possibilidade. A primeira hipótese é chamada de armazenamento off-chain, enquanto a segunda é on-chain:

When it comes to transferring NFTs, the location of the item matters, because off-chain storage is subject to deletion. The two main options for storage are on-chain and off-chain storage. Off-chain storage means that the art or other digital item being purchased is stored somewhere else in a centralized server. The token that someone buys merely keeps a record of who owns that item. The token contains a pointer that indicates that the token is tied to the digital item being sold similar to a deed that has the address of the property being bought. Items that are stored off-chain will cease to exist if the company maintaining the storage server ceases to exist, or even turns off the server. A user may also be subject to additional restrictions that are imposed by the server host. When a digital item is stored on-chain, the art itself is hashed directly into the token. On-chain storage allows for the item to continue existing even if the original company hosting the item on its servers no longer exists. On-chain storage thus provides greater security for a purchaser because the value of the NFT is no longer tied to the continued existence of any one particular server or company. The downside of on-chain storage is that space is much more limited. Only smaller bits of data can be stored and traded directly in the tokens". (FAIRFIELD, 2021, p. 42 a 44)

A partir dos *hashs,* há uma estruturação desses códigos em blocos, que são encadeados de forma linear, sempre na mesma direção. O termo *blockchain* se origina justamente desse fato[217]:

---

214 "Often, an NFT stands for ownership of something not directly stored on the blockchain—a piece of digital art, for example. The token contains a pointer to find the digital art file, and a hash of the file as proof. So a token representing digital art might contain a URL pointing to the art and a hash of the art file. In this way, an NFT might convey an ownership interest in a piece of digital art, an asset in an online game, a card in a collectible trading card game (think rare baseball cards here), or a plot of land in a virtual world. Or, a token might convey rights in a real-world asset, in an RFID-linked consumer good or a car that only unlocks and drives for the token owner". (FAIRFIELD, 2021, p. 23)

215 "Relevante destacar que o *blockchain* não armazena os dados em si, ou seja, ele não possui todas informações de um documento ou de uma transação que ele representa. Ao contrário, no *blockchain* os dados e informações ficam representados em códigos (*hash*) ou assinaturas digitais que, por sua vez, remetem aos dados que ficam armazenados no banco de dados". (MOREIRA, DELGADO e SANTOS, 2021, p. 40)

216 "Blockchain facilitates transactions and exchange of value on a distributed ledger by being able to add data to tokens, but it is rarely and unlikely to be efficient to store creative content on the blockchain simply because such data files will often be very large. (Cost efficient data insertion onto the bitcoin blockchain is on the order of kilobytes, certainly not megabytes, Sward et al 2018). Thus only relatively high value data is economically stored onchain. Therefore blockchain will likely continue to be best used to coordinate and validate off-chain storage of creative content data". (POTTS e RENNIE, 2017, p. 09)

217 "Blockchain platforms can re-architect registry systems and guarantee their integrity without trusted intermediaries like governments and banks, creating a form of "trustless trust". That trust is based on blockchain technology providing a way of guaranteeing that a record exists or existed on a ledger at a certain time. It does not matter what that

> Muito resumidamente, uma *blockchain* constitui-se em um banco de dados composto por "blocos encadeados" nos quais são registradas transações. Quando a capacidade de armazenamento de um bloco está completa e após ser validado – por meio de um protocolo que será analisado ao longo do artigo – ele é adicionado ao fim da "corrente". Tal analogia com uma corrente dá-se porque, se nela cada elo está atrelado ao anterior por meio de encaixe e solda, em uma *blockchain*, cada bloco faz referência ao antecedente, denominado "parent block" - ou, em tradução literal, "bloco pai" - por meio do armazenamento do *hash* deste. *Hash*, por sua vez, trata-se de um pequeno "pedaço de dados" que tem como intuito identificar "objetos digitais maiores". Ele é gerado mediante um processo criptográfico que foi desenvolvido pela U.S. National Security Agency (NSA) e funciona similarmente a uma "impressão digital", uma vez ser impossível obter o mesmo *hash* de "objetos digitais" distintos. [...] Mas como e por que essa analogia da tecnologia como uma "cadeia de blocos" existe? A cadeia de blocos agrupa as transações variadas e valida cada um desses grupos. Ou seja, a validação só ocorre depois de cada transação isolada ter sido incluída no bloco. Para cada rede baseada em *blockchain* há uma tentativa de buscar o consenso que orienta como as informações podem ser adicionadas ao repositório compartilhado. A *blockchain* é uma cadeia de blocos ordenados de forma temporal validados por meio de um algoritmo para resolver um problema matemático que envolve funções *hash* unidirecionais. O tamanho da *blockchain* aumenta conforme cresce o número de transações. Cada bloco contém um *hash* exclusivo (equivalente a uma espécie de digital única), lote das transações mais recentes e o *hash* do bloco anterior. (MOREIRA, DELGADO e SANTOS, 2021, p. 31)

---

record is – it may be a file, a piece of music, a transaction, a piece of digital art or an email. The majority of interest in blockchains concerns the storage of transaction records for digital tokens or cryptocurrencies, but the technology can effectively store any record in the same way. For example, with respect to intellectual property, a blockchain will not store the actual copyrighted material, but rather a cryptographic artefact that identifies that material as it existed at a particular point in time. To add such a record to a blockchain, the intellectual content (or transaction record, or any other data) is first run through an algorithm to create a unique, encrypted string of data called a "hash". This hash uniquely identifies the record, and guarantees its integrity because there is no way that the record can be altered without changing the hash. Once a record has been hashed, it is then gathered together with a small number of other hashes of other entries made to the ledger that were encrypted around the same time. This collection of entries is called a "block". Each block is then itself turned into a hash, with every new block also referring to the hash of the previous block, creating a cryptographically connected chain of blocks. Any modification to an older block will sever the chain because the hash of that block will no longer be validly referenced in the subsequent blocks. This is why the protocol is called the "blockchain" – it is a chain of blocks". (TRESISE, GOLDENFEIN e HUNTER, 2018, p. 02)

Cada bloco possui uma *hash*, que é gerada por meio de um algoritmo, como explicado anteriormente, e que fica registada em uma espécie de "livro-razão" público (*ledger*)[218]:

> Distributed ledgers, commonly called blockchains, are databases that no one entity controls, but that anyone can write to. In the case of many blockchains, the database is a list of who owns what—who owns which bitcoins, for example. The immediate problem of letting anyone write to the database is fraud. What if person A decides to pay B one unit, but then write to the database that she has retained that unit? Blockchains use a consensus mechanism to make it either too much work (proof of work systems) or too risky (proof of stake systems) to attempt to falsify the ledger. This is addressed by a mathematical relationship called a hash, and a consensus mechanism for verifying hashes. [...] Think of the blockchain like a book of transactions or a ledger. A new page is added to the book and people are able to write their transaction onto the new page. Since everyone is able to access the book, we might be worried that someone would come along and tear a page out, add a new page, or erase and alter a transaction from an earlier page in the book. Blockchain solves those problems. You know that a page is missing if the book goes from page two to page four without page three. You know a page is added if there are additional pages or more than one page seven. Each page is made impossible to alter by laminating and sealing each page. The blockchain provides similar protections for each information and transaction in virtual space by allowing each person to maintain a copy of the book and constantly checking each copy against one another. (FAIRFIELD, 2021, p. 15, 19 e 20)

Um aspecto extremamente relevante em relação à blockchain é que a informação que alimenta a hash function para gerar o código de um bloco necessariamente contém a hash do bloco anterior. Assim, qualquer tentativa de mudança na informação de um bloco geraria uma reação em cadeia, alterando os hashs de todos os blocos seguintes[219]. Essa é uma característica fundamental para assegurar a confiabilidade da informação contida em uma blockchain, uma vez que a

---

[218] "Blockchain is the technical protocol at the heart of Bitcoin. However, it has also recently spurred examinations of how we might change the legal system in areas like land title registration, share registries, privacy, financial regulations, banking and payments, secured transactions, currency systems, and many, many others. A blockchain is a form of "distributed ledger", and this term captures the essence of the technology – simply put, the blockchain is a technical protocol to create a secure, transparent ledger that reports transactions to everyone within a given blockchain's network". (TRESISE, GOLDENFEIN e HUNTER, 2018, p. 01)

[219] "A group of transactions can be recorded in what is called a block. New blocks are created through a process of "mining" in which different computers compete to solve a complicated math problem, and the computer that wins is rewarded the block. All of the transactions are recorded on that block and the block is closed and hashed, creating a unique identifying number. That number forms the basis for the next math problem that the miners then try to solve. Each block in the chain is mathematically linked to the block right before and right after it. When a new block is added, it is hashed together with the previous block's hash. Altering one block would mean that you have to alter every block that came before it. The connectedness of the entire chain protects the blockchain from fraud and censorship". (FAIRFIELD, 2021, p. 17 a 19)

alteração do conteúdo em determinado ponto seria notada inclusive pelas modificações em outros blocos da corrente:

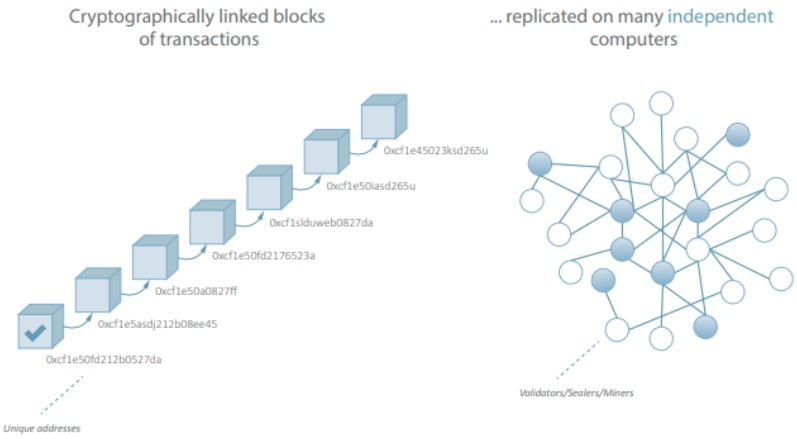
> Uma blockchain começa com um primeiro bloco, denominado "genesis block". No caso da Bitcoin, ele foi criado em 2009 e codificado com os protocolos da moeda digital, não podendo ser alterado. Todos os nós possuem uma cópia da blockchain, que começa desde o "genesis block". A rede está constantemente sofrendo atualizações, na medida em que novos blocos são validados e "adicionados" à cadeia, aumentando-se, dessa forma, a "altura" desta, "empilhando-se" cada vez mais blocos. "Block height", inclusive, é uma maneira de identificar a posição de um bloco, sendo que a block height do genesis block é zero. Como já dito, o link de um bloco com o anterior, o parent block, dá-se por meio do hash. Os nós, então, examinam o "header block", que consiste em três conjuntos de metadados insertos no bloco, entre os quais se encontra o hash do bloco anterior ou bloco pai. O hash do parent block afeta o cálculo do "child block", ou, em tradução literal, "bloco filho", que nada mais é que o bloco posterior que está sendo - ou que em algum momento foi - adicionado à cadeia. Se o hash do parent block for modificado, isso implica que o hash do child block também o será, assim como o de todos os subsequentes, gerando um "efeito cascata". Dessa maneira, a alteração de um determinado bloco, por menor que seja – como em uma tentativa de alterar qualquer aspecto de uma transação – consequentemente alteraria o seu hash, assim como o de todos os blocos posteriores. Para fazê-lo, requerer-se-ia um enorme poder computacional, tornando inviável tal tarefa na maioria dos casos. Quanto maior se torna a cadeia de blocos, maior o poder computacional necessário para alterá-la e, consequentemente, maior tende a haver, na prática, uma efetiva imutabilidade da blockchain. (MOREIRA, DELGADO e SANTOS, 2021, p. 32 e 33)

Além disso, o caráter descentralizado de validação do blockchain também é fundamental para a segurança do sistema, uma vez que ele opera por meio de um conjunto de computadores controlados por diversas pessoas diferentes, que trabalham conferindo a informação inserida na cadeia[220]. Nesse sentido, no caso de um

[220] "Blockchains are distributed peer-to-peer networks. Networks can be either client-server or distributed. Client-server networks are easy to administer, secure and police but rely on a trusted client to update the network, and consequently present a single point of vulnerability. By contrast, peer-to-peer networks are decentralized, robust, hard to police and censor, but also hard to administer and ensure consistency (consensus) about the state of the network. Blockchains also utilize an append-only database, where information is immutable, and transactions are recorded as additional data rather than overwriting existing data (as, for instance, a simple Excel spreadsheet does). Each block in the blockchain includes a 'hash' (a secure cryptographic summary) of the previous block in a chain all the way back to the genesis block mined by Nakamoto himself. [...] A blockchain is a secure distributed ledger, with security furnished by powerful token-based economic incentives (in a process called 'mining'), that records and validates 'blocks' of peer-to-peer transactions. These transactions are in effect exchanges of permissions to access an entry on a ledger (which they can hold or send to someone else), an exchange being valid if the node granting permission itself had valid access to that entry, forming a valid chain all the way back to the genesis. These numerical data 'entries' are the unit of the cryptocurrency, also known as a coin or token. Bitcoin, for instance, is the name given to these entries on the bitcoin blockchain. Because these entries have the qualities of money (scarce, fungible, unit of account), they can be used

blockchain aberto[221], a decisão de aceitar ou não a inserção de cada novo registo não está sujeita ao poder de uma única pessoa:

> Blockchain technology is also referred to as a trust engine or trust machine as it enables business between parties unknown to each other without involving a trusted intermediary to organise the exchange of assets. Blockchain technology derives its trust from two concepts (see Figure 4): 1. The continuous validation of transactional data, their packaging into blocks in constant time intervals and their cryptographical linkage in a continuously growing chain. A cryptographical linkage makes it impossible to alter a transaction without rechaining all the blocks added to the chain after the altered transaction. This chaining of blocks process is from where the term 'blockchain technology' is derived. 2. The replication of the blockchain data across a set of computers owned by different individuals or businesses. Computers that participate in a blockchain are called nodes. A consensus protocol built into the blockchain software ensures how the blockchain data are synchronised between the nodes. The more nodes participating, the harder it becomes to tamper with the data, which is why the technology is also referred to as distributed ledger technology (DLT).



Source: Banking Concepts.

Figure 4. The essence of blockchain technology.

> A blockchain is a decentralised database that is replicated on many servers or computers owned or governed by independent legal entities. Trust in a blockchain depends on two factors: 1. The low probability that one person or a group of persons have enough power to alter a transaction, recalculate all blocks after

as money, (indeed, Bitcoin was designed to be used as such)". (POTTS e RENNIE, 2017, p. 02 a 04)

221 Importante destacar que existem *blockchains* que não são abertos, chamados de *permissionários,* nos quais há um controle centralizado: "Existem Blockchains privados, como a plataforma Corda27, em que a participação na rede depende de aprovação e existe um controle sobre quem pode enxergar os dados de uma transação. Esses tipos de blockchains são protegidos por pessoa ou grupo de pessoas que têm membros conceituados e informações comerciais confidenciais. Além disso, essas redes são centralizadas, pois abrangem obrigatoriamente uma entidade permissionária, geralmente a organização que a criou. Ela é responsável por estabelecer quem pode ingressar no sistema" (SOUSA, 2022, p. 7)

> the transaction and force the remaining participants to accept these changes. A smaller chance of this scenario results in a higher level of trust. 2. The governance mechanisms for the changes of the software and consensus protocol. With better checks and balances in the development of the software supporting the distributed ledger, a higher level of trust is established. A drawback to having proper checks and balances is that needed changes to the software protocol may take longer and errors might not be corrected quickly. However, this result is part of the nature of democratic decision-making. (BRAUN-DUBLER, *et ali,* 2020, p. 61 e 62)

Isso colabora para dificultar as tentativas de alteração da blockchain, uma vez que, além de recalcular todas as hashs a partir do bloco modificado, seria necessário também atuar controlando um grande número das máquinas responsáveis pela validação para conseguir efetivar a mudança[222-223]. Isso demanda um enorme poder computacional, o que torna improvável o sucesso desse tipo de prática, inclusive porque o custo para realizar a adulteração poderia superar o benefício buscado pelo infrator[224]:

---

[222] "Diferentemente de outros sistemas online, a exemplo do Dropbox, a blockchain não possui um servidor central, mas faz uso da arquitetura de rede "peer-to-peer". Ou seja, não há na rede um único computador em que todos os dados estão armazenados e de onde um usuário, conectado a essa rede, possa ter acesso e baixar os arquivos que deseja. Em uma arquitetura peer-to-peer, todos os computadores participantes são "pares" uns dos outros, não havendo hierarquia. Todos os nós, como também são denominados os pares, possuem a mesma cópia da blockchain, o que torna desnecessária a existência de um servidor central. [...] A diferença do blockchain para um banco de dados comum é o fato de que, nele, as informações estão distribuídas e cada um dos nós da rede possui acesso àquele registro. Nos demais bancos de dados, também é possível que sua execução seja em plataformas em nuvem que ultrapassam os limites de um local físico. Contudo, ainda assim se diferenciam do blockchain, pois no banco de dados comum há o total controle dessas plataformas em nuvem e das próprias informações por uma pessoa ou grupo determinado que administra o banco de dados. Se assim o desejar, apenas o proprietário poderá fazer alterações no banco de dados ou descartar seu conteúdo. Os dados não estão registrados em rede "peer-to-peer", apenas se encontram acessíveis a vários usuários. No blockchain, ao contrário, não há centralização das informações, o que significa que não é apenas uma pessoa, ou um grupo delimitado de pessoas, que pode acessar aquele dado. O registro é feito em rede "peer-to-peer". (MOREIRA, DELGADO e SANTOS, 2021, p. 29 e 41)

[223] "[E]m razão da distributividade da blockchain, aliada ao mecanismo de consenso e ao algoritmo hash, uma vez que uma dada informação foi registrada, torna-se extremamente difícil modificá-la ou apagá-la, protegendo-a da atuação singular de um dos agentes nela envolvida (tamper proof). Tampouco é possível repudiar certo registro, tendo em vista o emprego de assinatura eletrônica (regra do não repúdio). A blockchain é, ainda, transparente, porque qualquer pessoa pode baixá-la e verificar as transações em que certa conta se envolveu. Conforme De Filippi e Wright, a impossibilidade de repudiar determinada transação, sua quase imutabilidade e sua transparência são fatores que contribuem para o fomento da confiança". (MOREIRA, DELGADO e SANTOS, 2021, p. 38 e 39)

[224] "O grande problema com arquiteturas distribuídas dá-se com o que é conhecido por "ataque Sybil". Como já mencionado, trata-se da criação orquestrada de nós maliciosos que têm como objetivo falsear o consenso. A resposta encontrada por Nakamoto a esse problema foi, primeiramente, o uso de assinatura por criptografia, por meio de uma chave-privada, garantindo que somente aquele que a possui é o autor de um determinado input. O outro mecanismo empregado é a já referida prova de trabalho. Como ela exige uma massiva e crescente capacidade computacional, os potenciais benefícios de um ataque Sybil tornam-se menores que os custos, o que faz

> Em uma rede descentralizada, há o risco da criação orquestrada de nós maliciosos que tem como objetivo falsear o consenso. Mas quando se faz necessário um poder computacional elevado para se resolver a prova de trabalho, os potenciais benefícios tornam-se menores que os custos, o que desincentiva tentativas de manipulação, preservando o consenso. A arquitetura em "cadeia de blocos" escolhida por Sakamoto para a Bitcoin possibilita a existência de uma rede descentralizada. Com o agrupamento de 1 de N transações em blocos e a necessidade de um considerável poder computacional para adicioná-los à corrente, a blockchain torna-se –quase – impermeável a ataques. (MOREIRA, DELGADO e SANTOS, 2021, p. 34)

O caráter descentralizado do sistema aberto também é importante para seu funcionamento contínuo, ainda que haja problemas com algum dos nós que compõem a rede:

> Ainda, a blockchain não só propicia a confiança de uma maneira inovadora, como também possui confiabilidade. Ambos os conceitos podem parecer tratar-se da mesma ideia, mas, conforme Bambara e Allen, confiabilidade é a capacidade de um sistema de computador de "[...] lidar com a falha de um ou mais de seus componentes" sem que isso prejudique o funcionamento do sistema como um todo. Se, em uma dada rede, um dos processadores apresenta mau funcionamento, o sistema como um todo deve ser capaz de continuar operando adequadamente. A confiabilidade na blockchain é atingida pelo processo de validação por meio do consenso alcançado pela maioria dos nós. Dessa forma, até o ponto em que tal maioria seja confiável, a rede funcionará devidamente. (MOREIRA, DELGADO e SANTOS, 2021, p. 39)

Assim, a *blockchain* pode implementar um sistema que não depende de uma autoridade central para validação das informações, quando utilizada na sua modadlidade aberta. No mesmo sentido, a autenticidade das transações registadas nos blocos, uma vez incorporadas aos mesmos, passa a não depender mais das partes originalmente envolvidas no negócio, uma vez que a cadeia é pública e validada pela rede descentralizada de computadores. Isso gera impactos tanto do ponto de vista do Direito quanto da Economia.

Sob o aspecto jurídico, a *blockchain* oferece uma nova maneira de atestar a autenticidade de uma informação ou documento, por meio de técnicas computacionais e matemáticas que lhe conferem segurança[225]. Além disso, o sistema

---

com que, na prática, esse tipo de ataque não seja vantajoso para o agressor". (MOREIRA, DELGADO e SANTOS, 2021, p. 38)

225 "Subjacente a cada rede baseada em blockchain está um mecanismo de consenso que governa como as informações podem ser adicionadas à base de dados compartilhados. Mecanismos de consenso tornam possível uma rede distribuída de pares registrar informações em uma blockchain, de maneira ordenada, sem a necessidade de confiar em um operador centralizado ou intermediário. Para garantir a integridade da rede e, também, a confiança no sistema, ao invés da utilização da figura do terceiro validador, o consenso é buscado por meio do uso da criptografia e funções

não se baseia em uma autoridade central e disponibiliza de forma pública as informações, o que gera uma redução dos custos de transação para o processo de conferência da validade do conteúdo por terceiros, gerando impactos positivos do ponto de vista econômico.

A tecnologia *blockchain* se tornou conhecida do público a partir do *bitcoin*[226]. No caso, por se tratar de uma criptomoeda, é fundamental que o sistema garanta que cada bitcoin seja gasto apenas uma vez pelo seu titular, mudando de proprietário com a transação de pagamento. O "livro-razão" do *blockchain* visa assegurar isso:

> The initial purpose of the blockchain was to ensure that tokens could be spent only once, and that a payment transaction, once validated, could not be repudiated. To achieve this, every Bitcoin transaction is validated by the network and placed into a public, distributed ledger. In this ledger, all transactions are grouped into blocks and cryptographically secured and linked. These linked blocks form the blockchain. Data can only be added to the database (i.e., the distributed ledger) through insertion to the next block, which, in Bitcoin, is built on average every 10 minutes. The cryptographical securing and linking of the blocks makes it substantially harder to tamper with the data because, in order to change a previous transaction, all subsequent blocks must be recalculated, relinked, and accepted by all network ledger participants. Every participant of the network can download the ledger and revalidate every transaction with minuscule effort to be sure that no one manipulated the ownership of the tokens. In order to send Bitcoin to another party, the sender must specify the amount, sign the data using a private key, encrypt it using the address (public key) of the recipient, and send the transaction to the network where it is validated. This validation process for Bitcoins consists of two functions: The first checks whether the sender is the legitimate owner and, if correct, creates a hash value of the transaction ID number. The second combines all hash values to be included in a block of transactions. (BRAUN-DUBLER, *et ali,* 2020, p. 63 e 64)

É importante destacar, contudo, que a aplicação do *blockchain* não se resume ao *bitcoin.* Um exemplo relevante de outro tipo de uso da tecnologia é o *ethereum*, que será especialmente relevante para o funcionamento dos NFTs. Uma característica

hash, para realização de registros sem risco significativo de que as informações sejam corrompidas ou modificadas. Sob essa perspectiva, refletir sobre o conceito do blockchain é também rever a forma como pensamos diversas categorias jurídicas com as quais lidamos no dia-a-dia. Trata-se da substituição do consenso estatal ou social pelo consenso computacional". (MOREIRA, DELGADO e SANTOS, 2021, p. 36)

[226] Deve-se destacar, entretanto, que o *blockchain* não surgiu com o *bitcoin*. Há registro, por exemplo, do trabalho "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups", elaborado em 1982 por David Lee Chaum, considerado como pioneiro na elaboração de vários princípios que hoje sustentam a dinâmica do *bitcoin.*

importante do *ethereum* é o seu uso de *smart contracts*[227-228]. Estes são protocolos de programação contendo regras de um contrato, que são executadas de forma automatizada. A possibilidade de uso dos *smart contracts* é bastante ampla, uma vez que o mecanismo permite sua aplicação em qualquer tipo de manifestação de vontade contratual:

> Blockchain platforms also allow us to automate transactions in ways that are both new and significant. Shortly before the White Paper that led to the creation of Bitcoin, Nick Szabo proposed a mechanism that he called a "smart contract", which was "a computerized transaction protocol that executes the terms of a contract". While smart contracts do not necessarily, in themselves, represent legal contracts, a smart contract can use computer code to represent an agreement. Unlike a regular contract however, smart contracts might automatically execute the terms of the agreement by transferring funds held in escrow or changing the state of registers or ledgers. (TRESISE, GOLDENFEIN e HUNTER, 2018, p. 03)

O modelo de negócio do NFT se utiliza da tecnologia do *ethereum* para gerar seus registos, autenticá-los como únicos e realizar transações no âmbito da criptoarte[229]. Para o usuário criar um token dessa forma, deve custear a operação com *ethers,* que é uma criptomoeda utilizada no âmbito do *ethereum.* A menor fração do *ether* é chamada de *wei*[230]. Genericamente, o custo para fazer as operações no *ethereum* é chamado de *taxa de gas*[231].

---

227 "A principal distinção de um smart contract em relação a um contrato regular é a de que, naquele, a execução das obrigações contratuais se dá de forma automatizada. Assim, muitos vêm nos chamados "contratos inteligentes" um poderoso mecanismo para redução de custos de transação e de eliminação de intermediários nas etapas de execução de um contrato. O contrato inteligente é formatado por meio de códigos que, idealmente, representam a vontade das partes. Assim, formatada a cadeia de códigos, cada etapa do contrato se concretizará de forma automática, evitando, portanto, descumprimentos ou alterações daquilo que foi inicialmente pactuado". (MOREIRA, DELGADO e SANTOS, 2021, p. 51)

228 "While Bitcoin is the first and most well-known blockchain and cryptocurrency, it is limited to the transfer of only Bitcoin. However, blockchain systems are not limited to cryptocurrencies. On the other end of the spectrum, Ethereum is the first and most popular open source platform supporting smart contracts. The label Ethereum is often applied with two meanings: The Ethereum permissionless blockchain, called Ethereum Main Net, is where traded Ether is mined and can be used by everyone to run decentralised applications with their smart contracts. The open source Ethereum software can be downloaded and used to create new permissionless or permissioned blockchains. This distinction is important for the clear assessment of blockchain projects". (BRAUN-DUBLER, *et ali,* 2020, p. 64)

229 "Blockchain was originally proposed by Nakamoto, where Bitcoin uses the proof of work (PoW) algorithm to reach an agreement on transaction data in a decentralized network. Blockchain is defined as a distributed and attached-only database that maintains a list of data records linked and protected using cryptographic protocols. Blockchain provides a solution to the long-standing Byzantine problem, which has been agreed upon with a large network of untrusted participants. Once the shared data on the blockchain is confirmed in most distributed nodes, it becomes immutable because any changes in the stored data will invalidate all subsequent data. The most prevailing blockchain platform used in NFT schemes is Ethereum, providing a secure environment for executing the smart contracts". (WANG *et alli*, 2021, p. 4)

230 10^{18} *wei* equivale a 1 *ether*.

231 https://ethereum.org/pt-br/developers/docs/gas/

A versatilidade do *ethereum* o torna um instrumento apto para implementar os NTFs na criptoarte, inclusive para indicar que determinado objeto digital é atestado como único:

> Non-Fungible Token (NFT) is a type of cryptocurrency that is derived by the smart contracts of Ethereum. NFT was _rstly proposed in Ethereum Improvement Proposals (EIP)-721 and further developed in EIP-1155. NFT differs from the classical cryptocurrencies such as Bitcoin in their inherent features. Bitcoin is a standard coin, in which all the coins are equivalent and indistinguishable. In contrast, NFT is unique which cannot be exchanged like-for-like (equivalently, non-fungible), making it suitable for identifying something or someone in a unique way. To be speci_c, by using NFTs on smart contract (in Ethereum), a creator can easily prove the existence and ownership of the digital assets in the form of videos, images, arts, event tickets, etc. Furthermore, the creator can also earn royalties each time of a successful trade on any NFT market or by peer-to-peer exchanging. Full-history tradability, deep liquidity, and convenient interoperability enable NFT to become a promising intellectual property (IP)-protection solution. Although, in essence, NFTs represent little more than code, but the codes to a buyer have ascribed value when considering its comparative scarcity as a digital object. It well secures selling prices of these IP-related products that may have seemed unthinkable for non-fungible virtual assets. (WANG *et alli*, 2021, p. 1 e 2)

Essa característica de "objeto único" difere o NFT das criptomoedas, em que pese usarem tecnologias similares. No caso das moedas digitais, há uma fungibilidade entre cada unidade monetária da mesma espécie, sobretudo para que possam exercer sua função como meio de troca. Já cada NFT, ao contrário, não é fungível, como o próprio nome indica. Esse aspecto é essencial para que esse tipo de *token* possa exercer a finalidade proposta para esse mecanismo, que se vincula a objetos considerados únicos[232].

É importante ainda notar que o NFT não necessariamente contém o arquivo digital, inclusive por uma questão de custos relacionados ao tamanho do bloco e ao trabalho necessário para operacionalizar as transações relacionadas ao mesmo[233]. Esse

---

232 "NFTs are not like previous cryptocurrencies, where one coin is much the same as another. Non-fungible tokens can be used to create digital artwork that can be bought, sold, and owned like a physical sculpture, or a database of real estate in which ownership is managed by electronic deeds that can be passed from one person to another with low or no transaction costs". (FAIRFIELD, 2021, p. 9)

233 "The block size defines the maximum number of bytes a block can contain. As the blockchain grows with every block added, the maximum size of a block plays an important role of how many people can participate in a blockchain, as it determines the disk capacity required for its operation. The block size for Bitcoin is 1MB and, as of December 2017, the size of the entire Bitcoin blockchain reached approximately 150 GB. As of June 2018, the average daily size of a Bitcoin block ranged from 0.5 to 1MB (Blockchain.com, n.d.-a). For Ethereum, the block size is defined slightly different as a limit in an 'energy unit', called gas, a block might contain. The energy units needed for a transaction are estimated from the number of bytes and the complexity of the functions a transaction contains, so the principle remains the same. As the block time for Ethereum is substantially shorter, the size of one block is also smaller, and, as of the second half of 2017, ranged from 20 to 25KB per block (Etherscan.io, n.d.-a). As of December 2017, the total size of the Ethereum database was 40GB. However, during the first five months of 2018, it grew much faster to 75GB (Etherscan.io, n.d.-c). Block times and block size determine how fast the blockchain database grows, which must be considered when designing a blockchain. Another consequence is that the blockchain is not designed to store large amounts of data, such as text documents, pictures, and videos. These types of data must remain off chain while the hashes representing these data files that ensures their integrity can be stored on the chain". (BRAUN-DUBLER, *et ali,* 2020, p. 66)

é um ponto relevante. Em vários casos, o NFT aponta para um destino fora da *blockchain*, onde a obra digital encontra-se hospedada. Isso pode implicar certas fragilidades, como nas hipóteses de o servidor onde a criptoarte está ser desligado[234], sofrer um ataque que deixe o acesso indisponível[235] ou ainda haver uma modificação do arquivo externo[236]. Por outro lado, ao usar a tecnologia *blockchain,* o NFT terá capacidade de registar todas as transações realizadas, contando essa informação com a segurança própria da cadeia de blocos contra adulterações[237].

Feitas essas explicações básicas sobre as características técnicas da *blockchain* e dos NFTs, é preciso agora analisar os aspectos jurídicos e econômicos relativos aos Direitos Autorais. Isso será fundamental para que seja possível compreender

---

234 "Another digital art marketplace, SuperRare, stores a hash of the digital art piece directly in the token on the smart contract. Other digital art marketplaces keep the art stored in a file that exists off the Ethereum blockchain, and the token keeps a record of who owns that file. With SuperRare, the art is in the token itself, so when someone buys a token, the art will continue to exist even after someone has stopped maintaining the external server. SuperRare has also focused more heavily on developing a social context for the owned items by creating a digital art social media space rather than simply a marketplace. As their website indicates, "collecting is inherently social," and part of the value of owning art is having the ability to display it in a collection or gallery. Thus, SuperRare creates the ability to share an art collection on the website and in virtual reality galleries". (FAIRFIELD, 2021, p. 28)

235 "Denial of servisse (Availability)

• The NFT data may become unavailable if the asset is stored outside the blockchain.

• Using the hybrid blockchain architecture with weak consensus algorithm.

Denial of Service (DoS). DoS attack is a type of network attacks in which a malicious attacker aims to render a server unavailable to its intended users by interrupting the normal functions. DoS violates the availability and breaks down the NFT service, which can indeed be used by unauthorized users.

Fortunately, the blockchain guarantees the high availability of user's operations. Legitimate users can use the required information when needed and will not lose data resources due to accidental errors. However, DoS can also be used to attack the centralized web applications or the raw data outside the blockchain, resulting in denial-of-service to NFT service. Recently, a new hybrid blockchain architecture with weak consensus algorithm was proposed, by which this architecture solves the availability issues using two algorithms". (WANG *et alli*, 2021, p. 9 e 10)

236 "Tampering refers to the malicious modification of NFT data, which violates integrity. Assume that the blockchain is a robust public transaction ledger and a hash algorithm is preimage resistance and second preimage resistance. The metadata and ownership of NFTs cannot be maliciously modified after the transaction is confirmed. However, the data stored outside blockchain may be manipulated. Therefore, we recommend users to send both the hash data as well as the original data to the NFT buyer when trading/exchanging NFT-related Properties". (WANG *et alli*, 2021, p. 9)

237 "In a blockchain system, each block has a limited capacity. When the capacity in one block becomes full, other transactions will enter a future block linked to the original data block. In the end, all linked blocks have created a long-term history that remains permanent. The NFT system, in essence, is a blockchain-based application. Whenever an NFT is minted or sold, a new transaction is required to send to invoke the smart contract. After the transaction is comfirmed, the NFT metadata and ownership details are added to a new block, thereby ensuring that the history of the NFT remains unchanged and the ownership is preserved". (WANG *et alli*, 2021, p. 6)

posteriormente a interação entre os temas, especialmente as consequências de se considerar como originais as obras certificadas pelos non-*fungible tokens.*

2 Direitos autorais

2.1 Conceito e Escopo

Os Direitos Autorais são uma espécie de Propriedade Intelectual, sendo esta composta pelas normas voltadas à proteção de certas criações intelectuais. O gênero ainda abrange a Propriedade Industrial, as Cultivares e as Topografias de Circuitos Integrados. Para melhor compreensão sobre o escopo dos Direitos Autorais, é importante fazermos uma breve explicação a respeito das demais espécies de Propriedade Intelectual, uma vez que cada uma delas é voltada à tutela de um determinado tipo de criação. Isso é especialmente relevante porque, como se verá mais adiante, a legislação brasileira não apresenta um rol taxativo em relação às hipóteses que estão sujeitas à proteção e regras específicas do Direitos Autorais. Assim, entender o objeto de cada espécie de Propriedade Intelectual ajuda, por exceção, a delimitar o alcance dos Direitos Autorais em diversos casos, considerando a especificidade de cada norma.

A Propriedade Industrial está prevista na Lei 9.279/96 e se divide em quatro espécies: patentes, desenhos industriais, marcas e indicações geográficas. As patentes protegem criações de escopo tecnológico, assim entendidas, neste caso, como aquelas que interferem ou interagem com as forças da natureza[238], gerando resultados diferenciados por meio de produtos ou processos passíveis de reprodução no ambiente industrial[239]. Na legislação brasileira, se dividem em invenções e modelos de utilidade, sendo as primeiras aplicáveis a processos industriais ou produtos que representem inovações de caráter disruptivo, enquanto os últimos são aperfeiçoamentos consistentes na modificação do formato de objetos pré-existentes, de modo a gerar-lhes alguma melhoria funcional[240]. Para ilustrar melhor a diferença

---

238 "Invento é uma solução técnica para um problema técnico. Essa a noção que deriva do texto constitucional. Invenção é a criação intelectual maior, objeto da patente de invenção, à qual, tradicionalmente, se concede prazo maior e mais amplidão de proteção. Assim, invento é termo genérico, do qual invenção é específico. A proteção, assim, se volta para uma ação humana, de intervenção na Natureza, gerando uma solução técnica para um problema técnico. Não têm proteção, mediante patentes, a simples descoberta de leis ou fenômenos naturais, as criações estéticas ou as criações abstratas (não técnicas), como planos de contabilidade, regras de jogo ou programas de computador. [...] Assim, não é invento a criação que não é técnica – se for abstrata, ainda que economicamente relevante, ou se for artística não satisfará o requisito de ser invento." (BARBOSA, 2003, p. 337 e 346)

239 "Como é sabido, as patentes possuem como fundamento a ideia de impulsionar o progresso técnico-industrial, fomentando a realização e a divulgação de invenções. Essas, por sua vez, consistem em regras para a ação humana e são o resultado de um processo criador humano, pressupondo a apresentação de um problema e a determinação de meios para solucioná-lo. Mais concretamente, em toda invenção são formuladas uma ou várias regras que indicam os meios técnicos cujo uso permite alcançar um resultado também técnico. Desta maneira, a técnica e o método constituem componente essencial da invenção, sendo como esta, obtido um resultado ou finalidade técnica industrial através de meios técnicos, isto é, de meios que atuam sobre as forças da Natureza." (ASSAFIM, 2005, p. 19 e 20)

240 Artigos 8º e 9º da Lei 9.279/96.

entre as espécies de patente: quando o avião foi criado, poderia ser considerado como uma invenção, para fins de patenteabilidade, uma vez que apresentava uma solução técnica totalmente distinta da que existia na época. Naquele momento, o voo era realizado por meio de balões e dirigíveis, que funcionavam com o uso de gases mais leves que o ar. Já o avião surgiu como um aparelho mais pesado que o ar e que, mesmo assim, era capaz de sair do chão sem depender de infláveis. A invenção fica configurada neste exemplo, uma vez que a inovação tecnológica não se deu em função da mudança do formato do produto existente, mas sim por meio de uma solução técnica totalmente nova. Já os aperfeiçoamos feitos no avião que envolvam alterações na forma de seus componentes, como hélices e asas, se enquadram como modelos de utilidade.

Já os desenhos industriais (DI) protegem criações de natureza estética, materializadas no formato de produtos ou padrões de linhas e cores que possam ser aplicados na superfície daqueles. Porém, é importante ressaltar que essa espécie de Propriedade Intelectual não se aplica a obras de caráter puramente artístico, nos termos do artigo 98 da Lei 9.279/96. Assim, o aspecto industrial referente à possibilidade de reprodução em massa do objeto estético deve estar presente para seu enquadramento como um DI, em que pese esse tipo de direito não tutelar nenhum elemento funcional da criação[241]. Com isso, formatos inovadores de produtos e embalagens, naquilo que não se relacionem com nenhum tipo de funcionalidade prática, podem ser protegidos por meio de registo de desenho industrial. O mesmo se aplica a estampas e outras configurações visuais que possam ser aplicadas na superfície dos produtos.

As marcas são sinais distintivos visualmente perceptíveis[242], de acordo com o conceito jurídico previsto na Lei 9.279/96243. Vale destacar, porém, que essa definição pode variar de diversas formas. No próprio campo do Direito, há países cuja legislação marcária permite a proteção de sinais percebidos por outros sentidos que não a visão. Nos Estados Unidos, por exemplo, é possível registar marcas sonoras, gustativas, olfativas ou táteis, além de sinais visualmente perceptíveis.

Ainda é importante destacar que outros ramos do conhecimento também se dedicam ao estudo do assunto, inclusive com abordagens e conceitos distintos dos que são adotados no âmbito do Direito. Nesse sentido, Carlo Fernandez-Novoa indica que uma das funções da marca é constituir um mecanismo para representar o valor intangível (reputação ou *goodwill)* dos produtos e serviços por ela identificados:

> En términos generales, cabe señalar que el *goodwill* es la buena fama o reputación de que gozan los produtos o servicios diferenciados a través de uma marca. Esta buena fama implica la preferencia o el reconecimiento que el publico de los consumidores manifiesta em relación com los produtos o

241 "Considera-se desenho industrial a configuração ornamental externa de um produto industrial ou um padrão gráfico aplicado a um produto. Os desenhos industriais protegem o design externo de um produto, independentemente de seu funcionamento, isto é: a forma externa é protegida pelo registro de desenho industrial, o funcionamento do objeto é protegido por patente". (GUIMARÃES, 2005, p. 25)

242 A obrigatoriedade de o sinal ser percebido pela visão como condição para o registro marcário é uma exigência da legislação brasileira, podendo esse requisito variar de acordo com o país.

243 Artigo 122 da Lei 9.279/96.

> servicios correspondientes. Así concebido, el *goodwill* es algo intangible que existe tan sólo em la mente del público comprador: es el estado de ánimo de los consumidores que induce a los mismos a comprar um determinado produto o contratar um certo servicio. (NOVOA, 1978, p. 56)

Contudo, por essa perspectiva, a marca seria composta então por todas as mensagens e experiências que transmite ao público consumidor, o que vai determinar sua reputação. Essa linha é própria de ciências como a Comunicação, Administração e Economia, extrapolando o conceito jurídico previsto no artigo 122 da Lei 9.279/96, que indica ser um "sinal distintivo visualmente perceptível, não compreendido nas proibições legais" e cuja função primordial é diferenciar produtos e serviços dos seus concorrentes no mercado. Tais sinais podem se constituir como nomes e figuras, utilizados de forma conjugada ou isolada.

Assim como as marcas, as indicações geográficas (IGs) também são espécies de sinais distintivos. Porém, não se confundem com aquelas, sobretudo porque são obrigatoriamente constituídas por um nome geográfico, que aponta a origem de determinado produto ou serviço. As IGs são, ainda, um direito de natureza essencialmente coletiva, na medida em que se configuram como uma prerrogativa exclusiva dos produtores locais quanto ao uso do sinal para indicar o local originário de produção.

Ainda relativamente incipientes no Brasil, as indicações geográficas são largamente utilizadas na Europa. Seu exemplo mais conhecido é a região de Champagne, na França, mundialmente famosa pela produção de vinhos espumantes.

As cultivares, por sua vez, protegem melhoramentos vegetais. Reguladas pela Lei 9.456/97, são, basicamente, modificações genéticas introduzidas em um vegetal. Este deverá possuir alguma nova característica oriunda dessa intervenção, alem de se mostrar capaz de transferi-la a novas gerações da mesma planta em uma escala de produção industrial. No Brasil, seu uso é observado especialmente em vegetais como soja e milho, cujas variações podem implicar em melhorias em relação à resistência a pragas, maior produtividade ou safras precoces, por exemplo. Importante destacar que a proteção legal das cultivares somente se aplica a inovações promovidas por meio da alteração da genética do vegetal, não sendo abarcadas técnicas que alterem características das plantas por outros meios[244].

As topografias de circuitos integrados estão previstas na Lei 11.484/07, sendo essencialmente voltadas para criações na área da eletrônica. Seu objeto de proteção são configurações relacionadas à condução de corrente elétrica em componentes que visam a transmissão, armazenamento e processamento de informações. Os projetos nesse campo podem inclusive otimizar a performance dos circuitos e reduzir o seu consumo energético, gerando vantagem competitiva para seus titulares.

Por fim, dentro dessa contextualização das espécies de Propriedade Intelectual, temos ainda os Direitos Autorais, que serão o foco deste trabalho. Sobre isso, é importante destacar inicialmente que, no Brasil, os Softwares estão contidos nesses

[244] Como os casos da melancia quadrada e morango em formato de coração, que são obtidos por meio de técnicas de contenção da fruta em moldes, durante seu crescimento (https://segredosdomundo.r7.com/melancia-quadrada/ e https://www.bbc.com/portuguese/ciencia/2010/01/100121_australiamorangosml). Tais casos não se enquadram na legislação de cultivares.

direitos[245] e não são uma espécie autônoma de Propriedade Intelectual, em que pese terem uma regulamentação própria por meio da Lei 9.609/98[246]. Para os temas que não tenham sido tratados nessa norma, aplicam-se aos programas de computador as regras gerais dos Direitos Autorais, nos termos da Lei 9.610/98.

A legislação indica que as "criações do espírito" serão protegidas com base nas normas dos Direitos Autorais. A Lei 9.610/98 indica uma lista de obras que se enquadram nesse conceito, porém trata-se de um rol meramente exemplificativo[247]. Assim, é importante compreender a essência do termo "criações do espírito", para o entendimento adequado sobre o alcance da legislação de Direitos Autorais.

Essa expressão foi cunhada a partir da percepção de que as criações autorais teriam uma relação muito forte com a personalidade do criador[248], de modo que o resultado desse tipo de atividade criativa seria uma representação do próprio "espírito" do autor[249]. Nessa linha, por exemplo, um pintor que passasse por uma fase difícil em sua vida poderia refletir isso nos seus quadros, que provavelmente adotariam temas tristes, cores escuras e outros elementos relacionados ao momento do artista. A visão de mundo deste seria determinante para o resultado da sua atividade criativa, que seria marcada pelos seus gostos e influências. Por essa lógica, a obra nada mais seria senão o resultado da projeção da própria personalidade do autor materializada concretamente em algum tipo de suporte, como um quadro, livro ou outro meio similar:

> A inserção do elemento psíquico próprio é que faz a criação intelectual; o escriba, ou o datilógrafo, ou o gravador, inseriu no material ideia de outro, ou, mais precisamente, a expressão, a forma, da ideia de outrem. [...] Para que haja criação duradoura é preciso que se dê, no plano do mundo fático, a especificação, que entre no mundo jurídico, como fato expressivo da nova *species*, com eficácia de atribuição de propriedade ao especificador. [...] A personalidade mesma estedeu-se até aí, incorporando psique na matéria. (PONTES DE MIRANDA, 2002, p. 47 e 63)

Na mesma linha, que é fortemente influenciada pelo viés artístico relacionado ao tema, as obras, além de geradas pelo "espírito" do criador, somente podem ser captadas pelo "espírito" de uma pessoa:

> [A] obra literária ou artísitca pertence ao mundo da cultura. Só se capta através do espírito. Um animal é completamente

---

[245] Tal enquadramento está alinhado com o artigo 10.1 do Acordo TRIPs (*Trade Related Intellectual Property Rights Agreement*), que dispõe: "Programas de computador, em código fonte ou objeto, serão protegidos como obras literárias pela Convenção de Berna (1971)".

[246] Artigo 7º, XII e parágrafo primeiro da Lei 9.610/98.

[247] Artigo 7º da Lei 9.610/98.

[248] "O direito de autor é fundado na criação da obra de engenho ou obra intelectual, denominada criação do espírito, na qual ele projeta muito de sua personalidade, razão de haver duas vertentes na composição desse direito: direitos morais – direitos da personalidade – e direitos patrimoniais". (CHINELLATO, 2015, p. 298)

[249] "[O] modo de expressão das ideias é parte da mente de um autor e pertence apenas a ele, o que torna o plágio e a pirataria errados. Nesse mesmo sentido, as proporções de trabalho e habilidade de uma pessoa são maneiras de externar a totalidade de sua personalidade". (PONTES, 2013, p. 85)

> opaco à obra literária ou artística, só chegando à percepção de manifestações físicas dispersas, como cores, sons ou movimentos. Logo, todo o Direito de Autor é necessariamente Direito da Cultura. (ASCENSÃO, 2007, p. 27 e 28)

Já as demais espécies de Propriedade Intelecutal, em tese, não sofreriam tanta influência do "espírito" do autor, apesar de não estarem completamente alheias a isso, evidentemente. O enfoque no vínculo entre a criação e seu autor seria menor porque tutelariam criações condicionadas também por outros fatores. As patentes, como já explicado, se aplicariam no caso de soluções técnicas obtidas a partir da interferência sobre as forças da natureza, que são elementos externos à personalidade do criador. Mesmo espécies de Propriedade Industrial que contém componentes estéticos, como o desenho industrial e a marca, são influenciados por aspectos que não se relacionam diretamente com o "espírito" do autor. Isso porque, nesses casos, o foco estará na percepção do consumidor a quem o produto ou serviço se destina e como tais elementos visuais podem influenciar na sua decisão de compra. Tecnicamente, uma marca de um restaurante, por exemplo, deve ser constituída por cores, formas e expressões que despertem o apetite do cliente em potencial, para estimulá-lo ao consumo do bem vinculado àqueles sinais. Essa é mais uma questão que não passa pela personalidade do autor, uma vez que as referências a serem observadas para criação da marca estão no público consumidor que se pretende atingir.

Evidentemente, essa explicação a respeito do conceito de "criações do espírito" não significa uma regra absoluta e nem que hoje toda ou qualquer obra protegida pelos Direitos Autorais tem perfeita correspondência com todos os aspectos da personalidade do autor. A própria Lei, já em 1998, incluía entre as criações tuteladas os bancos de dados, que certamente não são influenciados por essa perspectiva em termos criativos. Na mesma linha, há a questão referente à possibilidade de criações oriundas de inteligência artificial, sobretudo na medida em que esta, em sua vertente "forte", poderia até mesmo aprender a desenvolver novas coisas, para além de uma determinada tarefa para a qual tenha sido originalmente concebida:

> Além da própria definição de inteligência artificial, há outros termos técnicos que também devem ser considerados. Por exemplo, a diferença entre IA forte (wide) e fraca (narrow). Esta última é aquela que se limita a desenvolver uma ou mais atividades específicas para as quais foi programada, como uma máquina industrial especializada na produção de determinado componente, ou um programa de computador para jogar determinado game. Diversamente, IA forte é aquela capaz de desenvolver variadas atividades e, inclusive, "aprender" a fazer coisas novas ao longo do tempo. Quanto mais especializada for a aplicação de IA, em tese mais eficiente ela será, suplantando facilmente a capacidade de um ser humano na execução da mesma tarefa. Por outro lado, no estágio atual de desenvolvimento dessa tecnologia, ainda não existe uma IA forte o suficiente para se adequar a praticamente qualquer tarefa e ter "consciência" do que faz, tal como o ser humano. Se algum dia esse estágio de desenvolvimento tecnológico for alcançado, a literatura especializada sugere chamá-lo de singularidade ou superinteligência (PARENTONI, VALENTINI e ALVES, 2020, p. 10).

Logicamente, em tese tal possibilidade pode envolver até mesmo a criação de conteúdos previstos na legislação de Direitos Autorais, o que seria uma situação

absolutamente estranha ao conceito histórico de "criações do espírito". Considerando que a tecnologia hoje consegue gerar resultados como reproduzir a voz de um cantor falecido e "fazê-lo" gravar uma música que ele nunca interpretou[250], a questão do "espírito" de fato parece não alcançar todas as situações que podem gerar conteúdo protegido.

Neste trabalho, não se pretende discutir a possibilidade (ou não) de aplicação de direitos autorais sobre criações oriundas de inteligência artificial. Contudo, vale ressaltar que o tema é polêmico e que, no início de 2022, o Escritório Norte-Americano de Direitos Autorais (United States Copyright Office - USCO) rejeitou um pedido de proteção para uma arte desenvolvida totalmente por meio de inteligência artificial, por entender que não é possível esse tipo de tutela para objetos que não tenham sido fruto de autoria humana[251]. Na mesma linha, mesmo antes de a discussão sobre a proteção de criações oriundas da inteligência artificial se expandir, o autor português José de Oliveira Ascensão já se posicionava contra a tutela autoral em casos similares:

> Se o resultado final é previsível e quem opera o computador se dirige à caracterização de uma determinada ideia criadora – o vínculo de autoria individual não é posto em causa. O computador funciona então como um instrumento, tal como o pincel nas mãos do pintor. Terá quanto muito uma função acessória na criação: complementará uma ideia-base, mas é ancilar dessa ideia. O resultado não deixa de ser previsto e intencionalmente prosseguido pelo operador. Este e somente este é o autor, e as regras normais de autoria não são afetadas. Diferente é a situação quando se atinge um grau de indeterminação que escapa a todo o controle ou previsão do operador. Isto é tornado possível através de programas adequados. O operador pode programar a produção de um resultado cujos parâmetros determina, mas não pode prever o conteúdo desse mesmo produto. Neste caso, não há um direito do operador sobre o resultado produzido. A criação intelectual é a criação individualizada; é a expressão de uma ideia, que tem necessariamente de se antever com um conteúdo específico. Não é equivalente ao ato de pôr em funcionamento uma máquina de que derivam produtos indiscriminados. (ASCENSÃO, 2007, p. 664 e 664)

De toda forma, essa expressão vinculada à personalidade do autor é um conceito orientativo e não exauriente, que auxilia especialmente na avaliação de hipóteses não previstas expressamente na Lei 9.610/98 e sua eventual subordinação às regras dos Direitos Autorais. A essa abordagem devem ser acrescentados outros elementos para uma análise mais precisa de cada caso. São exemplos de critérios complementares nesse sentido a lista de hipóteses expressamente excluídas da proteção dos Direitos Autorais pela legislação[252], as criações já contempladas por outras espécies de Propriedade Intelectual[253] e a distinção entre expressões protegidas e concepções meramente abstratas.

---

250 https://www.tecmundo.com.br/software/211146-programa-tv-sul-coreano-recria-voz-cantor-morto-ha-25-anos.htm

251 A decisão administrativa (em fase recursal) pode ser acessada em https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf .

252 Artigo 8º da Lei 9.610/98.

253 Em que pese haver alguma divergência doutrinária em relação a isso, na medida que há autores que defendam a possibilidade de dupla ou tripla proteção para certos tipos de criação, especialmente no campo estético. Nesse sentido, poderia haver, em tese, uma aplicação cumulada dos Direitos Autorais, Desenhos Industriais e Marcas. A esse respeito: SILVEIRA, 2005. Em sentido contrário: "O interessado tem, pois, aa opção do ramo do Direito a que recorre para a sua tutela. E pode recorrer cumulativamente a

Esse último ponto é especialmente relevante não apenas para a questão dos Direitos Autorais, mas para todo o estudo da Propriedade Intelecutal. De um modo geral, a proteção jurídica aqui não recai sobre ideias abstratas, mas sim à sua efetiva concretização no mundo real, por meio da atividade intelectual do criador. Não basta simplesmente imaginar uma criação, sendo necessária a sua materialização por meio de um detalhamento quanto ao funcionamento de uma solução técnica (especialmente no caso das Patentes, Cultivares e Topografias de Circuitos Integrados) ou uma descrição das características concretas no caso de uma expressão artística (o que abrange as criações de fundo estético, inclsuive as protegidas por meio dos Direitos Autorais).

Assim, ideias em abstrato não gozam de proteção jurídica no âmbito da Propriedade Intelectual, mas sim o caminho desenvolvido pelo criador por meio de seu intelecto. Importante destacar que essas condições se encontram especialmente previstas na Lei de Direitos Autorais brasileira, sobretudo nos artigos 7º (que determina expressamente, em seu caput, a necessidade de as obras terem sido efetivamente experssas de alguma forma como uma das condições para haver proteção no âmbito dos Direitos Autorais) e 8º, I (que veda a proteção de ideias)[254].

Uma vez que o presente texto busca debater aspectos dos Direitos Autorais sobre arte digital, é fundamental esclarecer que a exteriorização da criação (condição necessária para que haja proteção autoral) não siginifica que esta se dê obrigatoriamente em um suporte físico/concreto[255]. Qualquer forma de apresentação é válida, desde que possa ser percebida pelas pessoas[256]. No caso da cripoarte, essa questão é crucial, pois o fato de a exteriorização da criação se dar em meio digital não invalida sua condição de criação protegida pelos Direitos Autorais[257]. É especialmente

ambos? Embora o ponto seja duvidoso, inclinamo-nos para a resposta negativa. Cada qualificação traz um sistema completo de proteção. Impressiona-nos particularmente a latitude que tem a tutela pelo Direito de Autor, o que parece tornar desproporcionado ainda o acrescento que fosse tirado de outro ramo do Direito". (ASCENSÃO, 2007, p. 415)

254 "A dicotomia ideia/expressão é precisamente o que define o escopo da tutela do direito de autor (expressão) daquilo que faz parte do domínio público (ideias), sob o qual não incide a proteção jurídica. Em outras palavras, a reprodução da expressão de algum autor exige sua permissão prévia e expressa, enquanto a abordagem acerca de uma ideia de um autor não depende de qualquer autorização, eis que domínio público". (PONTES, 2013, p. 14)

255 "De fato, é relevante mencionar que só são protegidas as obras que tenham sido exteriorizadas. As ideias não são passíveis de proteção pelos direitos autorais. No entanto, o meio em que a obra é expressa tem pouca ou nenhuma importância, exceto para se produzir prova de sua criação ou de sua anterioridade, já que não se exige exteriorização da obra em determinado meio específico para que, a partir daí, passe a existir o direito autoral. Ou seja, este existe desde o momento em que a obra é exteriorizada, independentemente do meio". (PARANAGUÁ e BRANCO, 2009, p. 23 e 24)

256 "De fato, a criação do espírito não pode permanecer no foro íntimo. Tem que se exteriorizar ou manifestar por meio que seja captável pelos sentidos. Esta exteriorização pode realizar-se das mais diversas maneiras, e os avanços técnicos permitem cada dia descobrir novos processos de expressão de criações do espírito". (ASCENSÃO, 2007, p. 30)

257 "Nos dias de hoje, é assente que o reconhecimento de uma obra de arte está diretamente relacionado à conscientização acerca do valor que se tem impregnado nela, seja pelo aspecto material ou estético, seja pela notoriedade do autor ou, ainda,

importante destacar essa questão, uma vez que a legislação brasileira sobre Direitos Autorais é do final dos anos 1990, não fazendo nenhuma referência a esse tipo de obra. Porém, esse fato não afasta a proteção autoral, inclusive porque a aplicação da Lei precisa se adaptar às mudanças fáticas que naturalmente surgem e ainda surgirão ao longo do tempo, ainda que tais situações concretas sequer passassem pela mente do legislador quando a norma foi editada. Justamente em função disso, a própria legislação indica técnicas para solucionar casos omissos, como a aplicação da analogia, dos costumes e dos princípios gerais de Direito, como previsto no artigo 4º da Lei de Introdução às Normas do Direito Brasileiro (Decreto-Lei 4.657/42)[258].

Exemplo nesse sentido pode ser observado no campo do Processo Civil. A dinâmica de informatização das ações judiciais gerou um debate a respeito de os arquivos eletrônicos poderem (ou não) ser considerados como documentos para fins de instrução processual. É inegável que a própria existência desse tipo de discussão se deve em grande parte pelo fato de se estar analisando a aplicação de uma legislação concebida a partir de uma realidade de documentação em papel em um mundo que agora se torna cada vez mais informatizado e digital. No caso, deve-se destacar que essa questão se assentou com o reconhecimento da validade dos documentos eletrônicos:

> [D]o ponto de vista teórico nada impede que um arquivo de computador seja considerado como documento em sentido técnico-jurídico. O que se deve frisar é que a prova documental é sempre uma prova *material*, pois deve estar gravada em um bem corpóreo. Pondera-se, apenas, que esse suporte material não precisa ser, necessariamente, o papel, admitindo-se também a mídia digital, caso em que se terá um documento eletrônico. [...] Países como Itália, Alemanha e Estados Unidos estão em estágio avançado de reconhecimento jurídico do documento eletrônico, contando com amplo apoio da doutrina local e dos governantes. A União Européia, inclusive, dispõe de Diretiva atribuindo-lhe valor jurídico em todos os países membros. (PARENTONI, 2007, p. 21 e 22)

Tal posição que será especialmente relevante para nossa análise sobre o que pode ser considerado exemplar original de uma criptoarte, o que será feito mais adiante no presente trabalho.

Outro elemento importante presente na legislação brasileira de Direitos Autorais é sua submissão a um regime declaratório[259-260], em contraposição ao regime atributivo

---

pela técnica utilizada. Uma obra de arte não depende, exclusivamente, do *corpus*, da substância material que a compõe". (LUCCA e PARENTONI, 2015, p. 389)

258 "NFTs provide a case for establishing strong digital personal property interests. The token is personal property. Whatever a court decides about the relationship between the token and any related intellectual property, it cannot avoid the fact of the token. The token grounds the property interest online just as the physical copy grounds it offline. Something must be done with it, and courts will choose to treat it as personal property". (FAIRFIELD, 2021, p. 97)

259 "Ato constitutivo: são aqueles que criam uma nova situação jurídica individual para seus destinatários. Ato declaratório: são aqueles que visam declarar a existência de uma situação de fato ou de direito preexistente". (CANÇADO, 2004, p. 60)

260 "Ato constitutivo é aquele pelo qual a Administração cria, modifica ou extingue um direito ou uma situação do administrado. [...] Ato declaratório é aquele em que a

ou constitutivo que normalmente se aplica no caso das outras espécies de Propriedade Intelectual[261]. Nesse sentido, a proteção decorrente dos Direitos Autorais não surge de nenhum ato estatal de concessão, mas sim da própria atividade criativa. No momento em que autor materializa sua criação, esta gozará de proteção jurídica, caso se trate de um objeto contido no escopo dos Direitos Autorais. Logo, nesse âmbito, nenhum tipo de registo cria qualquer direito[262], sendo que tal formalidade é facultativa e utilizada apenas como um meio de prova de autoria[263].

A adesão a essa sistemática declaratória está alinhada com a Convenção da União de Berna, que é o primeiro tratado internacional referente aos Direitos Autorais, formalizado em 1886 e vigente até hoje, com revisões realizadas ao longo do tempo. A CUB é a base do Sisitema Unionista, que também tem como caracterísitca a previsão de dois eixos distintos de prerrogativas em prol do autor: um de aspecto extrapatrimonial, dedicado a valorizar a pessoa do autor por meio de direitos de natureza não econômica e outro de caráter utilitarista, relacionado ao direito de exclusividade sobre o material[264]. Os primeiros são chamados de direitos morais, enquanto os segundos são nomeados de direitos patrimoniais.

Os direitos morais são inalienáveis e irrenunciáveis. Estão atrelados à figura do autor, que é quem efetivamente cria a obra[265]. e não podem ser transferidos a terceiros por ato de vontade. A única hipótese de seu exercício por outras pessoas refere-se à possibilidade de atuação dos herdeiros, após o falecimento do autor, no que diz respeito a algumas das prerrogativas contidas no rol dos direitos morais[266]. Entre estes, destacam-se a obrgação de indicação correta de autoria em qualquer uso da obra

---

Administração apenas reconhece um direito que já existia antes do ato". (DI PIETRO, 2006, p. 234 e 235)

261 No regime constitutivo, não basta o ato de criação para que haja direitos de Propriedade Intelectual. É necessário também observar as formalidades de requisição da proteção ao Poder Público e concessão, por parte deste, do direito. No Brasil, é esse sistema que opera como regra nos casos da Propriedade Industrial, Cultivares e Topografias de Circuitos Integrados. Existem exceções nesse âmbito, contudo. As marcas de entidades desportivas, por exemplo, são protegidas independente de registro, conforme previsão da Lei 9.615/98. E existe controvérsia, no caso das Indicações Geográficas, se estas se submetem a um regime declaratório ou constitutivo de direitos (MELO, 2019).

262 Com a possível exceção, no âmbito dos Direitos Autorais, às criações de natureza arquitetônica. Isso porque a Lei 12.378/10, que criou o Conselho de Arquitetura e Urbanismo, previu um ato de registro de projetos e demais trabalhos junto ao CAU para fins de comprovação de autoria, sem deixar claro, entretanto, se tal providência é obrigatória ou facultativa para fins de existência dos Direitos Autorais. Isso vem causando, desde então, dúvidas a respeito da aplicação ou não do sistema declaratório de direitos para esse tipo de criação.

263 Artigos 18 e 19 da Lei 9.610/98.

264 "Com efeito, por meio da Convenção de Berna, os países unionistas comprometeram-se a criar e/ou regulamentar, em seus territórios nacionais, legislações especiais que obedecessem aos princípios ali acordados. O principal deles é o respeito não só aos direitos patrimoniais de autor, mas também e principalmente aos direitos morais, enquanto garantia de manutenção da vontade do autor e de sua ligação intrínseca, subjetiva e personalíssima com a obra criada". (MENEZES, 2007, p. 31)

265 Artigo 11 da Lei 9.610/98.

266 Artigo 24 da Lei 9.610/98.

(crédito de paternidade) e possibilidade de oposição contra quaisquer modificações ou prática de atos no uso do material que possam prejudicar ou atingir o autor em sua reputação ou honra (direito de integridade).

Já os direitos patrimoniais consistem no poder de exclusão detido pelo seu titular, no sentido de ser juridicamente capaz de impedir que outras pessoas utilizem o conteúdo protegido. São prerrogativas de exclusividade temporária, de modo que, durante a sua vigência, qualquer uso da obra precisa ser autorizada, salvo nas exceções previstas na legislação. No Brasil, a regra geral é que os direitos autorais patrimoniais duram 70 anos, contados de 1º de janeiro do ano seguinte à morte do autor[267]. No caso de co-autoria, esse prazo somente se inicia após o falecimento do último dos co-autores. Essas regas estão previstas nos artigos 41 e 42 da Lei 9.610/98.

Os direitos patrimoniais podem ser cedidos, desde que observadas certas formalidades e restrições previstas na legislação. No caso de transferência definitiva de direitos, a Lei 9.610/98 determina a necessidade de cláusula escrita nesse sentido, nos termos dos artigos 49, II e 50 da LDA. Além disso, o artigo 4º dessa legislação indica que os negócios jurídicos envolvendo direitos autorais devem ser interpretados restritivamente, o que significa uma aplicação favorável ao autor no caso de omissões ou contradições no texto do contrato, uma vez que não é possível ampliar suas disposições para alcançar situações que não estejam expressamente autorizadas. Também é importante notar que é vedada a cessão de direitos autorais no caso de certas atividades profissionais criativas, em função de disposições previstas na legislção específica de cada profissão regulamentada. São exemplos nesse sentido os profissionais das artes cênicas[268] (Lei 6.533/78 e Decerto 82.385/78) e radialistas (Lei 6.615/78).

Para os fins do presente trabalho, duas disposições referentes aos direitos patrimoniais merecem destaque, especialmente por se aplicarem a questões de venda ou revenda de "original" de uma obra:

> Lei 9.610/98
>
> Art. 37. A aquisição do original de uma obra, ou de exemplar, não confere ao adquirente qualquer dos direitos patrimoniais do autor, salvo convenção em contrário entre as partes e os casos previstos nesta Lei.
>
> Art. 38. O autor tem o direito, irrenunciável e inalienável, de perceber, no mínimo, cinco por cento sobre o aumento do preço eventualmente verificável em cada revenda de obra de arte ou manuscrito, sendo originais, que houver alienado.
>
> Parágrafo único. Caso o autor não perceba o seu direito de sequência no ato da revenda, o vendedor é considerado depositário da quantia a ele devida, salvo se a operação for realizada por leiloeiro, quando será este o depositário.

[267] As exceções são as obras anônimas, pseudônimas, fotográficas e audiovisuais, cujo prazo de 70 anos começa a contar de 1º de janeiro do ano seguinte à sua primeira publicação ou divulgação, conforme artigos 43 e 44 da Lei 9.610/98.

[268] Apesar de a Lei 6.533/78 dispor genericamente em sua ementa sobre "profissões de Artistas e de técnico em Espetáculos de Diversões", o Decreto 82.385/78 indica efetivamente as atividades alcançadas por essas regras, que se aplicam no âmbito de atividades de teatro, dança, circo e audiovisual. Nesse sentido, a proibição de cessão de direitos autorais patrimoniais prevista nessas normas não alcança automaticamente outros tipos de artistas, especialmente os que têm regulamentação própria, como é caso dos músicos, regidos pela Lei 3.857/60, por exemplo.

Como será debatido mais adiante, dada a natureza das obras de criptoarte comercializadas por meio de NFTs, é importante avaliar se tais materiais podem ser considerados "originais" para os fins das disposições acima, sobretudo porque, no momento de promulgação da atual LDA (em 1998), não havia esse tipo de tecnologia aplicada às artes visuais da maneira como se tem percebido agora. É fácil concluir que, naquela época, a concepção de original de obra de arte estava ligada à ideia de um objeto físico. A questão então é avaliar se esse conceito poderia ser aplicado aos novos modelos de negócio e mercados envolvendo os NFTs, nos dias de hoje. Para essa análise, porém, é importante entender primeiro algumas questões de fundo econômico referentes às próprias prerrogativas de exclusividade contidas nos Direitos Autorais.

2.2 Efeitos Econômicos dos Direitos Autorais: escassez artificial

Os Direitos Autorais, assim como toda a Propriedade Intelectual, lidam com ativos intangíveis[269]. Ainda que as criações se materializem em produtos físicos, o que se protege aqui é a concepção intelectual, que não se confunde com sua representação tangível.

A partir dessa perspectiva, é importante analisar o assunto do ponto de vista da Ciência Econômica. Nesse sentido, três características são necessárias para que um

[269] "Do direito romano nos vem uma grande divisão, que distribui todos os bens em dois grandes grupos, o das chamadas coisas corpóreas e coisas incorpóreas, tendo em vista, segundo Gaio, a possibilidade de serem ou não tocados. [...] O critério distintivo básico era a tangibilidade ou possibilidade de serem tocadas, o que, no estado atual da ciência, seria inexato, por excluir coisas perceptíveis por outros sentidos, como os gases, que não podem ser atingidos materialmente com as mãos, e nem por isso deixam de ser coisas corpóreas. Das coisas corpóreas ou tangíveis distinguem-se as incorpóreas ou intangíveis, consistentes nos direitos. [...] O interesse prático da distinção das coisas em corpóreas e incorpóreas, que no direito romano se situava na forma de transmissão, de vez que as *corporales res* deviam obedecer ao ritual da *mancipato* ou da *traditio*, enquanto que as *res incorporales* eram transferidas por outras formas, como a *in iure cessio*, no direito moderno reduziu-se, embora ainda se possa indicar. Assim é que as coisas corpóreas se transferem pela compra e venda, pela doação, etc., enquanto que as incorpóreas pela cessão. Para certos direitos que se aproximam do de propriedade, mas que não podem, com rigor, definir como direitos dominiais, a tecnologia moderna reserva a expressão *propriedade,* a que acrescenta o qualificativo *incorpórea,* e refere-se, tanto em doutrina quanto na lei, à *propriedade incorpórea*. É assim que se qualifica de *propriedade literária, científica e artística* ao direito do autor sobre sua obra; *propriedade industrial* ao direito de explorar uma patente de invenção ou uma marca de fábrica; *propriedade de um fundo de comércio* ao direito de explorar os elementos corpóreos e incorpóreos ligados ao estabelecimento mercantil". (PEREIRA, 2000, p. 256 a 258)

bem seja considerado relevante para fins econômicos: escassez[270], utilidade[271] e disponibilidade[272]. Na ausência de algum desses elementos, o objeto não terá valor econômico, assim entendido como a disposição de alguém efetivamente pagar para ter acesso àquele bem[273].

A escassez merece uma análise destacada, inclusive porque o objeto de estudo da Economia é a gestão dos recursos considerados escassos[274-275]. Nesse sentido, tal elemento deve ser entendido como uma limitação quantitativa de determinado bem, frente à demanda[276] que exista por ele. É, portanto, uma questão relativa: não se considera apenas a quantidade em termos absolutos, mas sim se ela se apresenta em montante inferior ao número desejado pelos demandantes[277]. Mesmo se determinado

---

270 "Se a coisa necessitada existe em quantidade infinita ou ilimitada, ela não é um bem econômico, pois não determina nenhuma atividade econômica no sentido de obtê-la e dela usar. A essa classe de bens, mesmo úteis, mas não-econômicos, dá-se o nome de bens livres ou gratuitos. O economista lança mão da palavra escassez ou raridade para designar essa característica dos bens econômicos, isto é, a de não serem bens livres e de exigirem uma atividade econômica a fim de serem produzidos e poderem satisfazer uma necessidade humana. A limitação, a raridade ou a maior ou menor escassez dos bens pode-se originar de alguma dessas coisas: a) da avareza da natureza, que os contém em quantidade escassa; b) do custo de produção, que torna difícil a produção e a oferta; c) da lei, que pode estabelecer restrições ou racionamento." (GALVES, 2004, p. 53 e 54)

271 "Utilidade é a aptidão da coisa ou do serviço para satisfazer uma necessidade econômica. [...] As coisas e os serviços não entram no mundo da economia, não são bens econômicos, se o homem não sente necessidade deles. O juízo afirmativo do sujeito, sobre a necessidade que tem de uma coisa ou de um serviço, é que confere a estes a qualidade de bem econômico." (GALVES, 2004, p. 53)

272 "A coisa deve poder ser empregada na satisfação da necessidade. Embora útil, necessitada e escassa, a coisa pode não ser um bem econômico se, por qualquer motivo, não puder ser usada pelo sujeito econômico. O objeto útil e valioso, caído no fundo do mar, não é um bem econômico." (GALVES, 2004, p. 54)

273 "The economic value of something is how much someone is willing to pay for it or, if he has it already, how much money he demands for parting with it" (POSNER, 2007, p. 10).

274 "[E]m qualquer sociedade estabelecem-se relações e instituições destinadas a lhe permitir enfrentar o problema da escassez, vale dizer, a criar um padrão decisório coerente a ser utilizado quando recursos escassos devam ser destinados a um fim qualquer. A atividade econômica é, pois, aquela aplicada na escolha de recursos para o atendimento das necessidades humanas. Em uma palavra: é a administração da escassez. E a Economia, o estudo científico dessa atividade, vale dizer: do comportamento humano e das relações e fonômenos dele decorrentes que se estabelecem em sociedade." (NUSDEO, 2005, p. 30)

275 "Não é, pois, sem razão, que os economistas contemporâneos preferem definir a Economia como a ciência da escassez ou, mais claramente, a ciência que deve cuidar da eficiente administração dos escassos recursos disponíveis, tendo em vista a satisfação dos ilimitados desejos da sociedade" (ROSSETTI, 1991, p. 128)

276 Demanda ou procura é a "quantidade de um determinado bem ou serviço absorvida ou adquirida a um dado preço num dado período de tempo" (NUSDEO, 2005, p. 231).

277 "Em termos econômicos, a escassez surge do pressuposto de que as necessidades humanas são infinitas, ao passo que os bens ou os meios de satisfazê-las são sempre finitos. De acordo com as teorias econômicas neoclássicas, o homem pode produzir o suficiente de qualquer bem econômico para satisfazer completamente determinada

objeto existir em expressiva ordem de grandeza (milhões de unidades, litros ou toneladas, por exemplo), mesmo assim será considerado um bem escasso, para a Economia, se a demanda por aquele bem for ainda maior[278]. É o caso do petróleo, por exemplo.

Para adequada compreensão da escassez, é fundamental notar que, para que haja procura, é preciso que o objeto seja útil no atendimento de uma determinada necessidade. Esta, por sua vez, pode se manifestar de variadas formas, muito além de demandas básicas de subsistência. As necessidades econômicas podem inclusive variar ao longo do tempo, com o surgimento de demandas antes inexistentes[279-280]. Esse

---

necessidade, mas jamais poderá produzir o suficiente de todos os bens para atender simultaneamente a todas as necessidades. De acordo com essa definição, as ciências econômicas serviriam exatamente para gerir a escassez. Por outro lado, os bens econômicos são escassos porque normalmente se dispõe apenas de quantidades limitadas de recursos produtivos necessários para criar os bens em questão, recursos estes que compreendem basicamente o trabalho, a terra e o capital." (SANDRONI, 1999, p. 211).

278 "É bem verdade que nesse estágio de evolução econômica a escassez não significará necessariamente pouco, mas insatisfação, uma vez que os novos níveis de cultura da sociedade exigirão, em conjunto com outros fatores, a produção de novos tipos de bens e serviços. É por isso, aliás, que em nenhuma época da História uma economia conseguiu satisfazer plenamente às necessidades sociais. Mesmo nas economias altamente desenvolvidas de nossa época, a saturação dos desejos humanos está longe de ser alcançada. Conduzidas pelo despertar de novos desejos, as necessidades materiais parecem ilimitadas. Coisas ontem supérfluas são hoje imprescindíveis. E não podemos imaginar aonde seremos levados pela produção em massa, pelas novas necessidades que dia a dia são criadas e pela incapacidade de renunciarmos às posições materiais de bem-estar já conquistadas." (ROSSETTI, 1991, p. 127)

279 "O fato concreto é que no mundo de hoje todos pensam que desejam e "necessitam" de geladeiras, esgotos, carros, televisão, rádios, educação, cinemas, livros, roupas, cigarros, relógios, etc. As ilimitadas necessidades já se expandem para fora da esfera biológica da sobrevivência. Poder-se-ia pensar que o suprimento dos bens destinados a atender às necessidades biológicas das sociedades modernas seja um problema solucionado e com ele também o problema da escassez. Todavia, numa contra-argumentação dois problemas surgem: o primeiro é que essas necessidades renovam-se dia a dia e exigem contínuo suprimento dos bens a atendê-las; o segundo é a constante criação de novos desejos e necessidades, motivadas pela perspectiva que se abre a todos os povos, de sempre aumentarem o padrão de vida. Da noção biológica, devemos evidentemente passar à noção psicológica da necessidade, observando que a saturação das necessidades, e sobretudo dos desejos humanos, está muito longe de ser alcançada, mesmo nas economias altamente desenvolvidas de nossa época. Consequentemente, também o problema da escassez se renova". (RIZZIERI, 1998, p. 13)

280 "Sem dúvida, é provável que o suprimento dos bens destinados a atender às necessidades biofisiológicas dos habitantes das economias mais afluentes seja um problema solucionado. Entretanto, não se deve perder de vista dois fatos. O primeiro resume-se em que as necessidades primárias, de natureza biofisiológica, renovam-se dia a dia e exigem contínuo suprimento dos bens destinados a atendê-las. Mesmo que o suprimento desses bens possa ser satisfatoriamente providenciado por pequena parcela da população ativa, o problema de sua produção é perpetuado pela sua contínua necessidade. O segundo fato resume-se em uma observação tão simples quanto a anterior. Trata-se de que, nas modernas economias de tecnologia avançada, caracterizadas por uma notável produção em massa, embora as necessidades primárias se encontrem perfeitamente atendidas, o problema da escassez torna-se

enfoque é especialmente relevante nos mercados de arte digital, questão central do presente trabalho, uma vez que é fundamental compreender o que buscam os compradores desse tipo de material, cuja demanda é um fenômeno recente.

Nesse sentido, a literatura econômica destaca que há diferentes razões que motivam a procura por um determinado bem. Uma primeira hipótese se refere à "demanda funcional" ou "consumo utilitário". Nesse caso, o objeto em si detém algum aspecto de ordem funcional que atende diretamente à necessidade do demandante[281]. Há aqui uma questão de uso essencialmente prático: compro comida para me alimentar, preciso de sabonete, shampoo e creme dental para fazer minha higiene pessoal, quero um casaco para me proteger do frio, e daí por diante.

Em sentido contrário, há situações de compra caracterizadas por uma "demanda não-funcional", quando as razões para a procura pelo bem extrapolam a utilidade inerente ao objeto desejado[282]. São os casos de compras especulativas ou irracionais[283], mas também as hipóteses influenciadas pelo comportamento ou percepção das outras pessoas em relação à aquisição realizada pelo demandante[284-285]. Harvey Leibenstein (1950) desdobra essa última categoria em três espécies: "*bandwagon effect*" (efeito adesão), "*snob effect*" (efeito esnobe) e "*Veblen effect*" (nomeado a partir de estudos produzidos pelo economista norte-americano Thorstein Veblen)[286].

---

talvez mais grave que nas economias primitivas. A razão desse aparente paradoxo encontra-se na constante criação de novos desejos e necessidades, motivados pela perspectiva que se abre a todos os povos de sempre aumentarem o seu padrão de vida e o seu bem-estar material." (ROSSETTI, 1991, p. 125 e 126)

281 "No consumo utilitário, a importância está no produto consumido, que deve, no produto, apresentar as características funcionais necessárias para atender a uma necessidade objetiva do consumidor". (PORTO, 2011, p. 22)

282 "An article may be useful and wasteful both, and its utility to the consumer may be made up of use and waste in the most varying proportions. Consumable goods, and even productive goods, generally show the two elements in combination, as constituents of their utility; although, in a general way, the element of waste tends to predominate in articles of consumption, while the contrary is true of articles designed for productive use". (VEBLEN , 1902, p. 47)

283 "For the sake of completeness there should perhaps be some explanation as to what is meant by speculative and irrational demand. Speculative demand refers to the fact that people will often "lay in" a supply of a commodity because they expect its price to rise. Irrational demand is, in a sense, a catchall category. It refers to purchases that are neither planned nor calculated but are due to sudden urges, whims, etc., and that serve no rational purpose but that of satisfying sudden whims and desires." (LEIBENSTEIN, 1950, p. 189)

284 "By functional demand is meant that part of the demand for a commodity which is due to the qualities inherent in the commodity itself. By nonfunctional demand is meant that portion of the demand for a consumers' good which is due to factors other than the qualities inherent in the commodity." (LEIBENSTEIN, 1950, p. 188 e 189)

285 "Many persons purchase branded goods for the purpose of demonstrating to others that they are consumers of the particular goods, in other words to impress others. They advertise themselves (much as sellers of goods advertise their goods) by wearing clothes, jewelry or accessories that tell the world that they are people of refined (or flamboyant) taste or high income". (LANDES e POSNER, 2003, p. 305)

286 "Probably the most important kind of nonfunctional demand is due to external effects on utility. That is, the utility derived from the commodity is enhanced or decreased owing to the fact that others are purchasing and consuming the same commodity, or owing to

No primeiro caso ("*bandwagon effect*"), alguém deseja determinado objeto simplesmente porque outras pessoas também o possuem. A motivação para a aquisição é o desejo de integrar um certo "grupo", com uma associação identificada pela propriedade de um mesmo tipo de bem. Por exemplo, adquirir o dispositivo eletrônico que "está na moda". Já o "*snob effect*" opera de certa forma em sentido contrário: há um desejo de ser visto em uma posição de exclusividade em função da aquisição do objeto. Este geraria um diferencial entre seu adquirente e as demais pessoas. Por fim, a compra motivada pelo "*Veblen effect*" tem como fundamento, para o demandante, a possibilidade de demonstrar poder aquisitivo elevado, ao adquirir um produto por um valor muito alto. É o caso dos carros de altíssimo luxo, como os fabricados pela Ferrari. Nesse caso, quanto mais caro for o objeto, maior sua atratividade nesse contexto. Essa hipótese configura o chamado "*consumo conspícuo*", no qual o desejo principal do demandante é ostentar sua capacidade financeira por meio da compra e não ter alguma necessidade de caráter utilitário atendida pelo objeto adquirido[287-288]. Por exemplo, as viagens ao espaço comercializadas pela empresa Space X, que, apesar de durarem poucos minutos, custam uma fortuna.

O "*snob effect*" e o "*Veblen effect*" têm uma diferença bastante sutil. No primeiro caso, o que interessa para o adquirente é a obtenção de um bem de acesso limitado, de modo que o simbolismo para suas razões está no próprio objeto. Já na segunda hipótese, a questão está no alto preço pela aquisição. Não há exatamente a

---

the fact that the commodity bears a higher rather than a lower price tag. We differentiate this type of demand into what we shall call the "bandwagon" effect, the "snob" effect, and the "Veblen" effect. By the bandwagon effect, we refer to the extent to which the demand for a commodity is increased due to the fact that others are also consuming the same commodity. It represents the desire of people to purchase a commodity in order to get into "the swim of things"; in order to conform with the people they wish to be associated with; in order to be fashionable or stylish; or, in order to appear to be "one of the boys." By the snob effect we refer to the extent to which the demand for a consumers' good is decreased owing to the fact that others are also consuming the same commodity (or that others are increasing their consumption of that commodity). This represents the desire of people to be exclusive; to be different; to dissociate themselves from the "common herd." By the Veblen effect we refer to the phenomenon of conspicuous consumption; to the extent to which the demand for a consumers' good is increased because it bears a higher rather than a lower price. We should perhaps emphasize the distinction made between the snob and the Veblen effect - the former is a function of the consumption of others, the latter is a function of price". (LEIBENSTEIN, 1950, p. 189)

287 "A originalidade da noção de consumo conspícuo, devida a Veblen, é exatamente a superação da dicotomia necessidade e desperdício. No caso de consumo ostentatório, pagar mais do que se precisaria é sinal de ascendência e de poder; e exatamente o objetivo social visado pela aquisição é demonstrar a preponderância econômica entre um indivíduo e outro, entre os que tem-para-desperdiçar e os outros. Ora, essa necessidade específica – de demonstrar poderio – se destaca do mercado de utilidade prática, para se constituir num espaço econômico próprio. O mercado de ostentação, em que o consumo, ele mesmo, simboliza o poder de quem quer e quem pode desperdiçar. A utilidade é o símbolo". (BARBOSA, 2006, p. 391)

288 "Consumo conspícuo é o ostentatório e o sedutor; o consumo em que a utilidade reside no símbolo que a marca representa – de riqueza, de ostentação, de alto padrão. [...] Ainda hoje essa teoria é muito atual e serve para ilustrar o tipo de consumo baseado na ostentação e na vaidade, e não na utilidade, muito visto nos países onde o sistema de economia adotado é o capitalista". (PORTO, 2011, p. 20 e 21)

necessidade de que se trate de um objeto único, desde que a sua compra demonstre claramente que o adquirente é uma pessoa de grande poder aquisitivo e só assim conseguiu ter aquele bem[289], mesmo que este seja supérfluo[290]. Logicamente, mesmo o foco principal estando aqui na questão monetária (e não no objeto em si), deve haver também algum nível de limitação de acesso ao bem, porque a noção de riqueza financeira, no caso do consumo conspícuo, não deixa de ter um aspecto relativo. Quanto mais pessoas adquirirem o mesmo tipo de objeto, por terem dinheiro suficiente para isso, menor será a percepção de que esse bem é algo alcançável apenas por quem tem um destacado montante de recursos monetários.

Interessante notar que, apesar de o "*snob effect*" muitas vezes envolver também bens caros, na medida em que isso signifique uma distintividade para seu proprietário, nem sempre isso ocorre. Um exemplo que contém a questão do diferencial pelo objeto, mas cujo custo de aquisição é relativamente baixo em termos nominais, são os álbuns de figurinhas que disponibilizem cromos considerados raros. No ano de 2022 (data de elaboração deste texto), houve mais uma edição da Copa do Mundo de futebol. Por ser um esporte extremamente popular, o álbum de figurinhas dessa competição atrai um grande número de colecionadores. Especificamente nesse caso, há a prática de oferta reduzida de cromos raros, que acabam sendo muito valorizados justamente por serem raros. A figurinha dourada do jogador Neymar Jr., na série "Legends", chega a valer em torno de R$9.000,00 para colecionadores. Cada envelope contendo cinco cromos custa R$4,00, de modo que cada unidade tem um preço de aquisição normal de R$0,80. Porém, estima-se que essa figurinha diferenciada apareça apenas uma vez a cada 1.900 envelopes, o que força uma situação de escassez e fomenta o interesse de quem deseja obtê-la pela vontade de ter um objeto raro em sua coleção. Vale ainda destacar que o desejo pela obtenção de um desses cromos é tamanho que há notícias de colecionadores que chegam a usar balanças de precisão para pesar os envelopes antes da compra porque, supostamente, um pacote com a figurinha especial seria um pouco mais pesado que o normal[291].

Nesse sentido, o "*snob effect*" não será necessariamente oriundo de um alto valor pago na compra, que demonstraria grande poder aquisitivo pelo proprietário do objeto. Pode ocorrer simplesmente como um golpe de sorte, como é o caso noticiado na imprensa sobre o garoto que achou a figurinha rara do jogador Neymar Jr. no mesmo

289 "[A]lthough it is probably impossible to design public policy to distinguish between Veblen effects and snob effects, it is useful to keep in mind the difference between the two. In its purest form, the Veblen buyer is not affected directly by how many others purchase the item as long as the signal about the price paid remains clear. Conversely, the snob effect depends on limited access regardless of price. In other words, the snob effect requires that others are both unable to possess the item and conscious of that deprivation". (HARRISON, 2007, p. 210 e 211)

290 "Throughout the entire evolution of conspicuous expenditure, whether of goods or of services or human life, runs the obvious implication that, in order to effectually mend the consumer´s good fame it must be an expenditure of superfluities". (VEBLEN, 1902, p. 45)

291 https://g1.globo.com/sp/santos-regiao/noticia/2022/08/26/uso-de-balanca-de-precisao-para-encontrar-figurinhas-raras-da-copa-revolta-vendedores-e-surpreende-colecionadores-do-litoral-de-sp.ghtml

dia em que ganhou seu álbum e abriu os primeiros envelopes dados pelo seu pai[292]. Nesse caso, o custo nominal de aquisição do bem foi de apenas R$0,80, sem que isso prejudique o efeito de exclusividade típico do "*snob effect*". Esse exemplo ilustra bem como esse fenômeno está focado no objeto em si, enquanto o "*Veblen effect*" necessariamente se atrela ao preço, para que uma aquisição cara signifique poderio econômico perante outras pessoas.

A referida distinção é essencial para os objetivos deste estudo porque um dos principais fatores que atribui valor aos bens digitais infungíveis, como os NFTs, é justamente a demanda não-funcional que atraem, especialmente nas espécies "*snob effect*" e "*Veblen effect*". Seguindo no exemplo das figurinhas, mencionado anteriormente, basta pensar na hipótese de um álbum inteiramente digital, com as figuras da série "Legends" sendo comercializadas por meio de NFTs. De fato, isso já vem ocorrendo de variadas formas, desde cards digitais de automóveis[293] até registros de jogadas de atletas[294] e conquistas de clubes de futebol[295].

Para melhor compreensão dessas nuances, é importante destacar os conceitos econômicos de *bens rivais* e *não-rivais*. No primeiro caso, o uso do objeto por uma pessoa rivaliza com o acesso dos outros demandantes ao mesmo bem, de modo que o seu consumo reduz a disponibilidade do produto ou serviço em questão. Já na situação de não-rivalidade, o oposto ocorre e a exploração por um indivíduo não implica bloqueio/restrição de uso para os demais. Importante destacar que a condição de rival/não-rival é caracterizada de forma intrínseca ao próprio objeto. Trata-se de uma *situação de fato*, que não é gerada de forma artificial por normas jurídicas. Inclusive, variações nesse contexto fático podem alterar a natureza do bem quanto à rivalidade. Um exemplo clássico na doutrina econômica é o de uma rodovia que, com um fluxo normal de veículos para sua capacidade, é considerada um bem não-rival. Porém, no caso de um congestionamento, essa mesma estrada passa a ser tida como um objeto sujeito à rivalidade, na medida em que os motoristas prejudicam uns aos outros em relação à exploração do bem por cada um deles nessas condições.

Junto a esses conceitos, é relevante explicar também a questão dos bens *exclusivos e não-exclusivos*. Não se trata da mesma coisa representada pela rivalidade ou não-rivalidade, mas sim elementos utilizados de forma complementar àqueles. Segundo o princípio econômico da exclusão, um bem exclusivo está sujeito ao poder de determinada pessoa, que pode bloquear o acesso àquele pelos outros indivíduos. Note-se que tal prerrogativa pode ser implementada pela legislação, na forma de direitos de propriedade, seja ela física ou intelectual. Já os bens não-exclusivos não se sujeitam a esse tipo de impedimento.

---

292 https://g1.globo.com/mg/minas-gerais/noticia/2022/08/24/garoto-de-10-anos-de-bh-encontra-figurinha-impossivel-de-neymar-estimada-em-ate-r-9-mil-nao-vou-vender-ele-e-meu-idolo.ghtml

293 https://www.tecmundo.com.br/mercado/237289-volkswagen-lanca-colecao-nfts-cards-modelos-classicos.htm

294 https://www.lance.com.br/atletico-mineiro/idolo-do-atletico-mineiro-reinaldo-lanca-colecao-de-nfts.html e https://exame.com/future-of-money/giba-neles-idolo-do-volei-lanca-colecao-de-nfts-com-cards-colecionaveis-de-jogadas-marcantes/

295 https://www.tecmundo.com.br/mercado/231274-atletico-mg-ganha-colecao-nfts-especiais-bicampeonato-brasileiro.htm

Logo, temos aqui um aspecto relacionado à diminuição *fática* de disponibilidade do objeto em função de suas características naturais (bem rival) e outro relativo ao *poder* de exclusão de acesso, que pode inclusive ser implementado por meio de uma norma jurídica (bem exclusivo). Nesse contexto, um objeto rival e exclusivo é considerado um bem privado. Já um objeto em situação totalmente oposta (não-rival e não-exclusivo) é tido como um bem público para a Economia[296-297].

Tomando como base essas classificações, temos vários exemplos possíveis. Roupas são bens privados para a Ciência Econômica. A iluminação em ruas e praças são tidos como bens públicos. E existem ainda as situações intermediárias.

Um peixe pescado em alto-mar é um bem não-exclusivo (já que nenhum indivíduo tem poder para impedir alguém de fazer essa pescaria), porém rival, porque esse fato diminui a quantidade disponível do objeto, refletindo, portanto, no acesso de outras pessoas. Já o conhecimento e as criações intangíveis, a princípio seriam bens não-exclusivos e não-rivais. Porém, uma vez sujeitos aos direitos de Propriedade Intelectual, a característica referente à exclusividade se altera.

Para aprofundar nessa questão, é necessário primeiro traçarmos um paralelo entre os bens *tangíveis* e *intangíveis*. Um objeto que tenha caráter concreto (ou seja, algo corpóreo, composto por átomos) naturalmente estará sujeito a algum nível de desgaste ao longo do tempo. Inclusive, na ausência de direitos de propriedade sobre estes, a tendência é que haja um processo mais acelerado de exaurimento. Esse fenômeno é estudado pela Economia há algum tempo, especialmente por meio da doutrina da "Tragédia dos Comuns" e o trabalho de Garrett Hardin sobre o tema. Não havendo direito de propriedade sobre o bem concreto e estando ele sujeito a uma livre exploração por qualquer pessoa, ninguém teria incentivos para investir na conservação desse objeto, na medida em que assumiria, sozinho, esses custos ao mesmo tempo que

---

296 "A teoria neoclássica classifica os bens de acordo com suas características de serem rivais ou não-rivais, e de serem excluíveis ou não excluíveis. Um bem é rival quando seu consumo por uma pessoa reduz a quantidade disponível para o restante da sociedade. Um bem é excluível se é possível impedir que alguém o consuma. Quando os bens são rivais e excluíveis, trata-se do caso dos bens privados. No outro extremo, um bem que não é rival nem excluível é um bem público, para o qual o exemplo clássico é a segurança nacional". (TEIXEIRA, 2009, p. 443)

297 "A public good is a commodity with two very closely related characteristics: 1. *Nonrivalrous consumption:* consumption of a public good by one person does not leave less for any other consumer. 2. *Nonexcludability:* the costs of excluding nonpaying beneficiaries who consume the good are so high that no private profit-maximizing firm is willing to supply the good. [...] Most examples of property that we have discussed thus far in this book are what economists call "private goods." Goods that economists describe as purely private have the characteristic that one person's use precludes another's: For example, when one person eats an apple, others cannot eat it; a pair of pants can be worn only by one person at a time; a car cannot go two different directions simultaneously; and so forth. These facts are sometimes summarized by saying that there is rivalry in the consumption of private goods. The polar opposite is a purely public good, for which there is no rivalry in consumption. A conventional example of a public good is military security in the nuclear age. Supplying one citizen with protection from nuclear attack does not diminish the amount of protection supplied to other citizens. There is also another attribute that distinguishes private and public goods. Once property rights are defined over private goods, they are (relatively) cheap to enforce. Specifically, the owner can exclude others from using them at low cost". (COOTER e ULEN, 2016, p. 40, 102 e 103)

o uso (e o desgaste decorrente disso) permaneceriam amplos. Logo, o fato de o bem ser "comum" (aqui entendido como rival e não-exclusivo) levaria ao seu exaurimento, que seria a "tragédia" observada aqui.

Um exemplo clássico para ilustrar esse fenômeno é uma pastagem hipotética que, não sendo de propriedade de ninguém, é explorada por todos indiscriminadamente. Esse uso liberado provoca uma exploração ineficiente, na medida em que nenhum dos usuários se preocupa em realizar os gastos necessários para manutenção da terra, como reposição do pasto, o que afeta negativamente a produtividade do bem e gera seu esgotamento. A existência de um proprietário, nesse caso, permite que ele explore a pastagem com maior eficiência e conserve o bem, por meio de investimentos para sua manutenção, ao mesmo tempo em que poderá impedir o seu uso desordenado e indiscriminado por terceiros. Esse exemplo é citado pelo próprio Hardin[298] e por outros autores, como Landes e Posner (2003), sendo bastante utilizado para sustentar propostas visando evitar tal esgotamento, inclusive implementação de direitos de propriedade privada ou o controle do objeto diretamente pelo Estado.

Já um objeto intangível não está sujeito a esse tipo de exaurimento, sendo, naturalmente, um bem não-rival. Por essa mesma característica incorpórea, na essência se trata também de um bem não-exclusivo, na medida em que não é possível lançar mão de instrumentos de natureza física, como cercas ou portões, para bloquear o seu acesso[299]. Esse é outro fator diferente do que ocorre com objetos tangíveis, que estão,

---

[298] "A tragédia dos comuns se desenvolve desta forma. Imagine um pasto aberto a todos. É de se esperar que cada vaqueiro vai tentar manter o gado do maior número possível no terreno comum. Tal mecanismo pode funcionar de modo razoavelmente satisfatório durante séculos, devendo-se às guerras tribais, à caça furtiva, e à doença manter o número de homens e animais bem abaixo da capacidade de absorção do solo. Por último, no entanto, vem o dia do julgamento, ou seja, o dia em que o objetivo a longo prazo desejado de estabilidade social se torne uma realidade. Neste ponto, a lógica inerente do que é comum impiedosamente gera tragédia. Como um ser racional, cada vaqueiro procura maximizar o seu ganho. Explícita ou implicitamente, mais ou menos conscientemente, ele pergunta: "Qual é a utilidade para mim de acrescentar mais um animal para o meu rebanho?" Esta utilidade tem um componente negativo e um positivo. 1) O componente positivo é uma função do incremento de um animal. Desde que o pastor recebe todos os lucros provenientes da venda do animal adicional, a utilidade positiva é quase um. 2) A componente negativa é uma função do sobrepastoreio adicional criado por mais um animal. Como, no entanto, os efeitos do excesso de pastagem são compartilhados por todos os pastores, a utilidade negativa para tomada de decisão (decision-making) de qualquer pastor particular é apenas uma fração de -1. Somando-se os componentes parciais de sua utilidade, o vaqueiro racional conclui que o único caminho sensato para ele seguir é o de adicionar outro animal a seu rebanho. E outro, e outro .... Mas esta é a conclusão alcançada por todos e cada pastor racional partilha de um bem comum. Aí é se encontra a tragédia. Cada homem está preso em um sistema que o compele a aumentar seu rebanho sem limites - num mundo que é limitado. Ruína é o destino para o qual todos os homens correm, cada um perseguindo seu próprio interesse em uma sociedade que acredita na liberdade dos bens comuns. Liberdade num terreno baldio (common) traz ruína para todos" (HARDIN, 1968, p. 4).

[299] Uma criação intelectual que não é objeto de nenhum privilégio de exclusividade não se sujeita ao princípio da exclusão devido a seu caráter imaterial, que permite o livre acesso simultâneo a ela, sendo considerado um bem público para fins econômicos (POSNER, 2007, p. 41). Logicamente, essa perspectiva não leva em conta limitações de

em tese, sujeitos a serem apropriados por meios fáticos, mesmo em situações nas quais não haja respaldo jurídico para tanto[300].

Tais características, do ponto de vista econômico, indicam que uma criação intelectual não é escassa *em si mesma*. Não é escassa pela sua própria natureza. Isso porque, em função do seu aspecto intangível, todos os demandantes poderiam utilizá-la ao mesmo tempo, sem que isso impeça o acesso de outras pessoas ou que implique no seu esgotamento. Nesse sentido, seria possível atender toda a demanda, sem limitação, o que não se amolda ao conceito econômico de escassez. Por exemplo, o fato de uma pessoa realizar uma pesquisa no Google não impede que milhares de outras pessoas, desde que utilizando dispositivos eletrônicos diversos, realizem o mesmo tipo de pesquisa, simultaneamente.

Porém, a legislação de Propriedade Intelectual altera esse cenário, na medida em que implementa direitos de exclusividade que podem impedir o acesso por terceiros não autorizados. Dessa forma, entende-se que isso gera uma espécie de *escassez artificial*[301], limitando o alcance dos demandantes ao objeto, mesmo sendo esse intangível. Aqui, há uma alteração da própria natureza econômica da criação incorpórea, que passa de um bem não-exclusivo e não-rival para um bem exclusivo e não-rival. Como estamos falando aqui do princípio da exclusão, importante destacar, neste caso, que a barreira de acesso que alterou essa característica não se deu por uma situação de fato, mas sim por uma determinação de ordem jurídica:

> [Barreiras] podem ser divididas em dois grupos: barreiras institucionais e barreiras econômicas. No primeiro caso, a entrada é legalmente proibida, não havendo, portanto, um preço limite a partir do qual a entrada de novas firmas é induzida. Esse é, por exemplo, o caso do regime de patentes, que assegura a exclusividade de exploração de um produto por uma empresa. (AZEVEDO, 1998, p. 204)

Toda essa discussão vai confluir para a questão do preço do objeto, que é influenciado pelo movimento de demanda, considerando inclusive sua intensidade e motivação, bem como pelo nível de disponibilidade do bem. Via de regra, quanto maior a oferta, menor será o preço e vice-versa[302]. É a conhecida "regra da oferta e da

---

uso provenientes da legislação, como direitos de uso exclusivo próprios da Propriedade Intelectual.

[300] COOTER e ULEN (2016, p. 79) destacam que, mesma na ausência de um respaldo estatal em relação a direitos de propriedade privada, os indivíduos usariam da força para manter os seus bens, em uma situação chamada de "estado de natureza" (*state of nature*). As pessoas estariam dispostas a investir em medidas protetivas até o limite em que o custo disso seja, no máximo, equivalente à utilidade que o bem oferece a eles.

[301] "Tal se dá porque a possibilidade de reprodução irrestrita de bens físicos (ou serviços) a partir do bem incorpóreo *ideia da máquina* (o que Alois Tröller chama de regra de reprodução) retira de tais bens a escassez. [...] Para que se mantenha a produção intelectual como atividade racional de produção econômica, é preciso dotá-la de economicidade, através de uma escassez artificial. A transformação desta regra de aplicação ilimitada num bem econômico se dá pela atribuição de uma exclusividade de Direito." (BARBOSA, 2003, p. 21 e 71)

[302] "[Q]uando existir excesso de procura, surgirão pressões no sentido de os preços subirem, pois: a) os compradores, incapazes de comprar tudo o que desejam ao preço

procura". Um monopolista, por exemplo, almeja aumentar o valor das suas vendas por meio da redução da quantidade ofertada[303]. Em sentido oposto, ninguém estará disposto a pagar pelo uso de um bem que seja de livre acesso, independentemente de sua utilidade. São exemplos clássicos nesse sentido a luz solar ou o ar que respiramos.

Como indicado anteriormente, os direitos de Propriedade Intelectual criam, em relação ao seu objeto, a possibilidade de sua apropriação fática pelo titular, o que não seria possível em sua ausência. Essa questão é muito relevante, porque, como já explicado, um bem que não seja escasso não terá valor econômico e ninguém terá disposição de pagar para tê-lo. Havendo escassez, ao contrário, é possível uma valoração do objeto e sua precificação diante de uma demanda que buscará atender suas necessidades considerando uma oferta limitada[304-305]. Na mesma linha, havendo direitos de propriedade claramente estabelecidos, haverá, em tese, maior segurança jurídica para os envolvidos, o que é um elemento essencial para um ambiente de

existente, se dispõem e passam a pagar mais; b) os vendedores veem a escassez e percebem que podem elevar os preços sem queda nas suas vendas. Quando existir excesso de oferta surgirão pressões para os preços caírem, pois: a) os vendedores percebem que não podem vender tudo o que desejam, seus estoques aumentam e, assim, passam a oferecer preços menores; b) os compradores notam a fartura e passam a regatear no preço." (MONTORO FILHO, 1998, p. 117 e 118)

303 "Sendo o único vendedor, o monopolista tem pleno controle da oferta, podendo determinar, a seu bel-prazer, qual será a quantidade total ofertada no mercado. Por via de consequência, através da variação das quantidades ofertadas, poderá influir sobre o preço, fazendo-o oscilar de maneira inversamente proporcional ao volume da oferta. Ganancioso, tal como o competidor em concorrência perfeita, procurará obter o máximo de ganho possível em sua atividade, mas agora, como pode decidir qual será o nível de oferta no mercado, provocará intencionalmente a escassez, a fim de que os preços se elevem. [...] Fica claro, pois, que o monopolista aumentará a quantidade ofertada enquanto sua receita marginal [ganho auferido pela venda de uma unidade adicional do produto] for superior ao seu custo marginal [despesa suportada pela fabricação de uma unidade adicional do produto]. Enquanto isso ocorrer, a venda de uma unidade a mais representará ao monopolista um incremento nos lucros. No momento em que se igualarem receita marginal e custo marginal, o monopolista não mais aumentará a quantidade ofertada, já que isto representaria uma diminuição de ganhos." (BRUNA, 2001, p. 31 e 33)

304 "Desta forma, o direito subjetivo absoluto sobre o invento, sobre uma obra literária, ou sobre uma posição de mercado só pode se tornar propriedade através de uma restrição legal de direitos e liberdades. Isso se dá através de uma exclusividade criada juridicamente: como ou propriedade intelectual, ou propriedade literária ou monopólio mesmo. A exclusividade jurídica da utilização de um bem imaterial, ideia, forma, ou posição no mercado dão uma mínima certeza de que se terá a vantagem econômica da escassez." (BARBOSA, 2003, p. 22)

305 "O ponto é que quando um recurso não é escasso, não haverá uma demanda por direitos de propriedade. Entretanto, à medida em que a economia muda ou cresce, os recursos vão se tornando escassos e, eventualmente, a ausência de direitos de propriedade seguros leva à dissipação de rendas através da competição entre os agentes econômicos para se apropriar dos diversos retornos ao recurso. Essa situação gera incentivos para que surja uma demanda por direitos de propriedade seguros que eliminem essa dissipação. Essa dinâmica pode acontecer com qualquer recurso que esteja passando por um processo de se tornar mais escasso, por exemplo, recursos naturais como cardumes de peixes, direitos de propriedade intelectuais sobre marcas e obras artísticas, nome de domínio na internet, espectro magnético, entre outros." (SZTAJN, ZYLBERSZTAJN e MULLER, 2005, p. 96)

negócios. Nesse sentido, Natalino Irti aponta que não há como um mercado funcionar sem normas claras e adequadas do ponto de vista do Direito:

> À definição do mercado como locus artificialis (fórmula introduzida em 1998 no meio da linguagem jurídica) costuma-se responder que o mercado não precisa do direito estatal, pois é, ele mesmo, capaz de produzir o seu próprio direito. Não acreditamos merecer reprovação a respeito da troca entre legislativo e normativo, ou entre estatal e jurídico. O problema é outro, e se encontra no configurar e pensar a intrínseca normatividade do mercado. Não se conhece como verdadeiro qualquer mercado (mercado determinado no tempo e no espaço) que não pressuponha institutos jurídicos: também a elementar distinção do "meu" e "teu", da qual emana cada ato de troca, implica a remissão a um critério determinativo. O mercado não cria, mas postula a distinção entre "meu" e "teu", e, portanto, que os bens sejam reconhecidos como propriedade privada, e não como propriedade coletiva. A troca é, por sua essência, instituto jurídico, e não poderia não o ser, pois isto determina que o "meu" se torne "teu", e o "teu" se torne "meu". E este "meu" e este "teu" nada mais designam que o pertencimento dos bens, atribuídos e protegidos por qualquer que seja o direito. Destaque-se, ainda, que isso também diz respeito à pressuposição das moedas, ou de formas de garantias e responsabilidade patrimoniais, e assim por diante. (IRTI, 2007, p. 45 e 46)

Além da perspectiva de escassez considerando a Propriedade Intelectual, a mesma lógica vale para os NFTs aplicados à criptoarte. A própria noção do token não-fungível implica uma exclusividade sobre o objeto digital, que se torna único justamente porque comercializado por meio de NFT. Há, portanto, uma escassez criada aqui por esse mecanismo jurídico, de modo que eventuais cópias não autenticadas daquela mesma criptoarte não são consideradas, pelo mercado que negocia esse tipo de bem, como equivalentes àquela marcada pelo token não-fungível. Isso implica uma possibilidade de valorização econômica da obra autêntica, diante de uma demanda que busca efetivamente uma propriedade exclusiva sobre ela[306].

Essa questão é melhor compreendida a partir do conceito econômico de mercado relevante, cuja função básica é explicar, em um caso concreto, como a concorrência opera em determinado espaço geográfico considerando objeto ofertado e agentes competindo entre si (ou ainda se não existe competição nesse ambiente). A partir disso, pode-se, por exemplo, calcular o percentual de participação

[306] "Being rivalrous, private goods must be used and consumed by individuals, not enjoyed equally by everyone. Efficiency requires the use and consumption of each private good by the party who values it the most. In a free market, exchanges occur until each good is held by the party who values it the most. Thus, the law can achieve the efficient allocation of private goods by, for example, lowering bargaining costs by assigning clear and simple ownership rights. Once the state recognizes private property rights, the owner of a private good can exclude others from using or consuming that right, except by the owner's consent. The owner's power to exclude channels the use or consumption of private goods into voluntary exchange, which fosters the efficient use of those goods." (COOTER e ULEN, 2016, p. 103)

de cada fornecedor no mercado, bem como analisar o comportamento dos demandantes em relação aos produtos ou serviços ofertados[307].

O conceito de mercado relevante se divide em dois aspectos, ambos complementares e necessários para a correta avaliação das relações de oferta e demanda: mercado relevante material (ou quanto ao produto/serviço) e mercado relevante geográfico. No primeiro ponto, é feita uma análise de substituibilidade, o que significa avaliar quais produtos ou serviços são substituíveis entre si visando atender determinada necessidade dos demandantes. Com isso, é possível identificar potenciais relações de competição, uma vez que poderiam disputar a preferência do adquirente, que pode usar qualquer um para solucionar sua demanda[308]. Logo, produtos ou serviços substitutos naturalmente guardam entre si uma potencial relação concorrencial. Na mesma linha, se não forem capazes de atender a um mesmo tipo de necessidade, não haverá concorrência entre eles, pois o demandante não terá ambos como opção viável para a finalidade que deseja.

Já o mercado relevante geográfico procura identificar o local onde essas relações de concorrência efetivamente ocorrem. Esse aspecto da análise busca medir o raio de alcance da oferta, o que leva em conta diversos fatores, como a estrutura de logística, custos de frete, barreiras à entrada e características do produto[309]. Agentes econômicos que disponibilizam produtos ou serviços substituíveis dentro desse limite geográfico são considerados concorrentes. Ao contrário, se os ofertantes não conseguirem disponibilizar o bem no mesmo local, não haverá relação de competição, mesmo se o objeto da sua oferta for similar.

O estudo conjunto desses dois fatores permite que sejam traçados a estrutura do mercado e o perfil dos concorrentes, inclusive no que diz respeito à participação de

---

307 "O mercado relevante é aquele em que se travam as relações de concorrência ou atua o agente econômico cujo comportamento está sendo analisado. [...] É bastante comum, principalmente na doutrina estrangeira, que se identifique o mercado relevante com o abuso de posição dominante, ou mesmo com poder de mercado. Por essa razão, a maioria dos livros estrangeiros trata das matérias conjuntamente. Tecnicamente, entretanto, tal aproximação não deve ser automática, pois o *mercado relevante é um conceito que permeia todo o direito antitruste* (e não, apenas, o abuso de posição dominante). Com efeito, a partir do momento em que as práticas são vedadas por produzirem (ou poderem produzir) efeitos anticoncorrenciais, a determinação da ilicitude passará pela delimitação do *mercado relevante* no qual esses efeitos serão sentidos. Em outras palavras, não se pode falar de efeitos anticoncorrenciais senão em um *determinado mercado: o mercado relevante*". (FORGIONI, 2005, p. 230 e 231).

308 Isso não exige que haja absoluta identidade entre os objetos. Produtos ou serviços distintos, porém substituíveis entre si, são chamados de *sucedâneos*. Nesse sentido: "[T]endo a gasolina e o álcool se tornado sucedâneos praticamente perfeitos, o mercado relevante não será nem o da gasolina, nem o do álcool separadamente, mas sim o de combustíveis". (NUSDEO, p. 242, 2005)

309 Por exemplo: duas usinas de cimento, uma localizada no Brasil e outra na China, dificilmente serão concorrentes, apesar de disponibilizarem um tipo de produto bastante homogêneo. Os custos de frete impediriam que esses dois ofertantes se encontrassem no mesmo mercado relevante geográfico, além da natural sensibilidade do cimento a questões climáticas, o que colabora para tornar inviável seu transporte por longas distâncias.

cada um deles na oferta total[310]. Porém, essa análise depende essencialmente da avaliação adequada sobre a percepção dos demandantes nesse contexto, especialmente sobre qual necessidade desejam ver atendida e de que forma[311]. É esse elemento que será fundamental para avaliação da substituibilidade.

Nesse sentido, não basta considerar eventual similaridade entre os bens ofertados sem analisar como os demandantes reagem a eles, especialmente quanto à capacidade de atender (ou não) às suas necessidades. É esse aspecto que será fundamental para definir se produtos ou serviços são efetivamente concorrentes entre si, porque essa questão passa pela avaliação do consumidor: se este não entender que dois bens ofertados são capazes de suprir a sua necessidade, não haverá competição entre eles na preferência desse comprador.

Essa é uma questão fundamental no âmbito das NFTs aplicadas à criptoarte. Tecnicamente, é possível reproduzir a obra digital milhares de vezes, com precisão absolutamente idêntica, com exceção de um único aspecto: a certificação via blockchain apontando que um determinado arquivo – e apenas ele – é considerado o original. Para quem se dispõe a pagar altos valores por um NFT nesse âmbito, nenhuma das cópias oferece uma solução satisfatória. O que o demandante deseja é apenas o arquivo original, único[312].

Esse ponto é essencial para a compreensão do mercado relevante aqui abordado. Sob essa perspectiva, cópias e original digital não fazem parte do mesmo mercado, porque não atendem à demanda de um mesmo tipo de público[313]. Quem deseja o NFT não se contentará com um arquivo não certificado, ainda que apresente

---

310 Paula Forgioni (2005) aponta que a delimitação do mercado relevante pode ser flexibilizada, na prática, considerando os elementos que são analisados para definir os seus contornos. E que esse movimento pode ser usado como válvula de escape em determinadas situações, de acordo com o uso desejado desse conceito para fins de aplicação de políticas públicas na área econômica, especialmente no âmbito da Defesa da Concorrência. Assim, nesse campo, trata-se de um instrumento que pode sofrer variações dependendo do contexto de sua aplicação.

311 "A concorrência, para ser relevante para a propriedade intelectual (inclusive e principalmente para a repressão à concorrência desleal e para a configuração do espaço de proteção das marcas), é preciso que se faça sentir em relação a um mesmo produto ou serviço. Ou seja, no mesmo mercado, que se designa como mercado relevante. [...] Assim, a delimitação do mercado relevante predominante leva em consideração critérios de consumo, uma vez que as preferências dos consumidores são determinantes da substituibilidade dos produtos entre si". (BARBOSA, 2006, p. 386 e 387)

312 "What makes these assets valuable is that they are one-of-a-kind. Offline, we take the properties of rivalrousness and uniqueness for granted. Rivalrousness is the idea that if I have a thing, you don't. If I give it to you, you have it, and I don't. Uniqueness is a related and extended version of rivalrousness. If I have a unique object, there is no replacement for it. Individual baseballs may be rivalrous with each other, but not unique. A baseball signed by Mike Trout would be unique and rivalrous if it is the only baseball he ever signed". (FAIRFIELD, 2021, p. 5)

313 "We propose that value in digital art and collectible objects stems from two components: a combination of digital uniqueness and a socially engaged audience to admire and value the collector's action. After all, a digital asset isn't worth much if anyone can have a copy at the click of a button, nor is it worth anything if nobody knows or cares if you have it". (TRAUTMAN, 2022, p. 35)

uma obra visualmente idêntica[314]. Já quem se satisfaz em ter uma arte sem o token não-fungível não se mostrará disposto a pagar para ter a exclusividade atestada pelo blockchain. Logicamente, temos aqui duas demandas absolutamente diferentes.

Nessa linha, é ilustrativo citar o caso "Hermès x Hermes" (Recurso Extraordinário 115.820-4/RJ), julgado pelo Supremo Tribunal Federal. Essa demanda envolveu a famosa empresa francesa de artigos de luxo ("Hermès") contra a empresa brasileira ("Hermes") que fabricava uniformes de pessoal de serviço doméstico e industrial. Como a Hermès trabalhava no ramo de vestuário, entre outras frentes, ajuizou ação contra a Hermes alegando confusão entre as marcas. No caso, o STF decidiu que os nomes podiam conviver, porque, apesar de ambas as empresas lidarem com roupas, os públicos de cada uma seriam absolutamente distintos. Dizendo de outra forma, estaríamos então diante de mercados relevantes diferentes, em que pese os dois ofertarem peças de vestuário, porque, no caso da Hermès francesa, os demandantes procuravam roupas de luxo. Já o público da Hermes brasileira buscava uniformes de trabalho. Trata-se de necessidades claramente distintas, que não poderiam integrar o mesmo mercado na disputa da preferência dos consumidores.

Compreender a real dimensão do mercado relevante em questão é essencial para definir o nível de escassez do objeto, lembrando sempre que esse é um elemento que só pode ser medido levando-se em conta o tamanho da demanda. Nesse sentido, perceber que a oferta da obra certificada com um NFT não se confunde com o fornecimento de cópias digitais é fundamental. Caso contrário, haveria equívoco em relação à dimensão da oferta e, portanto, na mensuração do nível de escassez.

Outro ponto importante sobre essa questão é destacar que os NFTs, no ambiente da criptoarte, de certa forma sinalizam uma mudança de tendência. Desde a popularização da Internet, houve uma intensificação de movimentos defendendo a liberação de cópias e livre acesso aos mais variados tipos de conteúdos intelectuais. No início dessas discussões, foi possível notar inclusive posicionamentos mais radicais, no sentido de que nenhuma lei "terrena" deveria se aplicar ao ambiente da Internet[315]. Nesse espaço, deveria valer apenas o que os usuários da rede determinassem[316]:

---

314 "A diferença de mercado, reconhecida pela jurisprudência, claramente não se pauta pela utilidade – como índice de mercado relevante, nem muito menos pelas noções clássicas de especialidade marcaria. O mercado difere entre um perfume "genérico" e um de luxo pelo preço, ainda que os dois se aproximem ou se identifiquem pelo mesmo aroma – ou utilidade. Mas o genérico não impressiona pela honra que traz ao comprador como evidência de fortuna". (BARBOSA, 2006, p. 391)

315 "A internet pode ser vista por uns como um paraíso digital, um "território sem lei", um mundo alternativo sem regras. Essa utopia da internet seria realmente desejável se não fosse a realidade dos crimes que lá são configurados (redes de pedofilia, por exemplo), os excessos cometidos e alguns pecados da indústria implícitos. A pirataria é mais um tópico desta grande discussão. É um paradoxo. Se, por um lado, é considerada uma prática ilegal e falsamente democrática, por outro lado, pode ser uma forma de combater as estruturas de mercado dominantes". (ADOLFO e SOUZA, 2011, p. 114 e 115)

316 "La naciente Internet no era tan fabulosa, pero (John Perry) Barlow escogió esa denominación, porque consideraba el ciberespacio una realidade independiente del mundo físico em lá que los indivíduos podían relacionarse entre sí com total libertad y olvido completo de peculiaridades políticas, sociales, religiosas, raciales, etc. [...] Imbuído de afanes libertarios, Barlow rechazaba la aplicación de las leyes estateles em el ciberespacio, formando sólo por información digitalizada e inmune a la fuerza física monopolizada por los Estados. Em ciertos momentos, incluso ha negado todo papel del

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions. You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions. You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different. (BARLOW, 1996).

O debate acabou se consolidando no sentido de que a Internet não era um espaço imune ao Direito, havendo reconhecimento de que o conteúdo que é ali utilizado estaria sujeito normalmente à legislação, inclusive as normas aplicáveis ao DA[317]. Porém, duas constatações também se assentaram em relação ao assunto: a nova realidade digital demandaria uma releitura e adaptação de vários aspectos do Direito "clássico" ao contexto da Internet[318] e que, mesmo havendo incidência da

---

Derecho em Internet: bastarían reglas éticas estabelecidas por los mismos internautas". (PUERTO, 2012, p. 66)

317 "A Internet não mudou o direito autoral do ponto de vista jurídico, ou seja, o autor continua gozando das prerrogativas morais e patrimoniais sobre sua obra. No entanto, não se pode negar que houve uma mudança sob a ótica do usuário da Internet, e isso se deve à tecnologia, que permitiu a reprodução e a circulação como jamais poderíamos imaginar. Em outras palavras, a conjugação da tecnologia digital com a Internet mostra-se hoje o terreno fértil para a violação dos direitos autorais". (SANTOS, 2009, p. 108)

318 "The internet and other digital technology demand that we adapt and reformulate copyright doctrine to radically different markets, incentives, and possibilities for bottom-up speech that challenge large media firms´ domination of public disclosure. [...] The internet and other digital technologies empower individuals to copy, share, parse, manipulate, and access expression. In ways that significantly erode if not completely supplant the traditional markets upon which authors, publishers, and comercial media have long relied. To properly address these issues we need to translate copyright´s fundamental principles to circumstances that traditional copyright doctrine did not anticipate". (NETANEL, 2008, p. 56)

legislação de Propriedade Intelectual nesse ambiente, isso não altera o fato de que a cópia das obras se tornou muito mais fácil, do ponto de vista prático, com as novas tecnologias disponíveis[319].

Além dessa questão fática, foi possível observar também o surgimento de novas correntes de pensamento, que defendiam maior possibilidade de circulação das obras, sem, contudo, abolir a existência dos DA. Nesse contexto, ganharam notoriedade propostas no campo do *copyleft*:

> Enquanto o *copyright* é visto pelos mentores originais do *copyleft* como uma maneira de restringir o direito de fazer e distribuir cópias de determinado trabalho, uma licença de *copyleft* usa a lei do *copyright* de forma a garantir que todos que recebam uma versão da obra possam usar, modificar e também distribuir tanto a obra quanto suas versões derivadas. Assim, de maneira leiga, pode-se dizer que *copyleft* é o oposto de *copyright*.
>
> Entende-se, a partir da explicação acima, que o *copyleft* é um mecanismo jurídico para se garantir que detentores de direitos de propriedade intelectual possam licenciar o uso de suas obras além dos limites da lei, ainda que amparados por esta. Por meio das licenças inspiradas no *copyleft*, aos licenciados seria garantido, de maneira genérica, valer-se das obras de terceiros nos termos da licença pública outorgada. (BRANCO JÚNIOR, 2007, p. 153 e 154)

Um dos nomes que se destacou nesse tipo de proposta é o norte-americano Lawrence Lessig. Ele foi um dos fundadores do *Creative Commons* (CC), uma organização sem fins lucrativos criada em 2001 e que propõe o uso de licenças gerais e gratuitas para acesso a conteúdo protegido pela legislação de DA, com diferentes níveis de liberdade para quem utiliza o material licenciado:

> The Creative Commons is a non-profit corporation established in Massachusetts, but with its home at Stanford University. Its aim is to build a layer of *reasonable* copyright on top of the extremes that now reign. It does this by making it easy for people to build upon other people's work, by making it simple for creators to express the freedom for others to take and build upon their work. Simple tags, tied to human-readable descriptions, tied to bulletproof licenses, make this possible.
>
> *Simple*—which means without a middleman, or without a lawyer. By developing a free set of licenses that people can attach to their content, Creative Commons aims to mark a range of content that can easily, and reliably, be built upon. These tags are then linked to machine-readable versions of the license that enable computers automatically to identify content that can easily be shared. These three expressions together—a legal

[319] "A situação se torna particularmente complexa se consideramos as peculiaridades das obras em formato digital, já que sobre elas incidem as mesmas regras da LDA, a despeito da volatilidade peculiar ao mundo digital, o que resulta em facilidade de confecção de cópias e reproduções com qualidade muitas vezes idêntica ao original, a custo reduzido. [...] Com a facilidade da cópia, quer se tratasse de obras impressas (com as copiadoras), ou gravadas (por meio dos gravadores de fitas K7 e com o vídeo caseiro), houve sensível diminuição na distância entre a qualidade do original e da cópia. Além disso, o fácil acesso de qualquer habitante de grande centro a tais tecnologias facilitava em muito a possibilidade de obtenção de uma cópia não autorizada". (BRANCO JÚNIOR, 2007, p. 86 e 177)

> license, a human-readable description, and machine-readable tags—constitute a Creative Commons license. A Creative Commons license constitutes a grant of freedom to anyone who accesses the license, and more importantly, an expression of the ideal that the person associated with the license believes in something different than the "All" or "No" extremes. Content is marked with the CC mark, which does not mean that copyright is waived, but that certain freedoms are given. (LESSIG, 2005, p. 282 e 283)

Um aspecto recorrente na maioria das licenças estruturadas no âmbito do CC é a liberdade de cópia, distribuição e utilização da obra, de forma gratuita. É também comum a vedação a usos comerciais e a obrigatoriedade de compartilhamento pela mesma licença (ou seja, nas mesmas condições em que recebida a obra). Esta última significa que, se autorizada a modificação de um conteúdo licenciado por meio de uma liberação no âmbito do CC, a obra derivada dessa permissão deve ser obrigatoriamente disponibilizada ao público nos mesmos moldes que a pessoa utilizou para acessar o material original. Isso gera um efeito em cadeia, na medida em que uma única licença permitindo cópia, distribuição e utilização de forma gratuita (entre outras possibilidades) se desdobra em várias outras de mesmo perfil, para as obras que surgiram a partir da primeira.

Há críticas e polêmicas envolvendo as licenças de CC, como alegações no sentido de que o autor perde o controle sobre sua obra, na medida que esses instrumentos são efetivados em caráter irrevogável (PONTES, 2013). De toda forma, é inegável que houve na Internet uma popularização desse tipo de licenciamento e outros similares. Juntamente com a percepção que muitas pessoas têm, no sentido de que a cópia no ambiente digital seria "livre", esses fatores contribuíram para um alto nível de acesso às obras na internet. Logicamente, isso impacta no nível de escassez desse conteúdo e no seu valor econômico. Como explicado anteriormente, quanto maior a oferta de um objeto, menor tende a ser o seu preço. Assim, no ambiente digital, a questão da escassez foi em certo sentido mitigada, em função desses fortes movimentos de cópia e disponibilização gratuita de conteúdo.

Além disso, as criações intangíveis em geral, como já explicado, são por conceito bens não-rivais do ponto de vista econômico. O que se modifica com o exercício de direitos exclusividade (como os Direitos Autorais) é a questão do poder de excluir outras pessoas do acesso por meio de uma *prerrogativa jurídica*. Mas, no caso do CC, esse tipo de prerrogativa é usada para permitir o acesso, ao invés de bloquear. Tudo isso converge para um ambiente digital de pouca ou nenhuma escassez em relação aos conteúdos intelectuais.

No caso de NFTs aplicados à criptoarte o mercado se movimenta em sentido contrário. Esse modelo de negócio propõe estabelecer uma escassez no ambiente digital, o que não era o padrão observado na internet até então[320]. Além dos direitos de exclusividade oriundos do DA, o uso do NFT trata o bem intelectual como sendo rival, na medida em que a aquisição por um colecionador retira o objeto adquirido da disponibilidade dos demais (não sendo considerada aqui a demanda das pessoas que

[320] "NFTs lay the groundwork for fixing one of the oldest problems of the internet. The internet threatened intellectual property because it is a technology that operates by making infinite, cheap, identical copies. It took over two decades to develop a technology that brought uniqueness back to the internet, by which digital assets were no longer fully duplicatable with the click of a button". (FAIRFIELD, 2021, p. 98 e 99)

se contentam com a cópia não-certificada). Isso significa uma *mudança na própria essência econômica da obra digital*[321] e visa a impactar no seu preço de comercialização, via NFT.

Essa questão de escassez digital, aliada ao "*snob effect*" e ao "*Veblen effect*" (como visto, espécies de demanda não-funcional), ajudam a explicar os altos valores observados em algumas vendas de cripoarte baseadas no NFT. A noção de exclusividade atestada pelo *blockchain* é o que permite que o preço nessas negociações se mostre bastante elevado.

Entendidas as questões econômicas e a motivação dos compradores, é necessário agora avaliar se a criptoarte comercializada nesse novo contexto poderia ser considerada como o original de uma obra, para fins de aplicação da legislação de DA, o que será feito no próximo capítulo.

3. Originalidade da obra atestada pelo nft: efeitos jurídicos

3.1 Obra Original?

Para a análise de diversas questões relativas aos Direitos Autorais, é fundamental a compreensão do que seja uma obra original. No caso, não estamos nos referindo aqui a um grau de diferenciação ou novidade entre determinada criação e as demais, mas sim a uma concepção de *exemplar único*. Historicamente, esse é um aspecto particularmente aplicável ao campo das artes plásticas, cuja exteriorização das obras se deu ao longo dos tempos por meio de suportes físicos, como telas ou materiais esculpidos. Porém, o advento da arte digital traz um novo contexto, no qual a apresentação desse tipo de obra não depende de um meio tangível. Assim, a questão é se o conceito de "original" se aplicaria aqui, considerando que não há um objeto físico no qual a criação foi exteriorizada pela primeira vez:

> Já dissemos que não há obra de arte plástica sem a produção de um exemplar. A ideia, por mais clara e distinta que seja, tem de encarnar, ganhando forma visível. Normalmente, a obra nasce mediante uma primeira encarnação, que constitui o original e tem valor mais elevado. (ASCENSÃO, 2007, p. 405)

Para análise dessa matéria, o primeiro aspecto que precisa ser considerado é o fato de que a aplicação da legislação de Direitos Autorais deve levar em conta as mudanças tecnológicas que ocorrem ao longo do tempo[322]. No caso da Propriedade Intelectual, o ambiente digital sequer é o primeiro exemplo de alteração nesse sentido:

> Há quem entenda que a propriedade intelectual está em crise, especialmente por conta das inovações tecnológicas, que podem ser traduzidas em uma única palavra: Internet. Hoje a

[321] "NFTs are sold with the following representations: that an NFT token is the asset it represents, that the purchaser owns the asset, that the seller of the asset has no further control over an asset once conveyed, and thus that the buyer of the asset can do as they wish with it. NFTs are sold on a promise similar to the promise one receives when buying a physical object. When a person buys a book from a brick and mortar bookstore, she owns that physical book, and is able to do what she wants with it, including sell it, read it, throw it away, or donate it. Digital property has never carried such a promise, and NFTs now attempt to offer it". (FAIRFIELD, 2021, p. 35 e 36)

[322] "O destino do direito de autor é caminhar sempre lado a lado com a tecnologia e evoluir na medida em que esta evolui, adaptando-se às alterações e superando contradições, sem, porém, eliminar estas últimas". (LEITE, p. 2005, 109)

> rede mundial de computadores mostra-se terreno fértil para a violação de direitos autorais. Entendemos que a propriedade intelectual passa por um momento de grande transformação, mas isso não é novidade e certamente deve ter ocorrido situação semelhante quando Gutenberg criou a tipografia, nos idos do século XV. Assim como os seres vivos se adaptam a novas realidades, os institutos jurídicos também passam por mutações e adaptações e, no caso da propriedade intelectual, isso se deve ao desenvolvimento e à popularização das tecnologias da informação. (SANTOS, 2009, p. 154)

Na verdade, as novas realidades trazidas pelo avanço tecnológico impactam diversos ramos do Direito, como já explicado quando abordamos, por exemplo, a discussão sobre o documento eletrônico no âmbito do Processo Civil. E os mesmos argumentos indicados ali, que concluíram pela validade dessa nova forma de apresentação de provas documentais, também podem ser aplicados no caso de exemplares originais no âmbito da criptoarte. Tal como naquele debate, um ponto fundamental é considerar se o suporte no qual o objeto se materializa precisa, necessariamente, ser físico. E a conclusão é que não, especialmente porque o artigo 7º da Lei 9.610/98 indica que a obra pode ser exteriorizada por qualquer meio.

Outro ponto relevante é avaliar como a vontade das partes que negociam a venda de um NFT aplicado a uma obra de arte digital pode influenciar essa análise. Nesse sentido, é importante destacar que fica claro aqui que comprador e vendedor se colocam como participantes de uma negociação envolvendo um objeto considerado único, ainda que em formato incorpóreo. Na verdade, quando retomamos o conceito de mercado relevante, que contém um conjunto de demandantes que buscam ter determinada necessidade atendida por meio de um produto ou serviço, percebe-se que esse posicionamento vale para um grupo até maior de pessoas323. Basta considerar que, nesse contexto, quem se dispõe a pagar para ser proprietário de uma obra de criptoarte certificada por um NFT deseja um objeto considerado único, seja em função do "snob effect", seja em razão de uma situação de consumo conspícuo. Outro arquivo digital, ainda que visualmente idêntico, não atenderia essa necessidade e, portanto, não seria um substituto para a primeira opção.

Logo, do ponto de vista econômico, há um comportamento coletivo neste caso, no sentido de que o NFT certifica uma obra original, como um exemplar único. Tal percepção encontra respaldo também na esfera jurídica:

> [O]s preceitos que referimos, e muitos outros que se poderiam criar, vão todos no sentido de procurar as constelações de utilizações que correspondem ao fim daquele negócio e portanto à vontade tendencial das partes. Não interessa a textualidade das palavras usadas mas os interesses que as visarem regular. (ASCENSÃO, 2007, p. 363)

Na mesma linha, o artigo 112 do Código Civil também poderia ser invocado para sustentar o enquadramento dessa criptoarte como objeto único, uma vez que tal norma dispõe que "nas declarações de vontade se atenderá mais à intenção nelas

323 Logicamente, não estamos considerando aqui a figura do monopsônio, estrutura de mercado na qual existe apenas um comprador disponível.

consubstanciada do que ao sentido literal da linguagem"[324]. Como explicado anteriormente, a intenção das partes é claramente a negociação de uma obra original e única, ainda que configurada como um arquivo digital. Isso, aliado ao dinamismo que as novas tecnologias provocam na realidade da sociedade e nas relações entre as pessoas, são argumentos que ajudam a sustentar a ideia de objeto único aqui:

> In a changing society, new forms of property arise continually. To illustrate, property law for underground gas and the electromagnetic spectrum (radio and television broadcasting) developed in the United States during the last century; and property law for computer software, music, video, and other material on the Internet, and genetically engineered forms of life developed in the last several decades. The need for a new form of property law arises in situations corresponding to our thought experiment. For example, like corn, digital music can be stolen. Without effective property law, people invest a lot of resources in stealing that music or trying to prevent its theft. These efforts redistribute music, rather than invent or manufacture it. Now the United States has property law that prevents the stealing of digital music. The imposition of these laws may have greatly stimulated the production of music. So, our thought experiment is really a parable about the incentive structure that motivates societies to continually create property. [...] Legislation imposes many restrictions on what a person may do with his or her property. But at common law there are relatively few restrictions, with the general rule being that any use is allowed that does not interfere with other peoples' property or other rights. Indeed, we could say that common law approximates a legal system of *maximum liberty*, which allows owners to do anything with their property that does not interfere with other people's property or other rights. The restriction of noninterference finds justification in the economic concept of *external cost*. Recall that external costs are those costs involuntarily imposed on one person by another. Because market transactions are voluntary, externalities are

[324] "There is a developed legal literature on first-generation cryptocurrencies, which focuses on finding the right legal characterization of blockchain-based activities and assets. The overarching theme of that literature is that legal regulation of blockchain depends not on the technology, but on how humans are using it. [...] That use-drives-regulation approach has held as tokens create property interests. If a token is sold as property, treated by humans as property, passed down through wills as property, the law has begun to take it seriously as property. I and others have argued for over a decade that when digital assets are treated by owners as personal property, the law of personal property should apply; the same goes for tokens that act as digital deeds for real estate, a solution that could end the need for title searches and clear up confusion over ownership of land. [...] NFTs provide the opportunity for a serious examination of the tangled legal relationships online between property and contract, and between digital personal property and intellectual property. This reexamination is long overdue. Establishment of clear principles surrounding digital personal property—not intellectual property— is necessary for NFTs to succeed. NFT buyers and sellers clearly intend to convey an ownership interest in digital personal property. The law of online transactions has suffered badly from the lack of such anchoring examples. Buyers of NFTs believe they are buying personal property, and sellers claim they are selling it. The token itself is susceptible only to possession and control by one entity, just like a physical object. The power of NFTs as a grounding example for digital personal property cannot be overstated. (FAIRFIELD, 2021, p. 53 a 55 e 58)

> outside the market system of exchange—hence their name. (COOTER e ULEN, 2016, p. 80 e 105)

No caso dos NFTs, é importante também destacar que essa questão não fica limitada às condições definidas por comprador e vendedor da criptoarte. Isso porque a tecnologia blockchain adotada nesse modelo de negócio se presta a atestar a originalidade da obra. Logo, essa condição, uma vez instalada, não dependerá mais de qualquer declaração ou ato de confiança posterior, por quem quer que seja, para sua comprovação. Do ponto de vista econômico, isso terá consequências relevantes, pois a confiabilidade do sistema reduz custos de transação relacionados às pesquisas e verificações que o comprador necessita para avaliar a veracidade do objeto:

> What are transaction costs? Are they ever really negligible? We cannot use the Coase Theorem to understand law without answering these questions. Transaction costs are the costs of exchange. An exchange has three steps. First, an Exchange partner has to be located. This involves finding someone who wants to buy what you are selling or sell what you are buying. Second, a bargain must be struck between the Exchange partners. A bargain is reached by successful negotiation, which may include the drafting of an agreement. Third, after a bargain has been reached, it must be enforced. Enforcement involves monitoring performance of the parties and punishing violations of the agreement. We may call the three forms of transaction costs corresponding to these three steps of an exchange: (1) search costs, (2) bargaining costs, and (3) enforcement costs. (COOTER e ULEN, 2016, p. 88)

Na mesma linha, a definição clara de propriedade também gera impactos positivos para o ambiente de transações[325]:

> There is an extensive literature on bargaining games, including a large number of carefully constructed experiments testing the Coase Theorem. One of the most robust conclusions of these experiments is that bargainers are more likely to cooperate when their rights are clear and less likely to agree when their rights are ambiguous. Put in more formal terms, bargaining games are easier to solve when the threat values are public knowledge. The rights of the parties define their threat values in legal disputes. One implication of this finding is that property law ought to favor criteria for determining ownership that are clear and simple. The most immediate prescription for efficient property law is to make rights clear and simple. For example, a system for the public registration of ownership claims to land avoids many disputes and makes settlement easier for those that arise. Similarly, the fact that someone possesses or uses an item of property is easy to confirm. In view of this fact, the law gives weight to possession and use when determining ownership. Conversely, unclear ownership rights are a major obstacle to cooperation and a major cause of wasted resources. (COOTER e ULEN, 2016, p. 89)

325 "O objetivo da literatura sobre direitos de propriedade [...], é, portanto, analisar como a definição dos direitos em cada caso específico afeta o comportamento dos agentes econômicos. A ideia central é que os direitos de propriedade seguros e bem definidos, incluindo o direito de vender ou transferir a propriedade, farão com que o recurso venha a ser alocado ao uso que gere mais bem-estar." (SZTAJN, ZYLBERSTAJN e MUELLER, 2005, p. 93)

A certificação via blockchain pode gerar ainda outros desdobramentos relevantes em termos de segurança jurídica, especialmente no que diz respeito ao mapeamento de uma cadeia de propriedade da obra digital. Como se verá mais adiante, essa questão é importante para a aplicação efetiva do direito de sequência. Porém, antes de discutirmos esse ponto, é necessário diferenciar o ato de aquisição do original de uma obra da transferência dos direitos autorais sobre ela incidentes.

3.2 Aquisição de Original X Aquisição de Direitos Autorais

A compra do original de uma obra pode gerar alguma confusão em relação aos direitos autorais. Uma avaliação apressada poderia considerar que esse tipo de operação naturalmente implicaria automaticamente a transferência da Propriedade Intelectual para o adquirente. Porém, a questão não é exatamente assim.

Inicialmente, é importante destacar que a Lei 9.610/98 indica que os negócios jurídicos envolvendo Direitos Autorais devem ser interpretados de forma restritiva[326]. Na mesma linha, a legislação prevê uma série de presunções em prol do autor no âmbito dos contratos envolvendo o tema[327] e também que eventual autorização concedida para uso da obra não implica automaticamente permissões adicionais em relação à forma de exploração[328].

Assim, é possível notar que o contexto da LDA foi estruturado de modo a impor condições e limites visando a proteger os direitos do autor. Nesse sentido, a Lei 9.610/98 estabelece expressamente que a aquisição do original de uma obra *não* transfere automaticamente ao adquirente os direitos patrimoniais do autor[329], lembrando que os direitos morais são inalienáveis em qualquer caso. Além disso, como já indicado no capítulo anterior, mesmo a cessão dos direitos patrimoniais depende de forma escrita[330], não alcançando formas de uso ainda não existentes no momento da transferência[331].

A confusão entre a aquisição do original e a transferência de direitos autorais pode gerar impactos bastante relevantes. Um caso notório nesse sentido foi a compra de um exemplar raro de um livro de arte: *Jodorowsky's Dune*. Trata-se de uma obra surgida durante a tentativa de adaptação para o cinema do romance *Dune*, de Frank Herbert. No caso, o diretor Alejandro Jodorowsky encomendou a elaboração de um livro de arte contendo ilustrações sobre cenários, personagens e até uma reprodução ilustrada de todo o roteiro do que seria o filme, para presentear os executivos do estúdio responsável pela adaptação. A obra audiovisual não chegou a ser realizada naquele momento, mas estima-se que dez a vinte cópias do livro ainda existam, tendo se tornado objeto de interesse colecionadores. Eventualmente, um desses exemplares é vendido por valores na casa de U$D25.000,00.

Em novembro de 2021, um desses livros foi ofertado em leilão, sob a expectativa de ser negociado por cerca de U$D40.000,00. Porém, um grupo chamado Spice DAO adquiriu a obra por U$D3.000.000,00, valor muitas vezes maior do que o esperado. Na

326 Artigo 4º da Lei 9.610/98.

327 Artigos 49 a 51 da Lei 9.610/98.

328 Artigo 31 da Lei 9.610/98.

329 Artigo 37 da Lei 9.610/98.

330 Artigo 49, II e 50 da Lei 9.610/98.

331 Artigo 49, V da Lei 9.610/98.

época dessa aquisição, foi anunciado que a intenção dos compradores seria converter o livro em NFTs, queimar a cópia física e adaptar a história em uma série animada.

A questão é que, nesse caso, não houve transferência dos direitos autorais de modo a permitir tal plano, especialmente a realização de uma animação. O grupo posteriormente desmentiu que sua intenção seria essa, mas a notícia ficou famosa não só pelo preço fora do normal, mas também por ter sido entendida, de modo geral, como um grande investimento feito sem a análise adequada em relação aos direitos que efetivamente fazem parte desse tipo de negócio[332].

Assim, um ponto relevante é que, mesmo sendo o NFT um objeto único, sua aquisição não importa necessariamente a obtenção dos direitos autorais patrimoniais sobre a arte, a não ser que haja acordo escrito específico nesse sentido, durante a negociação[333]. São, portanto, questões distintas[334].

De fato, o que as partes envolvidas na compra e venda de um NFT relacionado à criptoarte parecem procurar é a propriedade exclusiva sobre o objeto digital certificado, tal como um colecionador de pinturas faz quando adquire quadros físicos, por exemplo. Já os direitos autorais sobre essa criação têm outro espectro de aplicação. No caso, serviriam especialmente para definir quem tem o poder de fazer cópias e alterações sobre a obra, entre outras prerrogativas. Porém, a intenção das pessoas interessadas nesse tipo de NFT não parece ser voltada a esse tipo de exploração do conteúdo, ainda que com fins econômicos. O elemento motivador seria a possibilidade de exibir a posse, ainda que digital, de um arquivo único, o que não é uma atribuição relacionada à Propriedade Intelectual nesse caso.

Porém, se o NFT indica a obra original e os direitos autorais não foram transferidos com a aquisição da primeira, então isso significa que eles permaneceram com o seu criador, nos termos da Lei 9.610/98. Considerando estritamente a legislação autoral, essa situação o permitiria inclusive fazer cópias da arte, ainda que nenhuma delas seja

---

332 https://www.esquire.com/entertainment/books/a38815538/dune-crypto-nft-sale-mistake-explained/

333 "By contrast, an NFT buyer is not purchasing a work, but rather a publicly available token that links to a work. For example, for a digital picture, the token may be a unique number and a link to a copy of the picture, hosted on a service such as IPFS. The token itself is visible to all, as is the work to which it points, so anyone else can look at the work and download it. And most NFT transactions don't purport to convey copyright or other intellectual-property interests regarding the work in question, so owning an NFT tied to an animation of, say a flying Pop-Tart cat doesn't put you in a position to use that animation any differently than someone who hadn't bought it. You have only a token that is hosted publicly online, 'registered' as assigned to your digital wallet rather than someone else's". (ZITTRAIN e MARKS, 2021)

334 "NFTs are therefore far more than a niche technology supporting online collectibles. They are a clear example of a purely digital interest sold as personal property. NFTs contain a component, the token itself, that is conceptually distinct from the abstract intellectual property rights. The token demands legal characterization, and the obvious legal characterization is personal property. NFTs therefore stand as a new and powerful grounding example of digital personal property, one that is capable of resisting the dominant online narrative whereby assets that are supposedly "sold" to consumers are in fact merely licensed". (FAIRFIELD, 2021, p. 98)

certificada pelo NFT transferido, uma vez que essa é uma das prerrogativas cabíveis ao titular dos direitos autorais patrimoniais[335].

Nesse sentido, cabe ponderar se o vendedor, ao realizar eventualmente uma cópia da arte, estaria cometendo algum tipo de infração ou simplesmente praticando o regular exercício dos direitos autorais que não foram transferidos com a venda do NFT. Incialmente, poderia haver algum questionamento relacionado à boa-fé objetiva, padrão de conduta leal que deve ser observado pelas partes em qualquer negócio jurídico[336]. Porém, a essência do modelo de negócio da criptoarte baseada em NFTs não é propriamente a exclusividade sobre a imagem da obra, mas sim a propriedade de um *certificado de autenticidade* do arquivo original. Nesse sentido, a mera realização de cópias não alteraria esse contexto, uma vez que o NFT continuaria a ser único. Além disso, a motivação do comprador aqui não é a possibilidade de reproduzir a obra, de modo que, a princípio, a manutenção pura e simples dos direitos autorais sob a titularidade do vendedor não o afetaria.

O que eventualmente poderia ser objeto de questionamento seria eventual conduta de geração e venda de *vários* NFTs e divulgar, em cada alienação, que *aquele* token é o original, ocultando a existência dos demais. Nesse caso, apesar de cada NFT ser único em si, todos eles estariam representando falsamente a mesma coisa, qual seja, a certificação de um original. No fundo, eventual conduta dessa natureza não parece diferir muito da prática de falsificação de quadros ou outras obras originais de artes plásticas, que é um tipo de ilícito muito antigo. Nesse caso, apesar de formalmente não haver ilegalidade do ponto de vista do direito autoral (partindo da premissa que eles não foram transferidos nesse exemplo e que o poder de cópia permaneceu com o vendedor), haveria uma infração ao dever de boa-fé objetiva em função da falsa comunicação, por meio dos NFTs, no sentido de cada obra ser a "original", mas existirem diversos arquivos certificados nesse sentido[337]. Além disso, do ponto de vista criminal, tal prática poderia ser entendida como estelionato, na medida que induz os compradores em erro para gerar uma vantagem indevida para o vendedor[338].

Diante dessas considerações, a princípio parece que o adquirente de uma obra de criptoarte certificada por um NFT poderia ter interesse na aquisição também dos direitos autorais especialmente para fins defensivos. Nesse caso, não se buscaria a

---

335 "Eden Gallery writes, "It can be difficult to wrap your head around the idea of buying digital art that can be copied. You can certainly copy a digital file, including art sold with an NFT. In some cases, the owner can buy the rights to reproduction, although artists usually retain this." While the original version of any artwork can only have one owner, "An NFT grants… ownership of the work, but it can be copied with permission or illegally. This is not actually that different from the reproductions we see all the time of traditional artwork. Just as the Mona Lisa has been reproduced countless times in print and digital…" (TRAUTMAN, 2022, p.27 e 28)

336 Artigos 113 e 187 do Código Civil.

337 "Imagine a seller who sells a hash to a buyer despite knowing that that hash is part of a fraudulent fork of a blockchain, or that the hash has been wrapped in another smart contract such that the collectible appears valuable but in fact is not recognized by anyone else.216 Even where the seller is not a merchant, if she knows that the buyer has a given purpose for the NFT and that the NFT is not fit for that purpose, she is liable to the buyer for breach of the warranty". (FAIRFIELD, 2021, p. 82)

338 Artigo 171 do Código Penal.

prerrogativa de fazer cópias do conteúdo e explorá-las, mas sim impedir que o antigo titular as faça, o que, em tese, dificultaria o ilícito imaginado sobre alienação de diversos "originais". De toda forma, considerando que o advento da Internet e outras tecnologias tornou a cópia muito fácil (e barata), do ponto de vista prático a titularidade dos direitos autorais, por si só, não é garantia de se evitar a ocorrência de cópias.

Além disso, não se pode desconsiderar a possibilidade de aproveitamento *econômico da obra por outros meios*, que não a cópia pura e simples. Há diversos exemplos que podem ser imaginados, sem afetar a exclusividade em relação à propriedade do arquivo digital original: aplicação da imagem da obra em peças de roupas, desenvolvimento de jogos e animações utilizando figuras ou personagens contidos na arte e daí por diante. Considerando a notoriedade que as operações envolvendo NFTs têm obtido, não é improvável imaginar o surgimento de mercados derivados desse fenômeno, porém caracterizados por outras formas de uso.

Um exemplo potencial nesse sentido é o *Bored Ape Yacht Club*[339]. Nesse caso, diversas pessoas famosas (e ricas) adquiriram NFTs de avatares de "macacos entediados". As imagens são geradas combinando aleatoriamente elementos como expressões, roupas e acessórios. Em comum, o fato de todos os macacos aparentarem tédio, mas cada um é caracterizado de forma única. A notoriedade do caso, aliada ao próprio poder de atração da fama dos adquirentes mais conhecidos (como Neymar, Eminem e Jimmy Fallon), pode, em tese, gerar um aspecto *cult* em relação a essas imagens. Não é impossível imaginar que os fãs de um dos proprietários famosos estejam dispostos a consumir produtos estampados com a figura do macaco pertencente a seu ídolo, buscando uma forma de associação com este. Isso pode gerar possibilidades adicionais de exploração econômica diretamente vinculadas aos direitos autorais, pois aqui sim haveria a cópia do conteúdo em outros contextos, sem prejudicar a exclusividade representada pelo NFT. Esse tipo de situação pode se mostrar relevante nas negociações envolvendo a criptoarte e a elaboração dos contratos de cessão desse objeto, uma vez que, como explicado anteriormente, a aquisição do original não implica automaticamente a transferência dos direitos autorais.

3.3 Direito de Sequência

Outro ponto importante é o direito de sequência. Trata-se de um dispositivo previsto na Convenção de Berna, com o objetivo de valorizar especialmente os criadores das artes plásticas. No caso, estes têm direito a receber um percentual sobre o preço ou sobre parte do lucro originado pela revenda de suas obras originais:

> O direito de sequência é previsto no art. 14, *ter* da Convenção de Berna. Tem por objeto obras de arte originais e manuscritos originais de escritores e compositores. [...] Há dois sistemas quanto à base de incidência do direito de sequência. Por um, recai sobre o preço. Pelo outro, recai sobre o aumento do preço realizado em cada nova transação. O segundo sistema tem a justificá-lo todas as razões que levaram ao estabelecimento do direito de sequência, notadamente:

[339] https://www.tecmundo.com.br/mercado/232736-nft-macaco-entenda-bored-ape-yacht-club.htm

> - a proteção do criador intelectual que por necessidade aliena suas obras a preço vil;
>
> - o fato de que com grande frequência os grandes criadores só granjearem reconhecimento público muito tarde, beneficiando então terceiros com a valorização de suas obras. (ASCENSÃO, 2007, p. 239)

No caso da legislação brasileira, há previsão de que o autor tem direito a perceber no mínimo 5% sobre o aumento do preço verificado em cada revenda da obra original[340]. Logo, no Brasil, é preciso que haja efetivamente lucro nominal na operação para que se possa invocar o direito de sequência. Em 2020, o Tribunal de Justiça do Rio de Janeiro negou indenização nesse sentido pelo fato de o autor não ter demonstrado qual teria sido o preço da venda anterior e, portanto, qual teria sido o aumento verificado na alienação seguinte[341].

Historicamente, os originais das obras podem alcançar uma enorme valorização ao longo do tempo. Há numerosos exemplos nesse sentido. A obra "No.5", de Jackson Pollock, foi vendida por U$D 140 milhões em 2006, maior valor por esse tipo de aquisição até aquele momento[342]. Já em 2017, a pintura **"Salvator Mundi", de Leonardo da Vinci, foi arrematada por** U$D 450,3 milhões, recorde que ainda permanecia até a elaboração deste texto, em 2022[343]. Em relação ao Brasil, a maior venda foi do quadro "A Caipirinha", de Tarsila do Amaral, em 2020. A obra foi leiloada por R$ 57,5 milhões[344].

A criptoarte também tem registos de grande valorização de obras digitais. Somente em 2021 já foram noticiados vários negócios milionários executados por meio desse novo modelo, com destaque para a venda de uma colagem digital do artista Mike Winkelmann (conhecido como Beeple) pelo valor recorde de US$ 69 milhões[345].

Em relação à valorização tardia das obras, um dos principais exemplos diz respeito ao acervo de Vincent Van Gogh. Em que pese a enorme fama e respeito que o pintor goza nos dias de hoje, ele não usufruiu do mesmo sucesso em vida, tendo vendido poucas obras naquele momento. É conhecido o caso da obra "Doutor Gachet", vendida em 1897 por 300 francos. Quase um século depois, foi leiloada por U$D 82,5 milhões em 1990[346]. Van Gogh talvez seja o maior exemplo de pintor valorizado apenas após sua morte, com consequente impacto nos preços das suas obras[347].

---

340 Artigo 38 da Lei 9.610/98.

341 Ação 0258468-48.2012.8.19.0001.

342 https://exame.com/invest/minhas-financas/os-10-quadros-mais-caros-do-mundo-ja-vendidos-no-mundo/

343 https://exame.com/casual/as-10-obras-de-arte-mais-caras-ja-vendidas/

344 https://g1.globo.com/sp/sao-paulo/noticia/2020/12/17/a-caipirinha-de-tarsila-do-amaral-e-leiloado-por-r-575-milhoes-maior-valor-ja-pago-por-uma-obra-brasileira.ghtml

345 https://g1.globo.com/pop-arte/noticia/2021/03/16/nft-como-funciona-o-registro-de-colecoes-digitais-que-ja-valem-milhoes-de-dolares.ghtml

346 https://exame.com/invest/minhas-financas/os-10-quadros-mais-caros-do-mundo-ja-vendidos-no-mundo/

347 "A obra de arte gráfica ou plástica tem como característica especial principal o denominado *droit de suíte*, ou direito de sequência, oriundo da França para proteção dos pintores que, mortos, enriquecem os *merchands*, enquanto os sucessores não desfrutavam da exploração de direitos patrimoniais". (CHINELLATO, 2015, p. 312)

A questão do aumento do preço das criações após o falecimento do autor naturalmente gerou debates sobre a transferência (ou não) do direito de sequência aos seus herdeiros. A Convenção de Berna e o artigo 38 da Lei 9.610/98 indicam expressamente que se trata de direito irrenunciável e inalienável, sem fazer referência à questão da sucessão:

> A Convenção de Berna declara o direito de sequência inalienável. O art. 39 acrescenta irrenunciável[348]. Outros dizem-no também imprescritível. [...] Não se pode imaginar que o autor que aliene um quadro aliene simultaneamente o direito de sequência. Isso iria contra toda a ratio do preceito, que é a de proteger o autor contra as suas alienações precipitadas e fazê-lo participar dos incrementos posteriores de valor. O mesmo há a dizer da renúncia ao direito de sequência. A irrenunciabilidade tutela o autor, como parte eventualmente mais fraca, a quem podia ser imposta a renúncia ao seu direito – por exemplo, a galeria de arte a que tivesse que recorrer para a venda. (ASCENSÃO, 2007, p. 242 e 243)

No Brasil, o caso mais conhecido sobre o tema é o Recurso Especial 594.526-RJ, julgado pelo Superior Tribunal de Justiça, em 2009. Trata-se de ação ajuizada por um dos herdeiros do pintor Cândido Portinari contra o Banco do Brasil, que havia recebido obras do autor em pagamento de um empréstimo, as revendeu com lucro e não quitou o direito de sequência:

> Trata-se, na origem, de ação de indenização por danos materiais e morais ajuizada por João Candido Portinari em face de Banco do Brasil S/A. Informa o autor que a empresa Candido Portinari Serviços, Indústria e Comércio Ltda, constituída para sustentar o projeto cultural denominado "Projeto Portinari", que visa a divulgação da vida e obra de seu finado pai, para continuar mantendo suas atividades, contraiu empréstimo junto ao Banco réu, tendo o autor como fiador. O valor total do empréstimo era de R$ 45.190,10 (quarenta e cinco mil, cento e noventa reais e dez centavos).
>
> Diante da impossibilidade de honrar o empréstimo, o autor deu em pagamento, como quitação total da dívida e acréscimos contratuais, obras originais de autoria de seu pai (28 - vinte e oito desenhos), avaliadas em R$ 73.710,31 (setenta e três mil, setecentos e dez reais e trinta e um centavos), segundo afirma a preço vil. Na posse das peças, o Banco réu realizou leilão, logrando obter com a venda dos desenhos, segundo informações da imprensa, o preço total de R$ 163.800,00 (cento e sessenta e três mil e oitocentos reais). Contudo, segundo o autor, embora notificado, o Banco do Brasil não realizou o pagamento da participação de 20% sobre o aumento do preço obtido na alienação das obras, quantia esta devida ao autor à título de "direito de seqüência". (STJ, REsp 594.526-RJ, Ministro Relator Luís Felipe Salomão).

A celeuma era definir se o direito de sequência seria passível de transferência via herança. No caso, o STJ entendeu que, por se tratar de uma espécie de direito

[348] Artigo 38, na Lei de Direitos Autorais brasileira.

autoral patrimonial, haveria sim transferência causa mortis, passando a ser devido aos herdeiros.

Outra questão que se aplica de forma recorrente ao direito de sequência é a dificuldade de seu monitoramento. Muitas obras não têm sequer seu proprietário atual conhecido e vários autores registam dificuldade em acompanhar as transações envolvendo o bem[349]:

> Trata-se de um instituto polêmico desde o seu nascimento, tanto para os artistas quanto para os seus usuários, uma vez que as regras estabelecidas interferem, diretamente, na comercialização das obras de artes plásticas, a gerar reflexos de natureza fiscal que decorrem da realização do próprio negócio, usualmente desprezados pelas partes envolvidas. É sabido que ninguém divulga ser proprietário de um quadro de Volpi ou de Salvador Dali, muito menos que deseja negociá-lo ou que o tenha vendido por um determinado preço. Quando o negócio se realiza, ele se dá quase sempre de modo silencioso, vindo a ser formalizado mediante o pagamento do preço pelo adquirente e a entrega da obra pelo próprio artista, ou por quem detém a titularidade desses direitos. (PONTES, 2015, p. 279 e 280)

Nesse contexto, o uso da tecnologia blockchain pode, em tese, ser um instrumento favorável aos autores na questão do direito de sequência aplicado aos NFTs. Isso porque, nesse caso, é possível registar de forma definitiva as transações por meio da arquitetura de software utilizada pelo sistema. Logicamente, isso seria capaz de indicar as transações envolvendo o NFT e, portanto, facilitar ao autor o exercício do seu direito de sequência.

Porém, a situação pode ser complexa na prática. As transações via blockchain podem ser criptografadas, o que ocultaria a identificação precisa das partes da transação de venda do NFT[350]. Essa é uma questão relevante, que deve ser ainda objeto de debates futuros, inclusive judiciais. O registo via blockchain das transações

---

349 "A questão é que, na prática, é muito difícil ao autor o exercício desse direito. As revendas normalmente se fazem longe do seu alcance, tendo o criador, a essa altura, muitas vezes já perdido completamente o contato com a obra. É de fato impossível ao autor estar em todas as feiras, exposições e demais mercados de circulação e comercialização da arte". (MENEZES, 2007, p. 88)

350 "At its heart then, the blockchain is simply a ledger of transactions, much like an electronic version of a handwritten bank ledger. But the blockchain ledger is unusual and profound in at least two ways. First, the blockchain records all of the transactions that ever occurred within the network. The technology of the blockchain is such that one party cannot make any transaction without the transaction being duly recorded in the authoritative ledger. Like the Domesday Book of William the Conqueror, the blockchain ledger tells the complete story of the division of property interests. Second, the blockchain ledger is public and promiscuous. All blockchains are transparent to the members of the blockchain, and once you become a member of a blockchain, you become privy to a complete copy of every transaction ever made on that blockchain. Members on a blockchain are identified with "addresses" rather than as specific persons. These "addresses" are the public side of a private/public cryptographic key pair (an address is a hash of the public key.) Knowing the private key allows individuals to link themselves to the address, and therefore perform transactions on the ledger on behalf of that address". (TRESISE, GOLDENFEIN e HUNTER, 2018, p. 02 e 03)

envolvendo NFTs por si só já parece representar um avanço em relação ao monitoramento das operações de vendas das obras, o que é hoje mais difícil no caso das artes. Porém, no caso de haver informações criptografadas, deve-se avaliar como e se tais dados poderiam ser revelados (inclusive mediante ordem judicial) e por quem. Essa é uma pergunta especialmente relevante no caso de objetos certificados via blockchain, considerando o sistema pulverizado de verificação que é utilizado por essa tecnologia.

Por outro lado, a tecnologia permite que o NFT contenha um smart contract que execute automaticamente a transferência do valor referente ao direito de sequência ao autor a cada venda do token[351]. Sob esse aspecto, o blockchain parece oferecer um mecanismo que pode ter grande eficiência na execução desse tipo de direito, que historicamente tem sido objeto de queixas, por parte dos autores, em relação à dificuldade de seu cumprimento efetivo[352]. Não se pode perder de vista, entretanto, que a existência dos smart contracts na cadeia implica custos maiores para a geração do bloco e execução das transações, uma vez que existe uma necessidade de maiores recursos computacionais para processamento das operações contendo os comandos inseridos por meio desse mecanismo[353].

Diante de todas essas questões, a conclusão principal é a de que as obras de arte digital certificadas por meio de NFTs podem ser consideradas como originais para fins de aplicação da legislação, especialmente quanto à não aquisição automática dos direitos autorais e também do direito de sequência.

---

351 "Furthermore, artists in general cases cannot receive royalties from future sales of their works. In contrast, NFTs can be programmed so that the artist receives a predetermined royalty fee each time when his digital artwork exchanges in the markets (e.g., SuperRare, MakersPlace, Rare Art Lab, VIV3). This is an efficient way to manage and protect digital masterpieces. In addition, several platforms (e.g. Mintbase and Mintable) have even established tools to support ordinary people to create their own NFT works easily". (WANG *et alli*, 2021, p. 12)

352 "Consider Rarible, a marketplace for unique digital art. To use the site, an artist creates a work. They then tokenize copies of the artwork, assigning each to a unique NFT. Creators transfer NFTs through the marketplace to collectors, who can in turn transfer the tokens further to other interested buyers as the digital assets rise in value. Because they are tokenized, the digital artworks are limited in number, and the smart contract governing token ownership cannot itself be altered once hashed to the blockchain. Rarible recreates a central aspect of the physical art world in the digital space—the ability to capture the rise in value of a piece of art. Prior to NFTs and marketplaces like Rarible, people were unable to effectively trade in decentralized digital assets. Rarible creates a marketplace that not only has led to a burgeoning trade in NFTs as buyers sell their purchases forward, but also allows content creators to make money from downstream sales of their products. Such an incentive, while unusual in the realm of IP, may lead to an increase in artists adopting the platform in the early stages of NFT development". (FAIRFIELD, 2021, p. 27)

353 "High gas prices have become a major problem for NFT marketplaces, especially when minting the NFTs at a large scale that requires uploading the metadata to the blockchain network. Every NFT-related transactions are more expensive than a simple transfer transaction because smart contracts involve computational resources and storage to be processed. At the time of writing, to mine an NFT token costs over USD 60 (equivalently in around 5 x 10^2 *wei*). To complete a simple NFT trade can run between USD 60 and USD 100 for each transaction. Expensive fees caused by complex operations and high congestion greatly limit its wide adoption". (WANG *et alli*, 2021, p. 13)

Conclusões

O fenômeno dos NFTs na criptoarte tem gerado diversos debates e chamado atenção, especialmente por causa dos grandes valores envolvidos em algumas transações. Sendo importante lembrar que não é a primeira vez que o mercado de arte se depara com preços elevados em situações que poderiam ser consideradas excêntricas, de modo que é importante considerar que não se trata necessariamente de casos pontuais:

> Long before cryptocurrency speculators got involved, art prices were capricious—as the British artist Banksy no doubt understands. Recently, the work "Game Changer," which he delivered unsolicited to an English hospital last year, earned it $23.2 million at auction—about $20 million more than experts had predicted. Banksy has famously mocked high-priced sales: In 2006's "Morons," he portrays an auction house selling a work that reads I CAN'T BELIEVE YOU MORONS ACTUALLY BUY THIS SHIT. (ZITTRAIN e MARKS, 2021)

Nesse sentido, é fundamental que as situações que possam gerar dúvidas sejam estudadas, visando a promover segurança jurídica aos envolvidos, fundamental para qualquer modelo de negócio[354]. O enquadramento dos NFTs como certificados de obras originais no âmbito da criptoarte é uma das questões mais relevantes nesse contexto, uma vez que isso gera consequências relevantes em função da legislação de Direitos Autorais.

Como indicado no presente texto, o desconhecimento das regras jurídicas aplicáveis às criações intelectuais pode gerar desdobramentos desastrosos para os compradores das obras, como é o exemplo da pessoa que compra o original achando que passa automaticamente a ser o titular dos Direitos Autorais também, o que não é verdade. A questão do direito de sequência é também extremamente relevante, inclusive porque há posicionamentos no sentido de que as revendas dos NFTs não deveriam gerar ganhos para o criador da obra[355]. Porém, no Brasil, essa questão é assegurada pela legislação como um direito do autor e deve ser respeitada. Logo, a

---

354 "Given the rapidly expanding importance of NFTs, lawyers must develop a stable way of characterizing and protecting these interests. This piece aims to lay bare the foundational problems in the legal regime surrounding NFTs, with the goal of permitting the technology (and its adopters) to benefit from strong and simple personal property interests when they buy or sell NFTs". (FAIRFIELD, 2021, p. 12)

355 "Constraints on the purchaser's right to transfer cut to the very heart of the NFT value proposition. [...] The buyer of art on the Rarible marketplace purchases a token tied to a piece of art. The art and the token are bound together by a URL and perhaps a metadata file pointing to and describing the artwork, so that the token proves that it is related to the art. But the token is not itself the art. The token merely shows that the token and the art have an immutable and unfalsifiable relationship. When the owner of a token tied to a piece of art on Rarible goes to sell that art, a portion of the sales price will be conveyed back to the creator of the token. Creators certainly have an incentive to sell their works, as they capture a fraction of each resale forward. But the result is the opposite of normal rules for the sale of goods. A book, once sold, does not kick back a percentage of future sales to the author. When we buy a car, we do not expect a portion of its sales price to be forwarded back to the person who sold it to us when we go to sell it. Tokens that claw back a portion of the profit each time they are resold do not square with the representation that a buyer of an NFT owns it free and clear". (FAIRFIELD, 2021, p. 36 a 38)

adequada compreensão desse aspecto jurídico é fundamental para o funcionamento do mercado de criptoarte, considerando inclusive que muitos compradores fazem a aquisição na expectativa de obter lucro em uma revenda futura[356]. Porém, como determinado pela Lei 9.610/98, parte desses ganhos deve ser compartilhada com o autor da obra.

Por fim, é relevante notar que a adoção da tecnologia blockchain no âmbito da criptoarte, por meio dos NFTs, disponibiliza ferramentas importantes para efetivação do direito de sequência. Este pode ser assegurado, do ponto de vista prático, por meio de smart contracts que realizem automaticamente o pagamento devido ao autor em cada revenda. Essa inovação pode se mostrar revolucionária para a aplicação desse direito, que, apesar de previsto há muito tempo na legislação, historicamente sempre se mostrou bastante difícil de ser plenamente observado. Essa perspectiva mostra que a introdução dos NFTs no mercado da arte não significa apenas uma nova forma de criar e ofertar obras, mas também pode trazer mudanças na própria aplicação concreta do Direito Autoral. Logo, é importante que haja mais estudos conjuntos sobre os dois temas, fundamentais para as novas tendências do mercado de arte.

Referências bibliográficas

ADOLFO, Luiz Gonzaga Silva e SOUZA Laís Cristina de. Ser ou Não Ser: o dilema hamletiano do pirata e a fundamentalidade que há no acesso à informação como no direito autoral. *in* SANTOS, Manoel J. Pereira (org.). *Direitos de Autor e Direitos Fundamentais.* São Paulo: Saraiva, 2011.

ASCENSÃO, José de Oliveira. *Direito Autoral.* 2ª ed. Rio de Janeiro: Renovar, 2007.

ASSAFIM, João Marcelo de Lima. *A Transferência de Tecnologia no Brasil:* Aspectos Contratuais e Concorrenciais da Propriedade Industrial. Rio de Janeiro: Lúmen Júris, 2005.

AZEVEDO, Paulo Furquim de. Organização Industrial. *in* MONTORO FILHO, André Franco *et al. Manual de Economia*: Equipe de Professores da USP. 3ª ed. São Paulo: Saraiva, 1998.

BARBOSA, Denis Borges. *Uma Introdução à Propriedade Intelectual.* Rio de Janeiro: Editora Lumen Juris, 2003.

_____. Marca e Status – Os Nichos da Concorrência Conspícua. *in* BARBOSA, Denis Borges. *Usucapião de Patentes e Outros Estudos de Propriedade Intelectual.* Rio de Janeiro: Lumen Juris, 2006.

BARLOW, John Perry. *A Declaration of the Independence of Cyberspace*. Davos: 1996. Disponível em https://www.eff.org/pt-br/cyberspace-independence. Acesso em 21/09/2022.

BRANCO JÚNIOR, Sérgio Vieira. *Direitos Autorais na Internet e o Uso de Obras Alheias.* Rio de Janeiro: Lumen Juris, 2006.

BRAUN-DUBLER, Nils, GIER, Hans-Peter, BULATNIKOVA, Tetiana, LANGHART, Manuel, MERKI, Manuela, ROTH, Florian, BURRET, Antoine e PERDRISAT, Simon. Blockchain: Capabilities,

356 "There is significant unmet market demand for digital personal property. That is, for example, what bitcoin does: it thrives on aftermarket demand for bitcoin. Owners expect to capture any rise in their property's value, and to be able to sell the property to the next purchaser. Thus, the initial purchase (the market) is less the point than the later sales (the aftermarket). For many NFTs, the aftermarket is the entire point. A buyer of a piece of art, or a trading card, or a unique digital pet expects to be able to profit from its rise in value". (FAIRFIELD, 2021, p. 92)

Economic Viability, and the Socio-Technical Environment. 2020. Disponível em https://www.researchgate.net/publication/342327813_Blockchain_Capabilities_Economic_Viability_and_the_Socio-Technical_Environment. Acesso em 05/10/2022.

BRUNA, Sérgio Varella. *O Poder Econômico e a Conceituação do Abuso em Seu Exercício*. São Paulo: Editora Revista dos Tribunais, 2001.

CANÇADO, Maria de Lourdes Flecha de Lima Xavier. Ato Administrativo *in* MOTTA, Carlos Pinto Coelho (coord). *Curso Prático de Direito Administrativo*. 2. ed. Belo Horizonte: Del Rey, 2004.

CHINELLATO, Silmara Juny de Abreu. Requisitos Fundamentais Para a Proteção Autoral de Obras Literárias, Artísticas e Científica. Peculiaridades da Obra de Artes Plásticas. *in* MAMEDE, Gladston, FRANCA FILHO, Marcílio Toscano e RODRIGUES JÚNIOR, Otávio Luiz. *Direito da Arte*. São Paulo: Atlas, 2015.

COOTER, Robert e ULEN, Thomas. *Law And Economics*. 6 ed. Boston: Pearson, 2016.

DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. 19 ed. São Paulo: Atlas, 2006.

FAIRFIELD, Joshua. *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*. (April 6, 2021). Indiana Law Journal: Vol. 97: Iss. 4, Article 4. Disponível em: https://ssrn.com/abstract=3821102. Acesso em 13/02/2022.

FINCK, Michèle. *Blockchains and Data Protection in the European Union*. European Data Protection Law Review. Berlin: Lexxion. v. 04, n. 01, p. 17-35, Feb. 2018. Disponível em https://ssrn.com/abstract=3080322

FORGIONI, Paula A. *Os Fundamentos do Antitruste*. 2ª ed. São Paulo: Editora Revista dos Tribunais, 2005.

GALVES, Carlos. *Manual de Economia Política Atual*. 15ª ed. Rio de Janeiro: Forense, 2004.

GUIMARÃES, Susana Serrão. *Proteção Legal do Design*. São Paulo: Limiar, 2005.

HARDIN, Garret. A Tragédia dos Comuns. *Science*. Vol. 162, n. 3859. Tradução de José Roberto Bonifácio. Washington (EUA): American Association for the Advancement of Science, 1968. Disponível em <https://edisciplinas.usp.br/pluginfile.php/3203283/mod_resource/content/2/a_trag%C3%A9dia_dos_comuns.pdf.> Acesso em 22/08/2022.

HARRISON, Jeffrey L., *Trademark Law and Status Signaling: Tattoos for the Privileged*, 59 Fla. L. Rev. 195 (2007). Disponível em http://scholarship.law.ufl.edu/facultypub/180 . Acesso em 24/08/2022.

IRTI, Natalino. A Ordem Jurídica do Mercado (tradução de Alfredo Copetti Neto e André Karam Trindade). *Revista de Direito Mercantil, Industrial, Econoômico e Financeiro*. n. 145 (jan/mar). São Paulo: Malheiros, 2007.

LANDES, William M. e POSNER, Richard A. *The Economic Structure of Intellectual Property Law*. Cambridge (EUA): Belknap Press of Harvard University Press, 2003.

LEIBENSTEIN, Harvey. Bandwagon, Snob, and Veblen Effects in the Theory of Consumers' Demand. *The Quarterly Journal of Economics*. Vol. 64, No. 2. Nova Iorque: Oxford University Press, 1950.

LEITE, Eduardo Lycurgo. A História do Direito de Autor no Ocidente e os Tipos Móveis de Gutenberg. *Revista de Direito Autoral*. v. 1, n. 2. Rio de Janeiro: Lumen Juris, 2005.

LESSIG, Lawrence. *Free Culture: The Nature and Future of Creativity*. Nova Iorque: Penguin Books, 2005.

LUCCA, Newton de e PARENTONI, Leonardo Netto. Arte em Crise: Breves Notas Sobre o Regime Jurídico Aplicável às Obras de Arte na Recuperação Judicial de Empresas e na Falência. *in* MAMEDE, Gladston, FRANCA FILHO, Marcílio Toscano e RODRIGUES JÚNIOR, Otávio Luiz. *Direito da Arte*. São Paulo: Atlas, 2015.

MELO, Renato Dolabella. *Indicações Geográficas e o Direito da Regulação e da Concorrência.* Rio de Janeiro: Lumen Juris, 2019.

MENEZES, Elisângela Dias. *Curso de Direito Autoral.* Belo Horizonte: Del Rey, 2007.

MONTORO FILHO, André Franco. Teoria Elementar do Funcionamento do Mercado. *in* MONTORO FILHO, André Franco *et al. Manual de Economia*: Equipe de Professores da USP. 3ª ed. São Paulo: Saraiva, 1998.

MOREIRA, Arthur Salles de Paula, DELGADO, Camila Campos Baumgratz e SANTOS, Gabriel Gonçalves. Repensando a tecnologia blockchain: por que nem tudo o que você leu até hoje era verdade? *in* PARENTONI, Leonardo; MILAGRES, Marcelo de Oliveira; VAN DE GRAAF, Jeroen (Coords). MOREIRA, Arthur Salles de Paula; CHAGAS, Ciro Costa; SANTANA, Mariana Damiani (Orgs). *Direito, Tecnologia e Inovação* - v. III: Aplicações Jurídicas de Blockchain. Belo Horizonte, 2021.

NETANEL, Neil Weinstock. *Copyright´s Paradox.* Nova Iorque: Oxford University Press, 2008.

NOVOA, Carlo Fernandez. Funciones de Marca. *Actas de Derecho Industrial.* n. 5. Madri: Montecorvo, 1978.

NUSDEO, Fábio. *Curso de Economia:* Introdução ao Direito Econômico. 4ª ed. São Paulo: Editora Revista dos Tribunais, 2005.

PAAR, Christof e PELZL, Jan. *SHA-3 and The Hash Function Keccak*: *Understanding Cryptography A Textbook for Students and Practitioners.* Berlin: Springer, 2010.

PARANAGUÁ, Pedro e BRANCO, Sérgio. *Direitos Autorais.* Rio de Janeiro: Editora FGV, 2009.

PARENTONI, Leonardo Netto. *Documento Eletrônico: Aplicação e Interpretação pelo Poder Judiciário.* Curitiba: Juruá, 2007.

_____; VALENTINI, Rômulo Soares; ALVES, Tárik César Oliveira e. Panorama da regulação da inteligência artificial no Brasil: com ênfase no PLS N. 5.051/2019. Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, RS, v. 15, n. 2, e43730, mai./ago. 2020. ISSN 1981-3694. DOI: http://dx.doi.org/10.5902/1981369443730. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/43730. Acesso em: 16/08/2022.

PEREIRA, Caio Mário da Silva. Instituições de Direito Civil – Introdução ao Direito Civil e Teoria Geral de Direito Civil. v. 1, 20. ed. Rio de Janeiro: Forense, 2000.

PONTES, Hidelbrando. O Regime Jurídico dos Criadores de Obras de Artes Plásticas e Seus Titulares. *in* MAMEDE, Gladston, FRANCA FILHO, Marcílio Toscano e RODRIGUES JÚNIOR, Otávio Luiz. *Direito da Arte*. São Paulo: Atlas, 2015.

PONTES, Leonardo Machado. *Creative Commons – Problemas Jurídicos e Estruturais.* Belo Horizonte: Arraes, 2013.

PONTES DE MIRANDA, Francisco Cavalcanti. *Tratado de Direito Privado.* Tomo 16. Atualização de Vilson Rodrigues Alves. Campinas: Bookseller, 2002.

PORTO, Patrícia Carvalho da Rocha. *Quando a Propriedade Industrial Representa Qualidade.* Rio de Janeiro: Lumen Juris, 2011.

POTTS, Jason e RENNIE, Ellie. *Blockchains and Creative Industries*. 2017. Disponível em https://ssrn.com/abstract=3072129 or http://dx.doi.org/10.2139/ssrn.3072129. Acesso em: 11/10/2022.

PUERTO, Manuel Jesús Rodríguez. Internet y los Problemas del Concepto de Derecho. *in* CUEVAS, Guillermo Cabanellas de las e OCA, Ángel Montes de (org). *Derecho de Internet*. 2. ed. Buenos Aires: Heliasta, 2012.

POSNER, Richard A. *Economic Analysis of Law*. 7ª ed. Boston: Little, Brown and Company, 2007.

ROSSETTI, José Paschoal. *Introdução à Economia.* 15 ed. São Paulo: Atlas, 1991.

RIZZIERI, Juarez Alexandre Baldini. Introdução à Economia. *in* MONTORO FILHO, André Franco *et al. Manual de Economia*: Equipe de Professores da USP. 3ª ed. São Paulo: Saraiva, 1998.

SANDRONI, Paulo. *Novíssimo Dicionário de Economia.* São Paulo: Best Seller, 1999.

SANTOS, Manuella Silva dos. *Direito Autoral na Era Digital: impactos, controvérsias e possíveis soluções*. São Paulo: Saraiva, 2009.

SILVEIRA, Newton. *Propriedade intelectual*. Barueri: Manole, 2005.

SOUSA, Isabella de Lima França. O Uso da Tecnologia Blockchain em Contratos de Seguro de Dano no Brasil. *Direito Unifacs – Debate Virtual.* n. 267. Salvador: UNIFACS, 2022.SZTAJN, Rachel, ZYLBERSZTAJN, Decio e MUELLER, Bernardo. Economia dos Direitos de Propriedade. *in* ZYLBERSZTAJN, Decio e SZTAJN, Rachel (org.) *Direito e Economia.* Rio de Janeiro: Elsevier, 2005. TEIXEIRA, Rodrigo Alves. A Produção Capitalista do Conhecimento e o Papel do Conhecimento na Produção Capitalista: Uma Análise a partir da Teoria Marxista do Valor. *EconomiA - Revista da ANPEC (Associação Nacional dos Centros de Pós-Graduação em Economia)*. Vol. 10, n. 2. Rio de Janeiro: Elsevier, 2009.

TRAUTMAN, Lawrence J. Virtual Art and Non-fungible Tokens. *50 Hofstra Law Review 361*. 2022. Disponível em SSRN: https://ssrn.com/abstract=3814087 ou http://dx.doi.org/10.2139/ssrn.3814087. Acesso em 05/10/2022.

TRESISE, Annabel, GOLDENFEIN, Jake e HUNTER, Dan. What Blockchain Can and Can't Do for Copyright. *Australian Intellectual Property Journal*. v. 144. 2018. Disponível em https://ssrn.com/abstract=3227381. Acesso em: 08/10/2022.

VEBLEN, Thorstein. *The Theory of the Leisure Class: An Economic Study of Institutions.* Nova Iorque: Macmillan, 1902.

WANG, Qin, LI, Rujia, WANG, Qi e CHEN, Shiping. *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges* (Tech Report). 2021. Disponível em https://www.researchgate.net/publication/351656444_Non-Fungible_Token_NFT_Overview_Evaluation_Opportunities_and_Challenges. Acesso em 07/10/2022.

ZITTRAIN, Jonathan e MARKS, Will. *What Critics Don't Understand About NFTs - The complexity and arbitrariness of non-fungible tokens are a big part of their appeal.* The Atlantic.0 2021. Disponível em https://www.theatlantic.com/ideas/archive/2021/04/nfts-show-value-owning-unownable/618525/ . Acesso em 12/10/2022.

III_Legislação e Jurisprudência Comentadas

Acórdão do Tribunal de Justiça nos Processos Apensos C-37/20 | Luxembourg Business Registers E C-601/20 | SOVIM

Diretiva antibranqueamento: a disposição que prevê que as informações sobre os beneficiários efetivos das entidades societárias constituídas no território dos Estados-Membros devem estar acessíveis em todos os casos a qualquer membro do público em geral é inválida

A ingerência nos direitos garantidos pela Carta decorrente desta medida não se limita ao que é estritamente necessário nem é proporcionada ao objetivo prosseguido

Em conformidade com a Diretiva antibranqueamento[357], foi adotada em 2019 uma lei luxemburguesa[358] que instituiu um Registo dos Beneficiários Efetivos e que prevê que determinadas informações sobre os beneficiários efetivos das entidades registadas devem neste ser inscritas e conservadas. Algumas dessas informações estão acessíveis a qualquer membro do público em geral, podendo esse acesso realizar-se nomeadamente através da Internet. Esta lei prevê igualmente a possibilidade de um beneficiário efetivo pedir ao Luxembourg Business Registers (LBR), gestor do Registo, que, em determinados casos, limite o acesso a estas informações.

Neste contexto, foram interpostos no tribunal d'arrondissement de Luxembourg (Tribunal de Primeira Instância do Luxemburgo, Luxemburgo), respetivamente por uma sociedade luxemburguesa e pelo beneficiário efetivo dessa entidade, dois recursos em cujo âmbito foi sem sucesso pedido que o LBR limitasse o acesso a qualquer membro do público em geral das informações que lhes dizem respeito. Por considerar que a divulgação de tais informações comporta um risco desproporcionado de violação dos direitos fundamentais dos beneficiários efetivos em questão, este último tribunal submeteu ao Tribunal de Justiça várias questões prejudiciais relativas à interpretação de certas disposições da diretiva

357 Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, que altera o Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (JO 2015, L 141, p. 73), conforme alterada pela Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018 (JO 2018, L 156, p. 43).

358 Lei de 13 de janeiro de 2019 que institui um registo dos beneficiários efetivos (Mémorial A 15).

antibranqueamento e sobre a validade destas à luz da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

No seu acórdão hoje proferido, o Tribunal de Justiça, reunido em Grande Secção, declara **a invalidade**, à luz da Carta, da disposição da diretiva antibranqueamento que prevê que os Estados-Membros devem assegurar que as informações sobre os beneficiários efetivos das entidades societárias e outras pessoas coletivas constituídas no seu território **sejam acessíveis em todos os casos a qualquer membro do público em geral**.

Segundo o Tribunal, o acesso do público em geral às informações sobre os beneficiários efetivos constitui uma ingerência grave nos direitos fundamentais de respeito pela vida privada e de proteção dos dados pessoais, consagrados respetivamente nos artigos 7.º e 8.º da Carta. Com efeito, as informações divulgadas permitem que um número potencialmente ilimitado de pessoas se informe sobre a situação material e financeira de um beneficiário efetivo. Além disso, as consequências potenciais, para os titulares dos dados, resultantes de uma eventual utilização abusiva dos seus dados pessoais são agravadas pelo facto de que, depois de terem sido disponibilizados ao público em geral, esses dados podem não apenas ser livremente consultados, como podem também ser conservados e difundidos.

No entanto, o Tribunal observa que, com a medida em causa, o legislador da União visa prevenir o branqueamento de capitais e o financiamento do terrorismo, implementando, através de uma maior transparência, um ambiente menos suscetível de ser utilizado para esses fins. O Tribunal considera que o legislador prossegue assim um objetivo de interesse geral suscetível de justificar ingerências, inclusivamente graves, nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, e que o acesso do público em geral às informações sobre os beneficiários efetivos é adequado a contribuir para a realização deste objetivo.

Contudo, o Tribunal constata que a ingerência decorrente desta medida não se limita ao que é estritamente necessário nem é proporcionada ao objetivo prosseguido. Além de as disposições em causa autorizarem a disponibilização ao público de dados que não estão suficientemente definidos nem são suficientemente identificáveis, o regime introduzido pela diretiva antibranqueamento representa uma violação consideravelmente mais grave dos direitos fundamentais garantidos nos artigos 7.º e 8.º da Carta do que o regime anterior (que previa, além do acesso das autoridades competentes e de certas entidades, o acesso de quaisquer pessoas ou organizações que pudessem provar ter um interesse legítimo), sem que esse agravamento seja compensado por eventuais benefícios que poderiam resultar do novo regime face ao anterior, no que se refere ao combate ao branqueamento de capitais e ao financiamento do terrorismo. Em especial, a eventual existência de dificuldades para definir de maneira precisa as hipóteses e as condições em que existe semelhante interesse legítimo, invocadas pela Comissão, não pode justificar que o legislador da União preveja o acesso do público em geral às informações em questão. O Tribunal acrescenta que as disposições facultativas que permitem aos Estados-Membros, respetivamente, optar por sujeitar a disponibilização das informações sobre os beneficiários efetivos a uma inscrição em linha e por prever, em circunstâncias excecionais, restrições ao acesso do público em geral a essas informações, não são, por si só, suscetíveis de demonstrar uma ponderação equilibrada entre o objetivo de interesse geral prosseguido e os direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, nem a existência de garantias suficientes que permitam aos titulares dos dados proteger eficazmente os seus dados pessoais contra os riscos de abuso.

Processo C-37/20 Resumo do Pedido de Decisão Prejudicial em Aplicação do Artigo 98.°, N.° 1, do Regulamento de Processo do Tribunal de Justiça

Data de entrada:
24 de janeiro de 2020

Órgão jurisdicional de reenvio:
Tribunal d'arrondissement (Tribunal de Primeira Instância, Luxemburgo)

Data da decisão de reenvio:
24 de janeiro de 2020

Demandante: WM Recorrido:
Luxembourg Business Registers

I. Objeto do processo principal

1 Em 5 de dezembro de 2019, o recorrente WM intentou uma ação no Tribunal d'arrondissement de Luxembourg (Tribunal de Primeira Instância do Luxemburgo), contra o agrupamento de interesse económico Luxembourg BUSINESS REGISTRERS (a seguir «G.I. E. LBR»), com vista a obter a alteração da anulação da decisão adotada pelo referido agrupamento em 20 de novembro de 2019. A referida decisão indeferiu o pedido do recorrente de limitar agrupamento de interesse económico, durante um período de três anos, o acesso aos seus dados no que se refere à sua qualidade de beneficiário económico da sociedade civil imobiliária YO, unicamente às autoridades nacionais, às instituições de crédito e financeiras, bem como aos oficiais de justiça e notários agindo na qualidade de funcionários públicos.

2 O Tribunal d'arrondissement de Luxembourg (Tribunal de Primeira Instância do Luxemburgo), órgão jurisdicional de reenvio, é chamado a pronunciar-se sobre a questão de saber se WM cumpre os requisitos legalmente estabelecidos para que o PT RESUMO DO PEDIDO DE DECISÃO PREJUDICIAL - PROCESSO C-37/20 2 acesso às informações relativas à sua qualidade de beneficiário económico da sociedade civil imobiliária YO seja limitado.

II. Quadro jurídico

1. Direito da União

– Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, conforme alterada pela Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE

3 Nos termos dos considerandos 14 a 16 e 36 da Diretiva 2015/849, conforme alterada:

«(14) A necessidade de dispor de informações exatas e atualizadas sobre o beneficiário efetivo é um fator essencial para rastrear os agentes do crime, que de outro modo poderão dissimular a sua identidade numa estrutura societária. Os Estados-Membros deverão por conseguinte assegurar que as entidades constituídas nos seus territórios nos termos do direito nacional obtêm e conservam informações suficientes, exatas e atuais sobre os seus beneficiários efetivos, além das informações básicas como a denominação social e o endereço, a prova de constituição e a estrutura de propriedade. Tendo em vista o reforço da transparência para combater a utilização abusiva de pessoas coletivas, os Estados-Membros deverão assegurar o armazenamento das informações sobre os beneficiários efetivos num registo central situado fora da sociedade, na plena observância do direito da União. Os Estados-Membros poderão, para esse efeito, utilizar uma base de dados central que recolha as informações sobre os beneficiários efetivos, o registo comercial ou outro registo central. Os Estados-Membros poderão decidir que as entidades obrigadas sejam responsáveis pelo preenchimento do

registo. Os Estados-Membros deverão assegurar que essas informações são colocadas à disposição das autoridades competentes e das UIF em todos os casos e que são fornecidas às entidades obrigadas quando estas tomarem medidas de diligência quanto à clientela. Os Estados-Membros deverão assegurar também que é concedido o acesso às informações sobre os beneficiários efetivos, nos termos das regras aplicáveis em matéria de proteção de dados, a outras pessoas que possam provar um interesse legítimo no que diz respeito ao branqueamento de capitais, ao financiamento do terrorismo e às infrações subjacentes associadas — tais como a corrupção, os crimes fiscais e a fraude. As pessoas que possam provar um interesse legítimo deverão ter acesso às informações sobre a natureza e extensão do interesse económico detido que expressem o seu peso aproximado. LUXEMBOURG BUSINESS REGISTERS 3
(15) Para esse efeito, os Estados-Membros deverão poder, nos termos do direito nacional, autorizar um acesso mais amplo do que o acesso previsto pela presente diretiva.

(16) Deverá ser assegurado o acesso atempado às informações sobre os beneficiários efetivos em moldes que evitem qualquer risco de alerta (tipping-off) da sociedade em causa.

[…]

(36) Além disso, com o objetivo de assegurar uma abordagem proporcionada e equilibrada e para garantir os direitos à vida privada e à proteção dos dados pessoais, os Estados-Membros deverão poder prever exceções à divulgação e ao acesso a tais informações sobre os beneficiários efetivos através dos registos, em circunstâncias excecionais, se essas informações expuserem o beneficiário efetivo a um risco desproporcionado de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação. […]»

4 O artigo 30.°, n.° 9, da Diretiva 2015/849/CE, conforme alterada, dispõe:

«Em circunstâncias excecionais a definir no direito nacional, se o acesso a que se refere o n.° 5, primeiro parágrafo, alíneas b) e c), expuser o beneficiário efetivo a risco desproporcionado, risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação, ou se o beneficiário efetivo for menor ou legalmente incapaz, os Estados-Membros podem prever uma isenção do acesso

à totalidade ou a parte das informações sobre o beneficiário efetivo numa base casuística. Os Estados-Membros asseguram que essas isenções são concedidas aquando de uma avaliação pormenorizada do caráter excecional das circunstâncias. […]»

2. Direito nacional

5 A Diretiva 2015/849 foi transposta para o direito luxemburguês pela loi du 13 janvier 2019 instituant un Registre de bénéficiaires effectifs (Lei de 13 de janeiro de 2019 que que institui um registo dos beneficiários efetivos.

6 Por força do artigo 15.°, n.° 1, da Lei de 13 de janeiro de 2019:

«Uma entidade registada ou um beneficiário efetivo podem solicitar, com base numa avaliação casuística e nas circunstâncias excecionais a seguir indicadas, com base num pedido devidamente fundamentado dirigido ao gestor, que o acesso à informação prevista no artigo 3.° fique limitado exclusivamente às autoridades nacionais, às instituições de crédito e financeiras bem como aos oficiais de justiça e notários agindo na qualidade de funcionários públicos, quando esse acesso possa expor o beneficiário a risco desproporcionado, risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação ou quando o beneficiário efetivo seja menor de idade ou incapaz.» RESUMO DO PEDIDO DE DECISÃO PREJUDICIAL - PROCESSO C-37/20 4

III. Factos

7 O recorrente WM, é beneficiário económico de 35 sociedades comerciais e da sociedade civil imobiliária YO. Cada uma destas sociedades solicitou que o acesso a esta informação, tal como definida no artigo 3.° da Lei de 13 de janeiro de 2019, fosse limitado no que se refere ao recorrente, nos termos do artigo 15.° da mesma lei, uma vez que a divulgação desta informação o exporia a ele e à sua família de forma caracterizada, real e atual a «um risco desproporcionado ao risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação». Estes pedidos foram indeferidos por decisões do G.I. E. LBR de 19 e 20 de novembro de 2019, sendo desta última data a decisão relativa à sociedade civil imobiliária YO.

IV. Argumentos das partes

1. WM

8 O recorrente afirma que as suas funções de administrador-geral das sociedades comerciais que operam a nível internacional sob o nome comercial XN o obrigam a deslocar-se com regularidade a países com regimes políticos instáveis e expostos a uma criminalidade de direito comum grave suscetível de o expor a um risco significativo de rapto, sequestro, violência e até de morte. O risco seria ainda maior se fosse revelado que exerce um cargo de direção e que é beneficiário económico de qualquer pessoa coletiva, pois essa qualidade daria origem a uma presunção de que era proprietário dessas pessoas coletivas e de que qualquer tentativa de apropriação indevida de fundos á sua custa seria especialmente lucrativa. Estas circunstâncias obrigam o recorrente a recorrer, nomeadamente, a escolta pessoal e a subscrever um seguro especial para cobrir o risco de rapto, cujos prémios aumentariam consideravelmente se fosse revelado ao público a qualidade de beneficiário económico das empresas em questão.

9 O recorrente apresenta dois argumentos para fundamentar o seu pedido.

10 Por um lado, a proteção conferida pela lei através da possibilidade de limitar o acesso às informações relativas ao estatuto de beneficiário económico não deve ser avaliada em relação às pessoas coletivas, mas em relação à pessoa do beneficiário económico. Uma abordagem diferente desvirtuaria o sentido da lei e o conceito de beneficiário económico. Por conseguinte, há que verificar se o beneficiário económico, nesta qualidade, está exposto um risco mais elevado. É irrelevante que no presente caso a sociedade civil imobiliária YO não exerça uma atividade particularmente exposta ou que em si mesma implique um risco acrescido.

11 Por outro lado, a qualidade de beneficiário económico deve ser examinado em relação a todas as pessoas coletivas em que o requerente tem essa qualidade e não apenas em relação à sociedade civil imobiliária YO. A possibilidade de limitar o acesso à informação é concedida devido ao risco subjetivo a que está exposta uma pessoa específica enquanto beneficiário económico de uma pessoa coletiva. Seria concedida uma proteção indivisível

que abarca todas as entidades em que uma pessoa singular tenha a qualidade de beneficiário económico, desde que a pessoa singular beneficie de tal proteção e relação a uma dessas entidades.

1.2 G.I. E. Luxembourg Business Registers

12 O G.I. E LBR considera que a situação do recorrente não cumpre os requisitos legalmente estabelecidos.

13 Sublinha a filosofia geral dos textos da União Europeia em que se baseia a Lei de 13 de janeiro de 2019, que consiste em garantir um acesso o mais amplo possível à informação sobre a identidade dos beneficiários económicos das pessoas coletivas. O artigo 15.º da Lei de 13 de janeiro de 2019, enquanto derrogação de um princípio geral, deve ser interpretado de forma restritiva.

14 O G.I. E. LBR nega que WM possa invocar, como exige a lei, tanto «circunstâncias excecionais» como a exposição «a um risco desproporcionado, ao risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação».

15 No que respeita ao conceito de «circunstâncias excecionais», o G.I. E. LBR considera que as condições materiais em que o recorrente exerce as suas atividades ou a sua situação financeira não são circunstâncias excecionais, e que admitir o contrário levaria muitas pessoas a beneficiarem da derrogação estabelecida no artigo 15.º da Lei de 13 de janeiro de 2019 o que a privaria em grande medida da sua substância.

16 No que respeita ao conceito de «risco», o G.I. E. LBR alega que este deve ser caracterizado, real, atual e recair efetivamente sobre a pessoa do beneficiário económico. Nega que o acesso à informação relativa à qualidade de WM como beneficiário económico da sociedade civil imobiliária YO «levaria a um aumento desproporcionado dos riscos a que está exposto o beneficiário económico». Em particular, nega que daí se possam tirar conclusões sobre a fortuna do beneficiário económico, ou que, supondo que desta situação se possa inferir a situação financeira, isso poderia levar a um aumento desproporcionado dos riscos a que está exposta essa pessoa.

17 Por outro lado, o G.I. E LBR salienta que WM figura no registre de commerce et des sociétés (registo de comércio e das sociedades) como sócio da sociedade civil imobiliária YO, e que o conceito de sócio é geralmente associado ao de beneficiário económico. Ora, as informações que constam no registo de comércio e das sociedades são, de qualquer modo, acessíveis ao público, pelo que limitar o acesso às informações sobre a qualidade de beneficiário económico não tem qualquer interesse para o recorrente.

18 O G.I. E LBR precisa ainda que o motor de busca do registo de beneficiários económicos não permite efetuar de buscas a partir dos nomes dos beneficiários RESUMO DO PEDIDO DE DECISÃO PREJUDICIAL - PROCESSO C-37/20 6 económicos, permitindo apenas selecionar pessoas coletivas a fim de verificar a identidade dos seus beneficiários económicos. Por conseguinte, a estrutura do seu sistema não permite, exceto à custa de grandes esforços, identificar todas as estruturas em que uma pessoa singular está declarada como beneficiária económica.

2. Apreciação do órgão jurisdicional de reenvio

1. Sobre o conceito de «circunstâncias excecionais»

19 Para beneficiar da restrição de acesso aos seus dados, prevista no n.° 1 do artigo 15.° da Lei de 2019, o beneficiário económico deve justificar que se encontra na situação de «circunstâncias excecionais».

20 O legislador luxemburguês transpôs o conceito de «circunstâncias excecionais a definir no direito nacional», constante do artigo 30.°, n.° 9, da diretiva 2015/849, com a expressão «circunstâncias excecionais a seguir indicadas», considerando que «[u]m risco desproporcionado, risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação, constituem em si mesmos as circunstâncias excecionais que podem justificar um pedido de limitação do acesso às informações que figuram no (registo dos beneficiários efetivos)» (parecer da Comissão de Justiça da Câmara dos Deputados, que reproduz em termos idênticos a posição do Governo expressa no comentário às alterações governamentais de 8 de outubro de 2018).

21 Contudo, o órgão jurisdicional de reenvio questiona-se sobre a questão de saber se a referência na diretiva a precisões a introduzir

pela legislação nacional pode resumir-se no direito nacional a uma remissão «a risco desproporcionado, risco de fraude, rapto, chantagem, extorsão, assédio, de violência ou intimidação», conceitos que já fazem parte das condições de aplicação do regime jurídico decorrente do direito da União, e que consequências deve o tribunal nacional tirar, se for caso disso, do silêncio do seu direito nacional sobre as precisões a introduzir ao conceito de «circunstâncias excecionais».

2. Sobre o conceito de «risco»

22 Além disso, o beneficiário económico deve justificar que o acesso aos seus dados o exporia «a um risco desproporcionado, ao risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação». A lei de transposição reproduziu no essencial os termos do artigo 30.°, n.° 9, da diretiva 2015/849, conforme alterada.

23 Contudo, o órgão jurisdicional de reenvio observa que o conceito de risco a ter em consideração sofreu alterações com a adoção da diretiva 2018/843, passando de uma exposição «ao risco de fraude, rapto, chantagem, violência ou intimidação» para a uma exposição «a risco desproporcionado, risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação». Esta evolução, mediante LUXEMBOURG BUSINESS REGISTERS 7 a inclusão do requisito de «desproporção», pode ser vista como um reforço, em detrimento dos beneficiários económicos, das condições para poder beneficiar da limitação de acesso.

24 Por outro lado, o órgão jurisdicional de reenvio refere que, na versão francesa da diretiva, a condição é enunciada de duas formas diferentes: o considerando 36 refere-se à exposição «a um risco desproporcionado - sem qualquer vírgula - de fraude, rapto, chantagem, extorsão de fundos, assédio, violência ou intimidação», ao passo que o artigo 30.°, por seu turno, se refere à exposição «a risco desproporcionado, risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação». A mesma variação pode ser encontrada na versão inglesa da diretiva, mas não na versão alemã, por exemplo.

25 Esta variação permite duas interpretações possíveis. Nos termos da primeira, a condição do risco é preenchida se o beneficiário económico for exposto a um risco desproporcionado,

independentemente da sua natureza, ou a uma série de outros riscos específicos (fraude, rapto, chantagem, extorsão, assédio, violência, intimidação) sem que todavia devam ser desproporcionados. Nos termos da segunda, a condição de risco é preenchida se o beneficiário económico for exposto à série de riscos acima referidos, sendo o risco específico e desproporcionado em cada caso.

26 Não podendo a imprecisão do texto ser resolvida pela análise das discussões preparatórias para a adoção da Diretiva 2018/843, torna-se necessária a sua interpretação e a remissão ao Tribunal de Justiça da União Europeia.

27 Além disso, a definição do conceito de «risco» suscita, segundo o órgão jurisdicional de reenvio, citando o fundamento apresentado por WM, a questão de saber se o risco em questão deve ser examinado tendo em conta apenas a pessoa do beneficiário económico na sua relação com uma pessoa coletiva específica da qual é beneficiário económico e para a qual pede a limitação de acesso, ou se devem ser tidas em conta as relações de beneficiário económico dessa pessoa com outras pessoas coletivas que possam criar ou agravar o risco a que se expõe. O órgão jurisdicional de reenvio considera que pode ser pertinente analisar se, para caracterizar o risco, pode ter-se em conta uma qualidade diferente da de beneficiário económico noutra entidade, como a de administrador-geral, empregado ou companheiro/cônjuge do beneficiário económico, do administrador-geral ou de um empregado.

28 Por último, o órgão jurisdicional de reenvio questiona-se, remetendo para a argumentação do G.I. E LBR, se o facto de ser notório que WM é beneficiário económico de pessoas coletivas que operam sob a denominação comercial XN, ou pelo menos o seu envolvimento nessas mesmas pessoas coletivas, ou se o facto de essas informações serem facilmente acessíveis por outros meios que não a consulta do registo de beneficiários económicos, beneficia o recorrente. Por conseguinte, há que submeter uma questão prejudicial sobre este ponto ao Tribunal de Justiça da União Europeia. RESUMO DO PEDIDO DE DECISÃO PREJUDICIAL - PROCESSO C-37/20 8

3. Sobre o conceito de risco «desproporcionado»

29 O órgão jurisdicional de reenvio afirma que o critério da «desproporção» parece aplicar-se em qualquer caso para efeitos da apreciação de um pedido destinado a limitar o acesso às informações relativas a um beneficiário económico, independentemente de o risco ser geral ou específico.

30 A aplicação do critério convida à ponderação de dois interesses igualmente dignos de proteção. O artigo 30.°, n.° 9, da Diretiva 20125/849 suscita, portanto, a questão de saber quais os interesses em conflito que devem ser protegidos no âmbito da sua aplicação. Uma primeira leitura da disposição, à luz do objetivo subjacente à Diretiva 2015/849, levam a uma confrontação entre, , por um lado, o objetivo de transparência prosseguido pela Diretiva 2015/849 para promover a luta contra o branqueamento de capitais e o financiamento do terrorismo e, por outro, a proteção da integridade física, moral e financeira do beneficiário económico que pode ser afetado por fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação levados a cabo por terceiros.

31 Uma segunda leitura tem em conta os considerandos da diretiva que precedem o texto legislativo e servem para apreciar o seu alcance. O critério da desproporção, inexistente na Diretiva 2015/849, foi introduzido pela Diretiva 2018/843, nomeadamente no seu considerando 36. Este faz referência ao direito ao respeito da vida privada, que parece abranger um âmbito mais amplo e ao mesmo tempo restrito do que os aspetos de proteção da integridade física, moral e patrimonial (destinados a evitar um risco em geral e/ou os riscos de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação), bem como o direito à proteção dos dados pessoais, que mais uma vez parece ser uma consideração mais limitada do que a proteção da integridade física, moral e patrimonial.

3. Fundamentação do reenvio prejudicial

32 Atendendo às considerações precedentes e às dúvidas quanto à interpretação do artigo 30.°, n.° 9, da Diretiva (UE) 2015/849, necessária para a decisão do litígio no processo principal, o Tribunal d'arrondissement de Luxembourg (Tribunal de Primeira Instância, Luxemburgo) pede ao Tribunal de Justiça da União Europeia que se pronuncie a título prejudicial sobre as seguintes questões.

4. Questões prejudiciais

33 Questão n.° 1: relativa ao conceito de «circunstâncias excecionais»

1 a) Deve o artigo 30.°, n.° 9, da Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, conforme alterada pela Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva LUXEMBOURG BUSINESS REGISTERS 9 (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE, na medida em que subordina a limitação do acesso às informações relativas aos beneficiários económicos a «circunstâncias excecionais a definir pela legislação nacional», ser interpretado no sentido de que autoriza o direito nacional a definir o conceito de «circunstâncias excecionais» unicamente como sendo equivalente a «um risco desproporcionado, um risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação», conceitos que já constituem uma condição para a aplicação da limitação do acesso através da redação do referido artigo30.°, n.° 9?

1 b) Em caso de resposta negativa à questão 1 a), e no caso de a legislação nacional de transposição só ter definido o conceito de «circunstâncias excecionais» mediante a remissão para os conceitos inoperantes de «risco desproporcionado, risco de fraude, rapto, chantagem, extorsão, assédio, de violência ou intimidação», deve o artigo 30.°, n.° 9, já referido, ser interpretado no sentido de que permite ao juiz nacional ignorar a condição das «circunstâncias excecionais», ou deve o referido juiz suprir essa omissão do legislador nacional determinando por via jurisprudencial o alcance do conceito de «circunstâncias excecionais»? Neste último caso, uma vez que, nos termos do artigo 30.°, n.° 9, se trata de uma condição cujo conteúdo é determinado pelo direito nacional, pode o Tribunal de Justiça da União Europeia orientar o juiz nacional na sua missão? Em caso de resposta afirmativa a esta última questão, que diretrizes devem orientar o juiz nacional na determinação do conteúdo do conceito de «circunstâncias excecionais»?

34 Questão n.° 2: relativa ao conceito de «risco»

2 a) Deve o artigo 30.°, n.° 9, da Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, conforme alterada pela Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE, na medida em que subordina a limitação do acesso às informações relativas aos beneficiários económicos «a um risco desproporcionado, risco de fraude, rapto, chantagem, extorsão, assédio, violência ou intimidação», ser interpretado de que remete para um conjunto de oito situações, a primeira das quais responde a um risco geral sujeito à condição de desproporção e as sete seguintes a riscos específicos subtraídos a essa condição, ou no sentido de que remete para um conjunto de sete situações, em que cada uma corresponde a um risco específico sujeito à condição de desproporção?

2 b) Deve o artigo 30.°, n.° 9, da Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de RESUMO DO PEDIDO DE DECISÃO PREJUDICIAL - PROCESSO C-37/20 10 financiamento do terrorismo, conforme alterada pela Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE, na medida em que subordina a limitação do acesso às informações relativas aos beneficiários económicos a «um risco», ser interpretado no sentido de que limita a avaliação da existência e da extensão desse risco apenas às ligações que o beneficiário económico tem com a pessoa coletiva em relação à qual solicita especificamente que seja limitado o acesso à informação relativa à sua qualidade de beneficiário económico, ou no sentido de que implica que sejam tidas em conta as ligações que o beneficiário económico em questão tem com outras pessoas coletivas? Se for necessário ter em conta as ligações com outras pessoas coletivas, deve ser tida em conta apenas a qualidade de beneficiário económico em relação a outras pessoas coletivas ou deve ser tida em conta qualquer ligação com outras pessoas coletivas? Se for necessário ter em conta qualquer ligação

com outras pessoas coletivas, a natureza dessa ligação influencia a avaliação da existência e da extensão do risco?

2 c) Deve o artigo 30.°, n.° 9, da Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, conforme alterada pela Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE, na medida em que subordina a limitação do acesso à informação relativa aos beneficiários económicos a «um risco», ser interpretado no sentido de que exclui o benefício da proteção resultante de uma limitação do acesso quando essas informações, ou outros elementos avançados pelo beneficiário económico para demonstrar a existência e a extensão do «risco» a que está exposto, são facilmente acessíveis a terceiros através de outros meios de informação?

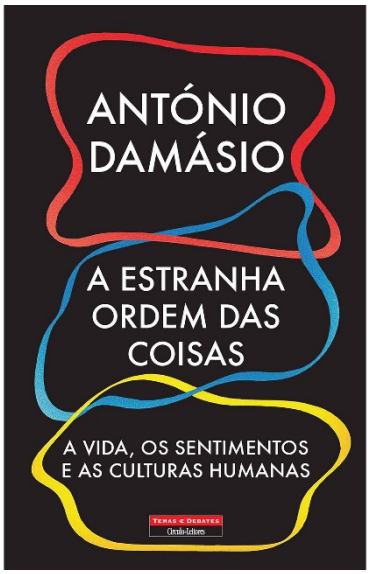
35 Questão n.° 3: relativa ao conceito de risco «desproporcionado»

3) Que interesses divergentes devem ser tidos em consideração no âmbito da aplicação do artigo 30.°, n.° 9, da Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, conforme alterada pela Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE, na medida em que subordina a limitação do acesso à informação relativa a um beneficiário económico à existência de um risco «desproporcionado»?

IV_Recensões

Notícia Bibliográfica

Cristina Maria de Gouveia Caldeira



Apresentamos duas obras distintas, mas que se complementam na sua problematização.

Pedro Domingos, na sua obra: *A revolução do algoritmo mestre*, publicada em 2017, refere que vivemos na era dos algoritmos, e que os mesmos se encontram inseridos no "tecido da vida quotidiana". Não apenas no nosso telemóvel ou computador portatil, mas também em nossa casa, nos nossos eletrodomésticos e brinqudeos. Contudo, é na aprendizagem automática que o autor coloca o enfoque, na medida em que a mesma está a reconfigurar a ciência, a tecnologia, os negócios, a política e a guerra, influenciando todas as dimensões da nossa vida. Com a aprendizagem automática, os computadores escrevem os seus próprios programas, para que não tenhamos de ser nós a fzê-lo. Assim, desde a análise de pedidos de crédito, investimentos na bolsa, seleção de candiatos a emprego e diagnósticos médicos, sem esquecer, os resultados das pesquisas que fazemos na *web*, e os filmes, livros e músicas que são recomendáveis para nós, tudo nos é facultado pela aprendizagem automática, que assim nos vai moldando diariamente, sendo "fundamental que a compreendamos, para utilizarmos cada vez melhor, enquanto cidadãos, consumidores e profissionais".

António Damásio, na sua obra: *A estranha ordem das coisas - a vida, os sentimentos e as culturas humanas*, cuja 1ª edição foi igualmente publicada em 2017, refere que os programas de aprendizagem automática aplicada aos diagnósticos

médicos são uma ferramenta natural, e podem produzir resultados fidedignos. Observa também, que o século XX, promoveu um desenvovimento espantoso na ciência, contudo, embora haja indícios de que é possível conceber organismos artificiais de modo a que operem de forma inteligente, chegando mesmo a ultrapassar a inteligência dos organismos humanos, não há na perspetiva de António Damásio, indícios de que tais organismos artificiais sejam capazes de gerar sentimentos e nada sugere que por si só consigam constituir a base daquilo que nos torna "distintivamente humanos".