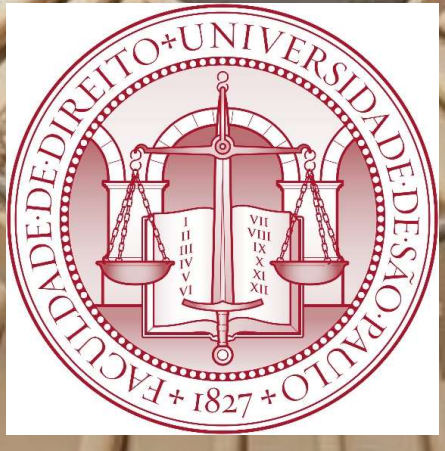
Sociologia do Direito Digital

Inteligência Jurídica na era da inteligência artificial

Organizador
Lucas Fucci Amato



Este livro reúne estudos de uma série de pesquisadores brasileiros (sobretudo vinculados à Universidade de São Paulo) e europeus (de universidades de ponta da Alemanha, França, Itália, Portugal e Reino Unido) sobre os temas mais atuais do direito e da sociedade digital, como inteligência artificial, privacidade de dados pessoais e *fake news*. Hoje, na era da "memeficação" e dos algoritmos, a concentração global de poder econômico, político e midiático pelas *big techs* serve à dissonância cognitiva e à ascensão de ideologias e movimentos autoritários. De outro lado, se pode ser produtivamente instrumentalizada para aumentar a eficiência da gestão de processos decisórios, a inteligência artificial também ameaça hipersimplificar a aplicação do direito, reduzindo-a a um processamento de dados alienado do juízo humano e capaz de produzir, colateralmente, vieses e injustiças graves e massivas.

Faculdade de Direito – Universidade de São Paulo
Portal de Livros Abertos da USP
https://www.livrosabertos.abcd.usp.br/portaldelivrosUSP

Lucas Fucci Amato
organizador

Sociologia do Direito Digital

Inteligência jurídica na era da inteligência artificial

Faculdade de Direito
Universidade de São Paulo
Portal de Livros Abertos da USP
2024

Dados Internacionais de Catalogação na Publicação
Biblioteca da Faculdade de Direito da Universidade de São Paulo

Sociologia do Direito Digital [recurso eletrônico] : inteligência jurídica na era da inteligência artificial / Lucas Fucci Amato, organizador. – São Paulo : Faculdade de Direito, 2024.
354 p.

ISBN 978-85-53062-07-2
DOI: 10.11606/9788553062072
Inclui referências bibliográficas

1. Direito digital. 2. Inteligência artificial. 3. Sociologia jurídica. I. Amato, Lucas Fucci. II. Título: Inteligência jurídica na era da inteligência artificial.

CDU – 34:004.738.5

Bibliotecário Sérgio Carlos Novaes CRB 8 - 6380

DOI: 10.11606/9788553062072

Eu quero entrar na rede
Promover um debate
Juntar via Internet
Um grupo de tietes de Connecticut
De Connecticut acessar
O chefe da Mac-milícia de Milão
Um hacker mafioso acaba de soltar
Um vírus pra atacar programas no Japão
Eu quero entrar na rede pra contactar
Os lares do Nepal, os bares do Gabão
Que o chefe da polícia carioca avisa pelo celular
Que lá na praça Onze tem um vídeo-pôquer para se jogar

(Gilberto Gil, *Pela Internet*, 1997)

Meu novo website
Minha nova fanpage
Agora é terabyte
Que não acaba mais por mais que se deseje
Que o desejo agora é garimpar
Nas terras das serras peladas virtuais
As criptomoedas, bitcoins e tais
Novas economias, novos capitais
Se é música o desejo a se considerar
É só clicar que a loja digital já tem
Anitta, Arnaldo Antunes, eu não sei mais quem
Meu bem, o iTunes tem
De A a Z quem você possa imaginar

Estou preso na rede
Que nem peixe pescado
É zapzap, é like
É instagram, é tudo muito bem bolado
O pensamento é nuvem
O movimento é drone
O monge no convento
Aguarda o advento de Deus pelo iPhone

Cada dia nova invenção
É tanto aplicativo que eu não sei mais não
What's app, what's down, what's new
Mil pratos sugestivos num novo menu
É Facebook, é Facetime, é Google Maps
Um zigue-zague diferente, um beco, um CEP
Que não consta na lista do velho correio
De qualquer lugar
Waze é um nome feio, mas é o melhor meio
De você chegar

(Gilberto Gil, *Pela Internet 2*, 2018)

SUMÁRIO

1. Levando os direitos digitais a sério[1]

Lucas Fucci Amato[2]

> Por um lado, a mente assemelha-se a uma máquina. É modular e formulaica, com partes que desempenham funções específicas. A ligação entre a função mental e a estrutura cerebral está sujeita a modificações devido à notável plasticidade do cérebro. Neste aspecto, porém, a mente funciona por regras, mesmo quando o seu funcionamento baseado em regras inclui o poder da infinidade recursiva: a capacidade de inventar algo novo por uma recombinação interminável de elementos familiares que podem acabar por sugerir ideias e procedimentos que são simultaneamente novos e úteis. Até este ponto, tudo na nossa experiência mental está em conformidade com um modelo comum na história anterior da natureza.
> Noutros aspectos, porém, a mente é uma antimáquina. Não é modular ou estereotipada. Pode ver algo, ou perspectivar uma transformação da realidade estabelecida, ou da nossa forma estabelecida de compreender o real, que não é aceito pelos pressupostos e métodos em que nos baseamos nas nossas práticas contínuas de investigação. As suas descobertas podem ser, desse modo, sem sentido. E, depois, pode desenvolver retrospectivamente os métodos e pressupostos que dão sentido a essas descobertas, de outra forma sem sentido.
> Este segundo lado da mente é aquilo a que chamamos imaginação. Há dois movimentos que a definem. O primeiro movimento é aquele que Kant enfatizou: o distanciamento do fenômeno – uma imagem é a memória de uma percepção. Esse distanciamento representa, na nossa experiência mental, a forma mais simples e básica de transcendência: a nossa remoção da cena imediata da percepção e ação.
> Podemos compreender melhor esse distanciamento como uma preliminar ao segundo movimento da imaginação: subsumir parte do mundo manifesto a uma gama de variações transformativas no espaço do possível próximo. A percepção do real só se aprofunda à medida que a imaginação do possível adjacente se expande. À medida que o mundo manifesto perde alguma da sua rigidez bruta – seu simples estar aí - tornamo-nos capazes de olhar menos e de compreender mais.
> Nada na estrutura física do cérebro predetermina o poder relativo destes dois lados da mente – a mente como máquina e a mente como imaginação, ou seja, a mente como agente da criação perpétua do novo. A proeminência relativa destes dois lados da mente depende das disposições da sociedade e da cultura. A história da política é interna à história da mente.
> (UNGER, Roberto Mangabeira. *The world and us.* London: Verso, 2024, p. 103-104)

[1] Agradeço ao amigo Matheus Della Monica pela sugestão do título!

[2] Professor Associado do Departamento de Filosofia e Teoria Geral do Direito da Faculdade de Direito da Universidade de São Paulo – USP. Pesquisador visitante nas Universidades de Cambridge, Oxford e Harvard. Livre-docente, pós-doutor, doutor e bacharel em Direito pela USP. Vice-Presidente da Associação Brasileira de Pesquisadores em Sociologia do Direito – ABraSD.

O século XX desacreditou a concepção mecânica de interpretação jurídica como mero raciocínio lógico-dedutivo, formulaico, estereotípico, suscetível à formalização e à incorporação de fórmulas em uma máquina ou na programação algorítmica; ao fim e ao cabo, a teoria do direito retomou a importância das artes inventivas e argumentativas no discurso jurídico e destacou suas bases morais e políticas. De outro lado, as instituições (juridicamente configuradas) da sociedade industrial foram capaz de generalizar alguns padrões de liberdade e bem-estar social, atingindo por vezes a precária e virtuosa retroalimentação de democracia e desenvolvimento. Hoje, na era da "memeficação" e dos algoritmos, a concentração global de poder econômico, político e midiático pelas *big techs* serve à dissonância cognitiva e à ascensão de ideologias e movimentos autoritários. Se pode ser produtivamente instrumentalizada para aumentar a eficiência da gestão de processos decisórios, a inteligência artificial também ameaça hipersimplificar a aplicação do direito, reduzindo-a a um processamento de dados alienado do juízo humano e capaz de produzir, colateralmente, vieses e injustiças graves e massivas. Os usos e abusos potencializados pela inovação tecnológica precisam ser enfrentados pela inovação jurídica, na forma do desenho de direitos e responsabilidades, poderes e obrigações, procedimentos e organizações. Novas ordens jurídicas, novos regimes regulatórios, novas arenas decisórias, novas normas e interpretações compõem o grande processo de "destruição criativa" do direito nessa era de digitalização da sociedade, da política, da economia, da educação, da saúde, da mídia, da arte, da família e também do próprio campo jurídico.

Este livro reúne estudos de uma série de pesquisadores brasileiros (sobretudo vinculados à Universidade de São Paulo) e europeus (de universidades de ponta da Alemanha, França, Itália, Portugal e Reino Unido) sobre os temas mais atuais do direito e da sociedade digital, como inteligência artificial, privacidade de dados pessoais e *fake news*, pauta também abordada por outro volume que publiquei neste mesmo Portal de Livros Abertos da USP,

intitulado *O direito da sociedade digital: tecnologia, inovação jurídica e aprendizagem regulatória*.

Nesta introdução, alinho o percurso desta obra coletiva, vista como um mapa da pesquisa sociojurídica contemporânea em temas de Direito Digital. No texto seguinte (capítulo 2: *Inovações constitucionais na era da inteligência artificial: separação de poderes e direitos digitais*), trago provocações sobre nossa necessidade e capacidade de digitalizar as categorias clássicas de direito constitucional (relativas à organização do poder estatal e aos direitos fundamentais), inovando-as para fazer frente aos riscos (de desigualdade extrema, exclusão econômica e autoritarismo político) hoje evidentemente reforçados pela disseminação das novas tecnologias.

No terceiro capítulo (*Constitucionalismo societal no mundo digital*), Angelo Golia Jr. e Gunther Teubner atualizam a clássica proposta de Teubner sobre a expansão do conceito de "constituição" para além do Estado nacional e mesmo do sistema político. Há pelo menos duas décadas o sociológico e jurista alemão, inspirado no conceito de "constitucionalismo societal" do americano David Sciulli, propõe o diagnóstico da emergência não apenas de um pluralismo jurídico global, mas de um verdadeiro pluralismo constitucional, com fragmentos de constituições "civis" (*i.e.* não estatais); para além da autorregulação, a autoconstitucionalização de ordens privadas, a partir de regimes que criam suas próprias regras primárias e secundárias (de organização), procedimentos, instâncias decisórias e doutrinas. Da mesma forma, Teubner tem há muito proposto a expansão do conceito de "direitos fundamentais" para além de uma abordagem individualista, para fazer frente a riscos difusos e coletivos que são gerados por redes e agentes privados, não apenas pelo Estado nacional e pelo sistema político. Como internalizar esses riscos produzidos na ambiência digital? Como generalizar e reespecificar para os protagonistas do mundo digital os controles impostos classicamente ao poder soberano? São questões-chave que abrem os diagnósticos e as propostas apresentados no texto.

No quarto capítulo (*Regulação para o mercado? Reflexões sobre direito e inovação na era das tecnologias disruptivas a partir de aportes schumpeterianos*), Marco

Antonio Loschiavo Leme de Barros e Julia Tosatto discutem o desafio do desenho de regimes jurídicos voltados a mercados caracterizados pela demanda de grandes economias de escala e alta dependência de investimentos em novas tecnologias. Como incentivar a inovação e facilitar a entrada de novos competidores nesses mercados? A clássica teoria de Schumpeter sobre o desenvolvimento econômico a partir da "destruição criativa" encontra a modelagem de ferramentas regulatórias como os *sandboxes*, que procuram dosar experimentalmente a imposição de pacotes de *standards*, obrigações e responsabilidades, à medida que um agente econômico inovador cresce e amadurece.

No quinto capítulo (*Inovações regulatórias para tecnologias disruptivas: o* sandbox *de inteligência artificial*), Caio Rezende Missagia igualmente explora os ambientes regulatórios experimentais, primeiramente implementados nos mercados financeiros, mas agora voltados também à IA, como dinâmicas que institucionalizam um aprendizado jurídico relacional e interativo entre regulador e regulados. Missagia avança a tese de que uma regulação adequada não apenas deixa de criar dificuldades à inovação tecnológica, mas tem uma função promocional, na qual o Estado pode se articular como propulsor de externalidades positivas e dinâmicas virtuosas de empreendedorismo, mimetizando o protagonismo que Schumpeter atribuía ao empresário disruptivo como líder do processo de "destruição criativa". O Estado, além de não entravar os empreendedores, pode atuar diretamente na abertura de novos mercados, no desenvolvimento de novos produtos e processos produtivos (ou no financiamento à pesquisa, básica ou aplicada, que culmina em invenções), na disponibilização de infraestrutura que dá acesso a novas fontes de insumos e, sobretudo, em inovações institucionais, que incluem um repertório de formas de direito econômico, regulatório e privado disponibilizadas para a cooperação entre agentes privados e entre estes e o Estado.

A seguir, temos um bloco de pesquisas dedicadas à regulação da inteligência artificial. Carolina Stange Azevedo Moulin (capítulo 6: *Diretrizes para a regulamentação da inteligência artificial: responsabilidade jurídica na era do algoritmo*)

traz reflexões acerca da categoria de responsabilidade civil sobre atos ilícitos decorrentes de ações de algoritmos. O texto se situa no campo de estudo do "Direito da Inteligência Artificial", que busca compreender as implicações éticas, sociais, econômicas, culturais e jurídicas do desenvolvimento de algoritmos autônomos de tomada de decisão. O capítulo dialoga com as premissas propostas por Aimatai e Oren Etzioni, bem como com questões relativas às consequências econômicas e sociais da IA, como desemprego em massa, automação do trabalho, renda básica universal, redução da jornada de trabalho e a necessidade de adoção de *standards* internacionais para garantir efetividade à regulamentação da IA.

Na mesma linha, Clara Martins Pereira (capítulo 7: *A Proteção de Direitos Fundamentais no Regulamento Europeu da Inteligência Artificial*) faz um esforço de digitalização do conceito de "direitos fundamentais", apresentando seu enquadramento no Regulamento Europeu da IA aprovado neste ano de 2024. O Regulamento então é contrastado com a Carta e a Convenção Europeia dos Direitos Humanos. Como pontua a autora, enquanto a interpretação dos direitos humanos admite apenas o mínimo necessário de interferências, a lógica do *AI Act* baseia-se no cumprimento de *standards* mínimos, que sopesam as vantagens econômicas e tecnológicas com potenciais desvantagens para a segurança e os direitos; se as primeiras superarem as segundas, os danos são admissíveis, ainda que indenizáveis.

Elena Esposito (capítulo 8: *Transparência versus explicação: o papel da ambiguidade na IA jurídica*) retoma o velho problema da "interpretação mecânica" do direito (acusação que realistas como Pound faziam às concepções formalistas clássicas). Aqui, na era da aprendizagem de máquinas e dos algoritmos, quais seriam os limites da argumentação jurídica, com sua lógica do razoável, e dos textos normativos, com sua ambiguidade e vagueza? Em que medida o processo decisório do direito é modular e formulaico, como uma máquina trivial, e em que medida depende de imaginação, juízo e retórica? Será que a inteligência artificial pode mimetizar, em sua programação algorítmica, a capacidade humana de julgar, sentir e criar?

Chegamos então a textos dedicados ao tema da privacidade de dados pessoais. Rafael Zanatta (capítulo 9: *Os sentidos do direito da proteção de dados pessoais: desmembrando a complexidade do direito e dos direitos*) especifica em que sentido se pode entender a privacidade de dados como um direito fundamental – não meramente individual como a intimidade – a ser afirmado diante de processos de "datificação", com fluxos comunicativos que atingem pessoas e moldam sistemas sociais. Para tanto, Zanatta retoma criativamente a centenária e incontornável construção de Hohfeld sobre as posições jurídicas fundamentais e os direitos subjetivos (que incluem uma série complexa de posições, como reivindicações/pretensões, imunidades, privilégios e poderes).

Raphael Marques de Barros (capítulo 10: *Privacidade e proteção de dados na academia: considerações sobre a cooperação Google Workspace for Education – USP*) Analisa o problema da privacidade de dados e da autodeterminação informativa a partir da contratação, pela Universidade de São Paulo, dos serviços da Google Workspace for Education, uma série de ferramentas com potencial uso educacional e que compreendem serviços de simulação de atividades em salas de aula e envio de tarefas, além de processamento de texto, planilhas, apresentações de slides, anotações, formulários, montagem de websites, canvas colaborativo, agenda, videoconferência e armazenagem de dados. Justapondo a Lei Geral de Proteção de Dados a uma série de instrumentos negociais, autorregulações (como políticas de privacidade) e discussões doutrinárias, o capítulo discute os impactos da coleta e do uso de dados pessoais no ambiente acadêmico, incluindo a apropriação desses dados para o treinamento de ferramentas de inteligência artificial. Ao mesmo tempo que a USP transferiu a seus estudantes a prerrogativa de concordar com todos os aspectos relacionados ao tratamento de seus dados pela Google, não há nenhuma determinação acerca do valor comercial desses dados, nem há não qualquer menção a se e como os dados coletados pela plataforma poderiam servir para o treinamento de suas ferramentas de inteligência artificial.

Finalmente, temos um bloco de pesquisas sobre *fake news*. No capítulo 11 (*Sociologia política do direito e sociedade digital: as* fake news *no Brasil*), Wanda

Capeller, João Pedroso e Andreia Santos lançam um olhar da Sociologia Política do Direito sobre o problema das *fake news* no Brasil. Este enfoque busca fornecer as ferramentas epistemológicas críticas necessárias à compreensão do fenómeno das *fake news* na sociedade digital, permitindo-lhes colocar uma questão inicial: podem o direito e a justiça, através da regulação, controlar o impacto massivo das notícias falsas no campo sociopolítico? A tese central do capítulo sustenta que a inteligência artificial, por meio de suas redes rizômicas, dá origem de forma exponencial a condições para a massificação da desinformação, agora projetada em escalas glocais. A sociedade digital, baseada na aceleração tecnológica e na alienação do mundo social conduz a um processo de de-subjetivação política e à falta de consciência jurídica. O argumento toma como base cinco premissas essenciais, nomeadamente: (1) homem, *mendax ab initio* (uma história da mentira, sobretudo no âmbito político); (2) com a colonização algorítmica da política, a sociedade digital inaugura a sociedade da pós-verdade; (3) a desinformação desconstrói o mito da neutralidade algorítmica; (4) a ordem digital leva à desordem do Estado de Direito; (5) os problemas globais exigem soluções globais e locais: estudo de caso sobre Direito e Justiça diante das notícias falsas no Brasil. Neste contexto, os autores sublinham o surgimento de cinco efeitos perversos: (1) o efeito da desordem digital; (2) o efeito da fractura social; (3) o efeito da confusão cognitiva; (4) o efeito da dissidência política; e (5) o efeito da exceção no Estado de direito.

No capítulo 12 (*Do trilema regulatório à metarregulação: o caso das* fake news), Leonardo Koyama e Lucas Fucci Amato analisam o instituto da "autorregulação regulada" previsto em uma das versões do Projeto de Lei das Fake News (Projeto de Lei nº 2.630/20), ainda em discussão no Congresso Nacional (neste final do ano de 2024). Defendem que essa forma de coordenação entre Estado e plataformas digitais seria capaz de responder aos desafios de uma solução jurídica que ao mesmo tempo seja eficaz para os usuários, não imponha custos e obstáculos excessivos ao desenvolvimento tecnológico nem seja instrumentalizada pelas *big techs*, que apenas têm interesse em construir sua autorregulação na medida em que ela não perturbe seus interesses políticos e

econômicos. Substantivamente, esse modelo institucional ajudaria a construir uma forma de liberdade de expressão moderada nas redes, evitando os extremos da censura ou autocensura e da disseminação de desinformação e discursos de ódio.

Boa leitura!

2. Inovações constitucionais na era da inteligência artificial: separação de poderes e direitos fundamentais digitais

Lucas Fucci Amato[3]

Introdução

Diante da herança absolutista de centralização estatal-nacional do poder e do direito, o constitucionalismo liberal organizou-se ao redor de um esquema de contenção do poder público e garantia de uma esfera privada individual. A contenção do poder se deu pela fragmentação e especialização funcional dos órgãos de Estado (em geral com o reconhecimento da supremacia do Legislativo), pelos vetos múltiplos organizados entre eles ("freios e contrapesos"), pela repartição estanque de competências legislativas e materiais no caso dos Estados federais e por uma série de direitos civis, incluindo liberdades públicas (religiosa, artística, científica, econômica) e autonomia privada (garantia da propriedade e da liberdade contratual). Com seu acento aristocrático, o liberalismo clássico confiava sobretudo no direito penal e no direito privado como ramos judicializáveis e capazes de manter e reforçar essa barreira entre cada indivíduo, os outros e o Estado.

O século XX assistiu ao advento da política de massas, com a universalização do sufrágio, a organização e diversificação das ideologias, partidos políticos, grupos de interesse e movimentos sociais (com destaque para a inclusão e mobilização dos trabalhadores), o crescimento do Poder Executivo (seja pelo incremento da burocracia pública, seja pelo avanço da liderança presidencial ou equivalente) e a extensão dos direitos sociais. Ainda que não

[3] Professor Associado do Departamento de Filosofia e Teoria Geral do Direito da Faculdade de Direito da Universidade de São Paulo – USP. Pesquisador visitante nas Universidades de Cambridge, Oxford e Harvard. Livre-docente, pós-doutor, doutor e bacharel em Direito pela USP. Vice-Presidente da Associação Brasileira de Pesquisadores em Sociologia do Direito – ABraSD.

judicializáveis, esses direitos eram desdobrados, de um lado, na forma de direitos trabalhistas individuais e coletivos, amparados por formas corporativistas de mediação estatal do conflito entre capital e trabalho. De outro lado, direitos sociais foram promovidos, fora dos tribunais, pela administração pública, isto é, por serviços públicos de saúde, educação, cultura etc., os quais, ao proporcionarem uma forma de "salário indireto", compensavam redistributivamente a ampla desigualdade econômica provocada pela concentração de riqueza na sociedade industrial. Sobretudo no pós-guerra, onde, em vez da participação popular direta (em "sovietes" ou órgãos de autogoverno afins) e da aclamação ao líder autoritário como símbolo nacional, o Estado social combinou-se com a democracia representativa, o avanço da participação popular (ainda que mediada por elites) teve como contraparte a difusão do controle judicial de constitucionalidade, com aprofundamento de suas técnicas e de seu alcance, tanto na forma difusa quanto na forma concentrada.

A pergunta-chave é: diante da herança liberal e social dos modelos de Estado e direito dos últimos séculos, como digitalizar o constitucionalismo nessa sua dupla faceta, de organização do poder estatal e garantia de direitos aos cidadãos? Este capítulo procura atualizar algumas reflexões apresentadas no livro *Inovações Constitucionais: direitos e poderes* (AMATO, 2018), à luz dos novos desafios impostos pela disseminação das tecnologias digitais. Seu ponto de partida é o modelo de direitos – de desestabilização, imunidade, participação e autonomia (DIPA)[4] – ali proposto e correlacionado a mudanças na separação dos Poderes. Para introduzir a discussão, vejamos o exemplo da problemática (atualmente discutida no Congresso Nacional do Brasil) sobre a regulação da inteligência artificial – e como ela repercute nos temas clássicos do constitucionalismo: garantia de direitos e organização de poderes.

[4] As categorias de direitos de imunidade e de desestabilização vêm de Unger (2001 [1987]).

Freios e contrapesos no ambiente digital[5]

Já em 1968, dez anos antes de ganhar o prêmio Nobel de economia, Herbert Simon (2019 [1968], p. 6) diagnosticava que vivíamos em um mundo mais artificial que natural; e conceituava o "artificial" ou um "artefato" como uma "interface" entre um ambiente interno (sua substância e organização) e um ambiente externo, o meio em que ele opera.

Dada a potência do acoplamento – entre seres humanos e máquinas e entre o mundo físico e o virtual – viabilizado pelas tecnologias genericamente rotuladas de "inteligência artificial", seus perigos e riscos, custos e benefícios tomam a ordem do dia. Quando se pensa no regramento das tecnologias digitais – particularmente, da inteligência artificial (IA) – as respostas à pergunta "por que regular?" definem o espectro de alternativas institucionais sobre "como regular".

A regulação da IA pode ter diversos objetivos – e, por isso, seria interessante que a proposta de um Marco Regulatório da IA se desdobrasse em especificações legislativas, regulamentares e jurisprudenciais setoriais. Por exemplo, no campo eleitoral, podemos pensar que o objetivo é garantir um voto livre e informado, não distorcido por falsas informações e induções da percepção da realidade. É o ponto básico focado pela proibição das *deepfakes* e pela exigência de sinalização do conteúdo gerado por IA nas campanhas eleitorais, como dispôs a Resolução nº 23.732/2024, do Tribunal Superior Eleitoral.

Há, porém, um ceticismo sobre a necessidade de regulação. Para desafiá-lo, precisamos apontar os riscos da falta de regulação, os quais são associáveis a três atores. Esses riscos são magnificados e retroalimentados quando não são de algum modo geridos e filtrados.

Primeiramente, temos as comunidades constituídas nas redes sociais e serviços de mensageria privada – os usuários, produtores e consumidores de conteúdo. Com a acessibilidade das ferramentas de IA generativa, exponencia-se a capacidade de geração de textos, áudios e vídeos que interferem na produção e

[5] Este tópico reproduz, com modificações e acréscimos, análise publicada no portal Jota, 15/05/2024.

percepção da realidade por meio de uma comunicação que circula de modo policêntrico e anárquico. Nas comunidades baseadas nas redes e plataformas, disseminam-se condutas de autocensura, "linchamentos" de opinião e "cancelamentos", em um verdadeiro "estado de natureza" virtual, que pode facilmente extravasar para o campo da violência física e das consequências concretas. Como resultando, tem-se um ambiente poluído, que distorce e conflagra, por exemplo, a arena eleitoral, maculando a liberdade de expressão e de informação.

Em segundo lugar, temos as empresas provedoras de tecnologia para a produção e circulação de informação em meio digital. Ao contrário dos meios tradicionais de comunicação de massa, como jornal, rádio e televisão, não se trata de editorialização e produção profissionais e centralizadas de conteúdo, a ser consumido massivamente. A produção e a disseminação desintermediadas dos meios analógicos é reintermediada pelas plataformas digitais. De um lado, há um problema concorrencial: em geral, trata-se de *big techs*, que atuam em todos os elos da cadeia produtiva da comunicação: a IA generativa facilita a produção de informação, as plataformas as empacotam em mensagens e usos específicos e a IA preditiva facilita o direcionamento da compreensão pelos diferentes perfis de público. Trata-se de um negócio lucrativo, que monetiza os dados e passos dos usuários das redes – o que estimula a inovação tecnológica, mas também dá margem aos abusos de um poder econômico concentrado. De outro lado, temos o problema da insuficiência da autorregulação. É verdade que as grandes plataformas digitais globais têm criado suas próprias regras, metodologias, procedimentos e instâncias de controle, revisão e moderação de conteúdo. Entretanto, a autorregulação pode ser tanto simbólica e ineficaz (valendo só como um escudo contra a regulação estatal) quanto autoritária e opaca aos cidadãos e autoridades públicas.

Em terceiro lugar, temos os riscos associados ao Estado: o medo de uma censura centralizada em determinada estrutura de comando e controle que supervisionaria cada conteúdo gerado e compartilhado nas redes pelas empresas e cidadãos. Na falta de uma regulação adequada, as respostas das autoridades

podem beirar o arbítrio. Por exemplo, o Judiciário, quando provocado, é obrigado a responder. Na falta de uma programação prévia das regras substantivas e procedimentais para lidar com determinado tema, acaba decidindo com base no casuísmo e na conjuntura política, com dificuldades para consolidar padrões argumentativos e com tendência a extrapolar em decisões não isonômicas, nem previsíveis nem consensuais ou colegiadas.

Esses riscos da ausência de regulação se combinam com os riscos das próprias tecnologias reguladas, focalizados e graduados pelas legislações na matéria. Por exemplo, o Regulamento de Inteligência Artificial da União Europeia (2024/1689) tem uma abordagem baseada em riscos (de danos físicos, psicológicos, sociais ou econômicos, a direitos fundamentais e a interesses públicos, como como a privacidade de dados pessoais, saúde e segurança). A gradação abrange sistemas de risco mínimo ou nulo (deixados basicamente à autorregulação pelo mercado e pelos provedores), de risco limitado (aos quais se impõem obrigações de transparência e confiança, como no caso de *deepfakes*) e de risco elevado (como identificação biométrica ou robôs para transporte, ensino ou tratamento médico, sistemas aos quais se impõem exigências estritas para autorização e monitoramento).

A resposta à pergunta sobre "como regular" tem que considerar as vias possíveis para minorar esses riscos da falta de regulação e mais três fatores importantes: o conhecimento (especializado manejado pelos próprios entes a serem regulados, as plataformas que desenvolvem e detêm a propriedade intelectual de suas tecnologias), o espaço (a transnacionalidade das plataformas, contraposta à nacionalidade do direito estatal) e o tempo (a necessidade de desenvolver uma articulação que permita renovar as regras acompanhando a velocidade da mudança tecnológica). É em meio a esses desafios que se precisa encontrar uma intersecção entre os interesses materiais (o progresso tecnológico pode barretear e democratizar produtos, inclusive campanhas eleitorais) e os interesses morais (de garantia e aperfeiçoamento das liberdades, da democracia, da concorrência por mérito).

Nessa linha, o que um marco legislativo pode ofertar é: 1) substancialmente, uma metodologia para graduar e focar os riscos associados aos usos e consequências da tecnologia em cada setor específico (eleitoral, comercial etc.); 2) procedimentalmente, um esquema de coordenação que permita associar diferentes atores (os diferentes Poderes do Estado, as plataformas digitais e o povo, particularmente representado pela sociedade civil, incluindo pesquisadores, associações e movimentos em torno dos direitos digitais). Nessa linha, caminha bem a proposta de revisão do Projeto de Lei do Senado 2338/2023 apresentada pela Comissão Temporária sobre Inteligência Artificial. Ela prevê um Sistema Nacional de Regulação e Governança de Inteligência Artificial composto por uma autoridade executiva de coordenação, que funcionaria como um nó articulador (*broker*) de uma rede composta por agências reguladoras setoriais, agências reguladoras de IA, CADE, pela autorregulação das plataformas e por entidades de certificação. É um ensaio que recupera a proposta de "autorregulação regulada" prevista a certa altura no PL das *Fake News* (ainda de futuro incerto no Congresso), mas retirada de sua última versão discutida (ver o capítulo de Leonardo Koyama e Lucas Amato, neste livro). Aliás, dinâmicas de algum modo similares de abordagem da autorregulação encontram-se rotinizadas em diversas experiências no Brasil mesmo[6].

Esse arranjo institucional pode ser lido com um verdadeiro esquema de freios e contrapesos para o ambiente digital. Tem em vista dois problemas. O primeiro é contrapor os interesses parciais dos diferentes atores (Estado, plataformas e usuários) e prevenir o abuso de seus poderes por meio de uma contenção a partir de vetos que cada um pode impor ao outro no desenho da regulação a ser desenvolvida e aprofundada a partir desse regime legal. O objetivo é buscar uma divisão de direitos, deveres, poderes e responsabilidades

[6] É o caso do SISMETRO (Sistema Nacional de Metrologia, Normalização e Qualidade Industrial), instituído pela Lei 5966/1973 e que reconhece a competência normativa da Associação Brasileira de Normas Técnicas (ABNT), uma entidade privada; do Conselho Nacional Autorregulamentação Publicitária (CONAR), organização da sociedade civil fundada em 1980; do Comitê Gestor da Internet (CGI.br) instituído pelo Marco Civil da Internet (Lei 12965/2014), que delega poderes à associação privada Núcleo de Informação e Coordenação do Ponto BR (NIC.br); e da Autoridade Nacional de Proteção de Dados (ANPD), instituída pela Lei Geral de Proteção de Dados Pessoais (LGPD, Lei 13709/2018).

que responda a uma intersecção identificável com o "interesse público". O segundo problema é lidar com a falibilidade dos diferentes atores e da sua produção regulatória. Para tanto, a coordenação deve facilitar a corrigibilidade, catalisando respostas jurídicas experimentais, testáveis com base em evidências e revisáveis. Uma autoridade coordenadora dessa rede de agentes pode atuar mediando as soluções e saídas para impasses na negociação entre os diferentes atores para a criação ou revisão das regras.

Não precisamos de um código digital com milhares de regras específicas, pensado para durar décadas; nem é suficiente uma lista de princípios, que apenas transferem poderes discricionários às autoridades que os devem aplicar, concretizando-lhes o sentido. O principal é termos um esquema de coordenação que articule os conhecimentos, interesses e legitimidades (parciais, mas relevantes) dos diversos jogadores das arenas digitais, com suas especificidades setoriais (partidos, candidatos, eleitores e Justiça Eleitoral, por exemplo, no campo das aplicações eleitorais da IA). Assim como a inovação econômica e tecnológica se expressa por meio de novos produtos e processos produtivos, a inovação jurídica não implica apenas novas regras, mas também, mais amplamente, criatividade nos regimes jurídicos e arranjos institucionais. Tal inovação institucional depende de uma compreensão dos limites do direito estatal para, em concorrência com outras ordens normativas do campo digital, incentivar/desincentivar, proibir, obrigar ou permitir condutas e estruturar órgãos e procedimentos.

Na dinâmica econômica de "destruição criativa" (SCHUMPETER, 1949 [1934]), uma fase de competição por preços em produtos padronizados é rompida pelo surgimento de inovações, a partir das quais o empreendedor domina o mercado e ganha lucros de monopólio, até que o conhecimento incorporado se dissemine entre os competidores e se restabeleça a fase concorrencial. Assim como as revoluções científicas estabelecem novos "paradigmas", que rompem com as metodologias e teorias estabelecidas e rotineiramente manejadas pela "ciência normal" (KUHN, 2007 [1969]), as inovações tecnológicas "disruptivas" ou "radicais" (por oposição às melhorias

"incrementais") não apenas introduzem redução de custos ou aumentos de qualidade marginais, mas sim produtos, processos e modelos de negócio que alteram todo o mercado, em termos das expectativas tanto dos consumidores quanto dos concorrentes, estabelecendo novos nichos, desalojando posições de poder econômico estabelecidas e mesmo destruindo antigos produtos, processos e profissões (CHRISTENSEN, 1997).

Da invenção à consolidação e à obsolescência, o ciclo de vida dos produtos e dos negócios caminha lado a lado à vida do direito e de suas regras. A disrupção tecnológica gera um conflito sobre os recursos jurídicos disponíveis (BIBER *et al.*, 2017). Em uma primeira situação, as formas do direito posto podem não alcançar os novos modelos de negócio desenvolvidos, por uma "lacuna regulatória" que passa a existir quando constatada ou pela exploração de ambiguidades e brechas na legislação existente, que deixa, portanto, de impor custos legais a certos atores econômicos e lhes permite obstaculizar a atuação dos demais, impondo-lhes externalidades negativas ou vetando-lhes o acesso a externalidades positivas. Ou o direito posto pode apenas tangenciar algumas das repercussões (discriminação, abuso concorrencial etc.) do novo negócio. Finalmente, as tecnologias e modelos de negócios podem desenvolver formas de autorregulação alternativas, que competem com o direito estatal e lhe impõem opacidades e bloqueios, e/ou superam as barreiras à entrada e os custos impostos pela regulação estatal (daí que uma saída seja o desenvolvimento de "ambientes regulatórios experimentais", *sandboxes*, que elevam gradualmente as obrigações impostas aos entes regulados *pari passu* à sua maturação mercadológica – ver AMATO; MISSAGIA, 2023).

A estrutura escalonada da ordem jurídica estatal se vê confrontada por outras hierarquias normativas, do local ao global: "[e]m vez da hierarquia contínua e linear que a imagem da pirâmide expressava, aparecem hierarquias descontínuas, como outras tantas pirâmides inacabadas, e hierarquias enredadas que formam 'anéis estranhos'", diz Delmas-Marty (2004 [1994], p. 87-88), visualizando entre ordens jurídicas diversas relações de "hierarquias descontínuas e pirâmides inacabadas".

E mais: nas redes digitais interconectadas em teias cada vez mais complexas, desenvolve-se uma dinâmica policêntrica, em que programadores, engenheiros, empresários de tecnologia, usuários, legisladores, juízes e tantos outros atores usam e corregulam o meio digital simultaneamente, atuando como nós de uma rede multitudinária em expansão exponencial. A codificação digital da informação permite assim a criação de uma ambiência análoga à dinâmica criada pelo dinheiro em uma economia de mercado. O dinheiro permite uma difusão e expansão dos meios econômicos sem um mecanismo central de distribuição dos recursos. Uma multidão de empresas e de consumidores – ou de produtores e compradores – usa o dinheiro para distribuir descentralizadamente os bens, independentemente dos desejos subjetivos e das necessidades objetivas. Essa indiferença – aos desejos e necessidades, mas também às estratificações sociais inatas – é institucionalizada pelo mercado, que promove o ajuste entre a oferta e a demanda a partir dos vários centros de iniciativa e decisão econômica. Michael Polanyi (1951 [1946]) adjetivou essa dinâmica de "policêntrica". O mesmo ocorre hoje no meio digital.

Como aponta Godoy (2024), a regulação dos equipamentos (*hardwares*) e sistemas operacionais (*softwares*) obedece a uma arquitetura que empilha diversas camadas de "protocolos de interconexão" entre dispositivos nos circuitos e redes em que a informação codificada transita (modelo de referência OSI, *Open Systems Interconnection*). Nas duas extremidades dessa pilha de camadas, o ser humano e o direito positivo conseguem atuar mais facilmente: trata-se, de um lado, da camada física pela qual se disseminam os *bits* que compõem a informação (das fibras óticas ao *wi-fi*) e, de outro, da camada de aplicação, interface de interação com o usuário dos dispositivos eletrônicos, em suas telas e aplicativos. Entre essas camadas de protocolos, porém, há uma programação algorítmica apenas parcialmente controlada pela intencionalidade humana, pois retroalimentada em uma teia de redes de conexão ininterrupta entre dispositivos e interações conscientes e inconscientes, diretas e indiretas, entre bilhões de nós comunicativos. Aí se encontram camadas de enlace de dados (da rede física aos dispositivos receptores), de endereçamendo dos pacotes de

informação nas redes e controle do tráfego, de transporte, detecção e correção de erros nos *softwares*, de comunicação entre diferentes máquinas e de conversão e formatação das informações. Essas camadas permitem uma fuga a critérios territoriais (pode-se camuflar a localização dos dispositivos) e controles temporais (a produção e a disseminação da informação tendem à instantaneidade). Programações algorítmicas direcionam comportamentos e levam à remoção automatizada de conteúdos, em uma normativização tecnológica que compete com as ordens jurídicas nacionais, inter, supra e transnacionais. O Estado pode delegar poderes legislativos, jurisdicionais e sancionatórios às plataformas, mas estas não apenas desenvolvem normatizações internas (*e.g.* políticas de uso) como também delegam poder normativo a aparatos automatizados (*scripts*, sistemas operacionais, algoritmos). Em sua forma condicional (se-então), os códigos-fonte e as instruções lógicas e matematizadas para a solução de problemas aprendem com suas próprias operações. De um lado, são autoexecutáveis e reduzem a margem de incerteza e indefinição; de outro, podem retroalimentar vieses. O certo é que essa normatização algorítmica compete com normas jurídicas emanadas de diversas ordens jurídicas (dos códigos de conduta e políticas de uso das próprias plataformas até a legislação e a jurisprudência estatais). Por sua vez, as normas jurídicas nem sempre têm a forma condicional e comumente dão ampla margem ampla à ponderação caso a caso e à indeterminação; mesmo regras podem conter cláusulas abertas e ser estendidas ou excepcionadas por alusão a princípios, políticas, propósitos. Assim, a indeterminação das próprias normas substantivas transforma-se em delegação de poder entre as autoridades daquela ordem jurídica (LUHMANN, 2004 [1993], p. 196-203). E mais: para operar sobre a normatização e programação algorítmica, atingindo de alguma forma as diferentes camadas de protocolos de interconexão no ciberespaço, as formas institucionais da juridicidade (advogados, promotores, juízes, burocratas, acordos, leis, despachos) dependem da cooperação de outros agentes (operadoras, redes, plataformas, programadores, desenvolvedores).

Direitos de imunidade e de desestabilização: o escudo e a espada

Na história do constitucionalismo ocidental, a construção de uma esfera de imunização do cidadão diante do poder estatal se deu na forma de direitos e garantias individuais e, depois, com o complemento de um pacote de direitos sociais que contemplaram também formas coletivas de titularidade e ação, proporcionando um mínimo de inclusão (econômica, mas também educacional, cultural etc.) e um amortecimento diante das oscilações dos ciclos políticos e econômicos, com suas fases de crise, capazes de gerar, por exemplo, ameaças de violência e escassez (perseguição política, desemprego). Como pensar hoje o equivalente funcional a essa função de imunização do cidadão?

Uma pauta evidente, por exemplo, é a consideração da privacidade de dados pessoais como um direito civil, individual, diante do qual a antiga proteção constitucional do sigilo de dados precisa ser atualizada e digitalizada (ver MORTOZA, 2024). Na esfera do direito privado, isso equivale a compreender as relações digitais como contratos relacionais, com obrigações de consentimento informado, mas também com deveres e obrigações de solidariedade implícitos, definíveis tacitamente apenas de maneira retrospectiva, quando surgido um conflito entre usuário e plataforma, cujo vínculo se pretende baseado na confiança e na boa-fé.

Entretanto, assim como os danos e os direitos ambientais pode ser vistos como difusos – afetam e são titularizáveis por coletividades indeterminadas de pessoas –, também podem ser assim abordados os direitos digitais (ZANATTA, 2022). Shahar (2019), por exemplo, propõe não resumir o tratamento dos dados digitais a um problema jurídico de privacidade, mas os regular como um problema de "poluição de dados". A regulação dos dados pessoais na esfera digital não envolve apenas uma relação privada, com assimetrias de informação a demandarem um consentimento informado por parte do usuário e garantias para sua privacidade. A proliferação da coleta e do registro de dados na navegação digital tem gerado danos colaterais (custo social, externalidades negativas), como o próprio direcionamento da navegação e a formação de bolhas de comunicação que exponenciam o potencial de desinformação e a criação de

grupos radicais enclausurados em suas "evidências" idiossincráticas ou "*fake news*". Daí que se chegue a propor não apenas a vedação de vantagens dadas aos usuários pelo fornecimento de seus dados (por exemplo, cadastros virtuais que autorizam descontos no comércio eletrônico) como também a tributação dos "poluidores de dados".

Se, em sua função de imunidade, os direitos fundamentais são um escudo do cidadão contra as instabilidades sociais e os abusos de poder público e privado, tais direitos também precisam contar com meios de defesa incisivos para cobrar a reordenação desses mesmos poderes e seu realinhamento com os preceitos constitucionais – ou seja, precisam contar com uma espada que permita sua defesa em situações de negação reiterada das promessas do Estado democrático de direito.

Direitos de desestabilização seriam prerrogativas voltadas a acionar algum processo, órgão ou agência "reconstrutora" do Estado para realizar intervenções localizadas mas estruturais contra práticas rotineiras, públicas ou privadas, que renitente e coletivamente violam direitos fundamentais, como a isonomia (UNGER, 2001 [1987]; ver também ZANATTA, 2019). Equivalem às injunções ou ações estruturais, mas não necessariamente dependeriam de um encaminhamento estritamente judicial – podendo comportar uma atuação em rede de cooperação (AMATO, 2024a) de órgãos como Conselho Nacional de Justiça, Ministério Público, Defensoria Pública, secretarias, ministérios e agências (como a Autoridade Nacional de Proteção de Dados). Portanto, complementar à abordagem dos direitos digitais como direitos de imunidade individuais e coletivos é sua mobilização como direitos de desestabilização, quando configurados os traços de sua (i) indeterminabilidade, (ii) titularidade tendencialmente difusa e (iii) gozo por pessoas desorganizadas e em posição de subcidadania. Particularmente as formas "inovadoras" de assistência jurídica e advocacia de interesse público vinculadas a movimentos de direitos digitais podem buscar formas judiciais e extrajudiciais de amparo de direitos digitais como direitos difusos ou coletivos de desestabilização contra os abusos de poder

de plataformas digitais, ou das autoridades reguladoras (ZANATTA, 2024)[7]. As ações coletivas (*class actions*), rotinizadas hoje na Europa e nos Estados Unidos (ver WÖRLE; GSTREIN, 2024), são apenas uma dessas vias de mobilização dos direitos digitais como ferramentas de desestabilização, por exemplo para forçar as plataformas a respeitar os *standards* de proteção dos dados de seus usuários (ou para forçar as autoridades regulatórias a impor tais padrões normativos).

Direitos de participação: entre o perigo à democracia e o potencial democratizante

Passou o tempo das grandes esperanças de que a internet quebraria o monopólio da classe política e conduziria a democracia representativa a uma maior abertura a mecanismos de participação direta ou a procedimentos semidiretos – como plebiscitos e referendos –, os quais rotineiramente poderiam mobilizar os cidadãos pelos cliques de seus celulares para registrarem suas opiniões sobre quase todos os problemas sociais e as políticas públicas. A distopia da disseminação massiva de notícias falsas, ainda uma novidade diante da qual o direito brasileiro e outras ordens jurídicas patinam (ver SABA *et al.*, 2021), colocou em questão mesmo o patamar mínimo da democracia representativa cristalizado ao longo do século XX: a higidez de eleições periódicas, com debates públicos que promovam o mínimo de informação, conscientização e mobilização dos cidadãos para escolherem quem escolherá as políticas públicas e operará as instituições de Estado. O debate público pelos meios de comunicação de massa perde impacto diante do conteúdo autoproduzido por candidatos e suas redes digitais oficiais ou oficiosas, sem maiores controles de ética jornalística. A descrença geral na mídia e na política convive com uma crença em narrativas conspiratórias e soluções mágicas e instantâneas promovidas por pretensos

[7] Agradeço a Rafael Zanatta pelo esclarecimento desse ponto sobre a atuação das associações e movimentos de direitos digitais. Campilongo (2011 [1991]) esquematiza o contraste entre serviços jurídicos tradicionais e inovadores, apontando como os primeiros tendem a uma abordagem individualista e paternalista da tutela de direitos, enquanto que os últimos promovem formas mais coletivizadas de conflito, mobilizam equipes e saberes interdisciplinares e utilizam estratégias políticas e jurídicas, judiciais e extrajudiciais, de cooperação e composição. Sobre as formas de mobilização do direito pelos movimentos sociais, ver também Campilongo (2012).

outsiders do sistema político, que monetizam suas campanhas e mandatos. O próprio mandato representativo aproxima-se do imperativo, quando conveniente, por parlamentares que promovem um *reality show* do exercício de seu cargo e de suas votações. É ainda incerto o quanto as instituições e os procedimentos eleitorais – tão importantes quanto os três Poderes classicamente focalizados pelo constitucionalismo – conseguirão se aperfeiçoar a ponto de fazer os benefícios das tecnologias digitais para a democracia superarem seus custos, revertendo a tendência atual em que tais tecnologias turbinaram o autoritarismo e a dissonância cognitiva.

Permanece, entretanto, pouco explorado o potencial de instrumentalização democrática dos meios digitais. Para aumentar a liberdade individual e coletiva de revisar as próprias estruturas sob as quais vivemos, reduzindo a distância entre as práticas políticas sob a moldura constitucional e legal dada e a própria revisão democrática desse quadro institucional, Lara (2024) imagina "arenas de experimentação democrática". No limite, seria um novo Poder do Estado arquitetado na forma de uma rede que institucionaliza a participação, ajudando a enraizar a auto-organização da "sociedade civil" e a diminuir a distância entre minorias organizadas e maioria desorganizada, hiato este que marca o caráter elitista da democracia de massas contemporânea (MOSCA, 1939 [1896], cap. 2). O interessante nessa modelagem é a combinação de elementos de deliberação ativa e negociação (uma espécie de democracia direta, conciliar ou "soviética") com meios digitais e remotos de votação "plebiscitária" e majoritária, simplesmente agregando votos, o que ajudaria a "vascularizar" a organização e institucionalização em sociedades desiguais, enfraquecendo tanto o poder dos grupos organizados (*lobbies*) quanto as exigências para a participação política mais ativa. Quer dizer: os cidadãos em geral têm tempo, energia e conhecimento restritos para a dedicação aos assuntos políticos, mas ferramentas como a inteligência artificial generativa podem organizar dados e subsídios para a formulação das opiniões e também facilitar a expressão de sua voz e voto, sem os tornar reféns de um pequeno grupo mais ativo de cidadãos dedicados à deliberação e à participação direta na proposição

de reformas (com prioridade de agenda legislativa ou na deliberação de agências executivas), na implementação de políticas-piloto e na gestão de assuntos de interesse público (tarefas que tampouco prescindem do apoio de quadro técnico e de bases de dados digitais para monitoramento e transparência das ações e resultados). Isso não exclui a possibilidade de incentivos à participação, como benefícios fiscais, prêmios ou mesmo acesso condicionado a certos serviços. Uma parcela dos participantes diretos poderia ser voluntária e outra poderia ser selecionada por sorteio, entre toda a população ou cobrindo grupos específicos e representativos para a deliberação de certas pautas. As arenas poderiam ser organizadas em círculos concêntricos, desde um núcleo mais ativo na deliberação e gestão até uma periferia simplesmente incentivada a disparar consultas sobre problemas, opinar substantivamente sobre soluções e votar entre alternativas pré-elaboradas, como em um plebiscito.

Por outro lado, evitando recair em um mero participacionismo simbólico, sobre temas marginais ou com relação a uma parcela ínfima do orçamento público, essas arenas teriam diferentes canais e intensidades de ligação com o centro decisório do governo (isto é, com o Legislativo e o Executivo), partindo de uma mera "audiência" a demandas, passando por uma posição consultiva e tendo até mesmo alguns poderes diretos de tomada de decisão (incluindo não apenas a definição de políticas públicas, mas também sua implementação experimental, com recursos e autonomia para tanto). Essa configuração complementaria a disputa entre governo e oposição, sem estar diretamente alinhada às linhas e coalizões partidárias; por outro lado, uma supervisão judicial minimalista serviria para garantir que a vontade da maioria não tripudiasse sobre direitos fundamentais, erodindo as imunidades pessoais e coletivas que trazem segurança para a própria tomada de riscos de se propor e testar inovações institucionais.

As "arenas de experimentação democrática" poderiam ter uma moldura nacional de organização (regras de inclusão, organização, quadro técnico, orçamento, procedimento), com margens para variações federativas, locais e estaduais. Embora a proposta parte do modelo da representação local, baseada

em critérios territoriais ou geográficos, pode-se pensar em outros critérios de associação de interesses. A rede de arenas de experimentação democrática também contemplaria mecanismos de monitoramento e compartilhamento dos resultados alcançados por cada um de seus nós, difundindo as melhores práticas e as implementando com escopos e escalas mais abrangentes na forma de reformas experimentais (*by-passes* institucionais) – isto é, caminhos alternativos aos já existentes para a prestação de serviços públicos ou a organização de atividades econômicas, por exemplo.

A rede de arenas participativas, partindo de uma estrutura territorial descentralizada (local), poderia ser encimada (municipal, estadual e nacionalmente) por uma assembleia representativa e um conselho de governo, com ligação mais direta junto ao centro legislativo e executivo de governo (UNGER, 2001 [1987], p. 459-61; AMATO, 2018, p. 308). Desse modo, a participação (com sua força centrífuga de adicionar novas demandas, variáveis e alternativas de problemas e soluções) não se dispersaria, mas se coordenaria com as vantagens da representação política (como a disponibilidade para negociação e redução de complexidade na tomada de decisão).

Cabe enfatizar, mais uma vez, o papel constitutivo das tecnologias de inteligência artificial na organização das "arenas de deliberação democrática". Como destaca Lara (2024, p. 199-200), as demandas vocalizadas, as variáveis levantadas em discussão, as alternativas pautadas, os votos computados, os resultados mensurados e graduados de cada medida proposta, seu itinerário de implementação e seus resultados, tudo isso se valeria das capacidades analíticas, dialógicas e sintéticas das ferramentas de inteligência artificial, com a gestão de grandes aglomerados de dados, de forma que recursos humanos seriam dedicados à garantia da integridade algorítmica dos sistemas e de sua operabilidade; as reformas institucionais e políticas públicas desenvolvidas a partir daquelas arenas podem também ser integradas ao quadro institucional/linguístico do direito, por referências à Constituição federal, aos regulamentos setoriais, à jurisprudência dos tribunais superiores etc., de modo que se jogaria luz sobre a própria efetividade das provisões constitucionais,

institucionalizando nas expectativas dos cidadãos em geral a ligação entre os quadros normativos, os problemas concretos e cotidianos e os resultados práticos das medidas correlatas; reduzindo complexidade e ruídos informacionais; realinhando expectativas; produzindo maior discernimento individual e coletivo sobre prioridades de agenda e estratégias alternativas de endereçamento dos problemas.

Direitos de autonomia: reconhecimento e limitação constitucional da autorregulação

Não existe uma única ordem jurídica identificável como uma *lex digitalis* global, mas sim uma série de ordens jurídicas semiautônomas, as mais desenvolvidas contando não apenas com normas autorreguladas, mas também com comitês equivalentes a órgãos jurisdicionais de solução de conflitos (NEGÓCIO, 2023).

Como abordado no capítulo de Golia Jr. e Teubner, neste volume, e aqui ilustrado pela discussão sobre a regulação (da autorregulação) da inteligência artificial, o constitucionalismo digital precisa se desprovincianizar da circunscrição territorial do Estado nacional. Ao mesmo tempo, porém, as constituições nacionais precisam dar abertura e impor limites (substantivos e procedimentais) a ordens jurídicas não-estatais, particularmente à autorregulação transnacional, como aquela criada por plataformas digitais. Diante do pluralismo jurídico global, o Estado pode ofertar uma "metarregulação" (AMATO, 2021; 2024b), regulando a autorregulação, garantindo um piso de direitos a seus cidadãos (impondo o respeito a esse piso como condição para a operação da plataforma digital no território nacional) e produzindo um "interdireito" para gerenciar a colisão entre diferentes ordens jurídicas. O pluralismo jurídico não pode mais ser produtivamente retrotraído a um monismo estatalista; tal pluralismo tem potencial positivo para favorecer o experimentalismo de formas jurídicas, referências cruzadas e mesmo controles mútuos, prevenindo o abuso de ordens (estatais ou privadas) pela própria multiplicidade de ordens jurídicas que se observam como que em um "panótico

acêntrico". Porém o direito estatal, ao "re-enviar" problemas para outras ordens ou "recepcioná-las", pode lhes impor parâmetros procedimentais (generalidade, clareza, prospectividade e isonomia em suas prescrições, além de mecanismos de monitoramento e correção, diligência devida, auditoria independente etc.). É nessa linha que o constitucionalismo estatal pode não simplesmente confiar no "constitucionalismo societal" (SCIULLI, 1992; 2001) espontâneo da "sociedade civil global" (criticamente, ver AMATO, 2015), mas deve forçar a negociação e composição entre os múltiplos interesses e poderes parciais envolvidos (agentes empresariais, estatais, tecnológicos, acadêmicos), buscando alguma interseção que represente o "interesse público"; de outro lado, a constitucionalização da autonomia – como direito à autorregulação, submetida porém à regulação estatal – incrementa a corrigibilidade das diferentes ordens jurídicas, ao reconhecer a falibilidade dos diversos agentes. A imagem simples de proteção da sociedade contra o Estado (paradigma liberal), ou de prestações positivas do Estado para a sociedade (paradigma social), cede espaço para a figura de um móbile de Calder, onde o Estado não deixa, porém, de ter seu ponto de observação e regulação em relação a outras ordens, inclusive autorreguladas.

Conclusão: para além do constitucionalismo digital

Se o constitucionalismo digital é uma das manifestações da pressão que as novas tecnologias digitais e suas repercussões sociais provocam sobre o direito público, é certo que também o direito privado carece de inovações. Não é possível conceber que toda a desigualdade exponenciada na sociedade digital – polarizada entre um pequeno clube de *big techs* e mercados financeiros globalizados e uma massa de cidadãos subempregados ou submetidos ao desemprego estrutural – vá se resolver pela judicialização de direitos individuais ou mesmo pela focalização de benefícios sociais compensatórios, como transferências de renda para o combate à miséria. Novos direitos sociais (como formas de renda básica e herança social) são demandados como mecanismos de inclusão no mercado e garantias mínimas contra os riscos e instabilidades de uma

economia que não mais garante posições estáveis de emprego, como a velha indústria fordista.

Além das formas de trabalho demandarem proteções portáveis ao longo dos diversos setores e carreiras pelas quais o cidadão poderá transitar ao longo de sua vida economicamente ativa, o próprio capital na sociedade digital pode e precisa contar com ferramentas de descentralização e democratização. Por exemplo, formas de "propriedade desagregada" (AMATO, 2022) que combinem pretensões fragmentárias e parciais, temporárias ou condicionais, de diversos agentes econômicos (investidores, empreendedores, bancos públicos, trabalhadores cooperativados) sobre um mesmo conjunto de recursos produtivos. Essas arquiteturas jurídicas podem cobrir direitos reais e propriedade intelectual, mas também formas de sociedades de participação (*holdings*) e fundos de fundos, para uma combinação de recursos públicos e privados voltados ao investimento de empresas nascentes, *startups*.

No limite, até mesmo os usuários poderiam ser incluídos nas rendas das plataformas que eles consomem, mas também coproduzem. Sob uma dinâmica de desagregação proprietária, a monetização de dados pessoais pelas empresas de tecnologia (geralmente com poder de mercado global), sem contrapartida ao usuário das plataformas digitais, haveria de ser substituída por um regime de propriedade, pelo usuário, dos dados que ele produziu; as empresas poderiam então pagar compensações e rendas pelo uso dos dados, ou até mesmo ceder participações acionárias fracionadas, as quais poderiam ser agrupadas, monetizadas e negociadas em um mercado secundário; conforme o grau de contribuição dos produtores de dados (os usuários das plataformas) ao negócio dos usuários destes dados (as plataformas que os decodificam, agrupam e gerenciam), os consumidores-produtores poderiam ter maior ou menor participação econômica nos empreendimentos derivados dessa colaboração, cogita Unger (2018, p. 127-128).

A sociedade digital será capaz de generalizar e aprofundar a democracia e o desenvolvimento – como, no auge da sociedade industrial nas décadas após a segunda guerra mundial, o Estado de bem-estar social conseguiu fazer em

alguma medida, em algumas regiões do mundo – ou a inteligência artificial se unirá às forças ambientais para nos fazer retornar ao estado de natureza, com uma vida "solitária, miserável, sórdida, brutal e curta" (HOBBES, 2003 [1651], cap. 13, p. 109)?

Referências

AMATO, Lucas Fucci. Direitos humanos e sistema econômico: estrutura e semântica de um fragmento constitucional global. **Revista Brasileira de Sociologia do Direito**, v. 2, n. 2, p. 150-161, 2015. Disponível em: https://revista.abrasd.com.br/index.php/rbsd/article/view/21 . Acesso em 22 set. 2024.

AMATO, Lucas Fucci. **Inovações Constitucionais:** direitos e poderes. Belo Horizonte: Casa do Direito, 2018.

AMATO, Lucas Fucci. Fake News: regulação ou metarregulação? **Revista de Informação Legislativa**, v. 58, n. 230, p. 29-53, 2021.

AMATO, Lucas Fucci. **Propriedade Desagregada e Empreendedorismo Democrático:** instituições da economia de mercado e formas jurídicas do capital. Porto Alegre: Fi, 2022. Disponível em: https://www.editorafi.org/436propriedade . Acesso em 22 set. 2024.

AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Ambientes regulatórios experimentais: O sandbox no sistema financeiro brasileiro. **RBSD – Revista Brasileira de Sociologia do Direito**, v. 10, n. 3, p. 143-171, 2023. Disponível em: https://revista.abrasd.com.br/index.php/rbsd/article/view/747 . Acesso em 23 set. 2024.

AMATO, Lucas Fucci. Structural litigation, destabilization rights and trans-judicial cooperation networks: lessons from comparative constitutional law. **Suprema, Revista de Estudos Constitucionais**, 2024a.

AMATO, Lucas Fucci. **O direito da sociedade digital:** tecnologia, inovação jurídica e aprendizagem regulatória. São Paulo: Faculdade de Direito da Universidade de São Paulo, 2024b. p. 392-410. Disponível em:

https://www.livrosabertos.abcd.usp.br/portaldelivrosUSP/catalog/book/1314 . Acesso em 22 set. 2024.

BEN-SHAHAR, Omri. Data pollution. **Journal of Legal Analysis**, v. 11, p. 104-159, 2019.

BIBER, Eric; LIGHT, Sarah E.; RUHL, J. B.; SALZMAN, James. Regulating Business Innovation as Policy Disruption: From the Model T to Airbnb. **Vanderbilt Law Review**, v. 70, n. 5, p. 1561-1626, 2017.

CAMPILONGO, Celso Fernandes. Assistência Jurídica e Advocacia popular: serviços legais em São Bernardo do Campo. *In:* CAMPILONGO, Celso Fernandes. **O direito na sociedade complexa.** 2 ed. São Paulo: Saraiva, 2011 [1991]. p. 17-49.

CAMPILONGO, Celso Fernandes. **Interpretação do direito e movimentos sociais:** hermenêutica do sistema jurídico e da sociedade. Rio de Janeiro: Campus Elsevier, 2012.

CHRISTENSEN, Clayton M. **The innovator's dilemma:** when new technologies cause great firms to fail. Boston: Harvard Business School Press, 1997.

DELMAS-MARTY, Meirelle. **Por um direito comum.** Tradução de Maria Ermantina de Almeida Prado Galvão. São Paulo: Martins Fontes, 2004 [1994].

GODOY, Daniel Gabrilli de. **O direito na era da interconexão tecnológica.** 2024. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2024.

HOBBES, Thomas. **Leviatã, ou matéria, forma e poder de uma república eclesiástica e civil.** Edição de Richard Tuck. Tradução de João Paulo Monteiro e Maria Beatriz Nizza da Silva. São Paulo: Martins Fontes, 2003 [1651].

KUHN, Thomas Samuel. **A estrutura das revoluções científicas.** Tradução de Beatriz Vianna Boeira e Nelson Boeira. 9 ed. São Paulo: Perspectiva, 2007 [1969].

LARA, Gustavo Dalpupo de. **Institutional alternatives for a high-energy democracy and experimentalist constitutionalism in Brazil.** 2024. Tese (Doutorado em Direito) – Universidade Federal do Paraná, Curitiba, 2024.

LUHMANN, Niklas. **Law as a social system.** Tradução de Klaus A. Ziegert. Oxford: Oxford University Press, 2004 [1993].

MORTOZA, Pedro Henrique Partata. O sigilo de dados e a Sociologia da Constituição: um diálogo entre Tércio Sampaio Ferraz Jr. e Giancarlo Corsi sobre o conteúdo e a função dos direitos fundamentais. *In:* AMATO, Lucas Fucci; RIBEIRO, Rodrigo Marchetti (orgs.). **Sociologia & História do Constitucionalismo Brasileiro.** São Paulo: Faculdade de Direito da Universidade de São Paulo, 2024. p. 392-410. Disponível em: https://www.livrosabertos.abcd.usp.br/portaldelivrosUSP/catalog/view/1384/1261/4873 . Acesso em 22 set. 2024.

MOSCA, Gaetano. **The ruling class.** Tradução de Hannah D. Kahn. New York: McGraw-Hill, 1939 [1896].

NEGÓCIO, Ramon. Dos problemas constitucionais diluídos na rede à construção de uma *lex meta*. **Revista Direito Mackenzie**, v. 17, n. 1, p. 1-22, 2023. Disponível em: https://editorarevistas.mackenzie.br/index.php/rmd/article/download/15791/12366/77214 . Acesso em 22 set. 2024.

POLANYI, Michael. Profits and polycentricity. *In:* POLANYI, Michael. **The logic of liberty:** reflections and rejoinders. Indianapolis: Liberty Fund, 1951 [1946]. p. 170-188.

SABA, Diana; AMATO, Lucas Fucci; BARROS, Marco Antonio Loschiavo Leme de; PONCE, Paula Pedigoni. **Fake news e eleições:** estudo sociojurídico sobre política, comunicação digital e regulação no Brasil. Porto Alegre: Editora Fi, 2021. Disponível em: https://www.editorafi.org/203fakenews . Acesso em 13 abr. 2024.

SCHUMPETER, Joseph A. **The theory of economic development:** an inquiry into profits, capital, credit, interest, and the business cycle. Tradução de Redvers Opie. Cambridge, MA: Harvard University Press, 1949 [1934].

SCIULLI, David. **Theory of societal constitutionalism:** foundations of a non-Marxist critical theory. Cambridge: Cambridge University Press, 1992.

SCIULLI, David. **Corporate power in civil society:** an application of societal constitutionalism. New York: New York University Press, 2001.

SIMON, Herbert A. **The sciences of the artificial.** 3 ed. Cambridge, MA: MIT Press, 2019 [1968].

UNGER, Roberto Mangabeira. **False necessity:** anti-necessitarian social theory in the service of radical democracy. From Politics, a work in constructive social theory. 2 ed. London: Verso, 2001 [1987].

UNGER, Roberto Mangabeira. **A economia do conhecimento.** Tradução de Leonardo Castro. São Paulo: Autonomia Literária, 2018.

WÖRLE, Karl; GSTREIN, Oskar Josef. Collective Data Protection Litigation: A Comparative Analysis of EU Representative Actions and US Class Actions Enforcing Data Protection Rights. **European Journal of Comparative Law and Governance**, v. 11, n. 2, p. 275-308, 2024. Disponível em: https://brill.com/view/journals/ejcl/11/2/article-p275_003.xml. Acesso em 23 set. 2024.

ZANATTA, Rafael Augusto Ferreira. Imunidade, desestabilização e propriedade: o sistema de direitos em Unger. *In:* TEIXEIRA, Carlos Sávio (org.). **Rebeldia Imaginada:** instituições e alternativas no pensamento de Roberto Mangabeira Unger. São Paulo: Autonomia Literária, 2019. p. 241-287.

ZANATTA, Rafael Augusto Ferreira. **A proteção coletiva dos dados pessoais no Brasil:** a defesa de direitos entre autoritarismo e democracia. 2022. Tese (Doutorado em Ciência Ambiental) – Instituto de Energia e Ambiente da Universidade de São Paulo, São Paulo, 2022.

ZANATTA, Rafael Augusto Ferreira. **A ANPD no banco dos réus?** Coletivização da proteção de dados e seus efeitos colaterais. Texto ainda inédito. 2024. Disponível em: https://www.researchgate.net/publication/382640345_A_ANPD_no_banco_dos_reus_Coletivizacao_da_protecao_de_dados_e_seus_efeitos_colaterais . Acesso em 23 set. 2024.

3. Constitucionalismo societal no mundo digital[8]

Angelo Golia Jr.[9]

Gunther Teubner[10]

Tradução de Caio Rezende Missagia[11]

Introdução

Este capítulo introduziu originalmente o número do *Indiana Journal of Legal Studies* dedicado ao do simpósio "Constituição Digital: Sobre o Potencial Transformativo do Constitucionalismo Societal" (*Digital Constitution: On the Transformative Potential of Societal Constitutionalism*), em que um grupo de acadêmicos, utilizando o constitucionalismo societal como teoria de fundo, apresentou propostas concretas para um direito constitucional digital. Dessa forma, este número do simpósio procurou responder a três questões inter-relacionadas: Qual é a mensagem do constitucionalismo societal para a emergente constituição digital? Como podem os princípios fundamentais das constituições dos Estados-nação ser generalizados e reespecificados para a

[8] Publicado originalmente no dossiê: GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). Digital constitution: on the transformative potential of societal constitutionalism. **Indiana Journal of Global Legal Studies**, v. 30, n. 2, 2023. Tradução e publicação autorizada pelos autores. Os autores agradecem à equipe editorial do *Indiana Journal of Global Legal Studies*, especialmente a Alfred C. Aman Jr., Emma DeLaney Strenski e Daniel Schumick. Gostaríamos também de agradecer aos participantes do workshop "*Digital Constitution: On the Transformative Potential of Societal Constitutionalism*", realizado nos dias 17 e 18 de junho de 2022 e, em especial, aos colegas que generosamente atuaram como debatedores dos artigos preliminares apresentados na ocasião: Francisco de Abreu Duarte, Lorenzo Gradoni, Amy Kapczynski, Fleur Johns, Marta Maroni, José Gustavo Prieto Muñoz e Sofia Ranchordás. Por fim, os autores agradecem a Anne Peters, a Julieta Lobato, por seus comentários e apoio, bem como ao Instituto Max Planck de Direito Público Comparado e Direito Internacional e ao centro de pesquisa "Normative Orders", da Universidade Goethe, por seu apoio institucional. Todos os sites foram visitados pela última vez em 8 de março de 2023, salvo indicação em contrário.

[9] Professor assistente da Faculdade de Direito da Universidade de Trento.

[10] Professor emérito da Universidade Goethe, Frankfurt.

[11] Mestrando em Filosofia e Teoria Geral do Direito pela Faculdade de Direito da Universidade de São Paulo (USP). Graduado em Direito pela USP e pela *Université Jean-Monnet Saint-Etienne (licence en Droit)* e pós-graduado em Administração de Empresas pela Fundação Getúlio Vargas (FGV EAESP).

digitalidade global com uma perspectiva transformativa? Como seriam os novos arranjos institucionais e práticas interpretativas? Nesta introdução, procuramos superar três tendências reducionistas legadas pelo constitucionalismo tradicional (seção II). Argumentamos que o constitucionalismo digital deve olhar para além (1) do ainda dominante estadocentrismo dos princípios constitucionais, (2) do seu foco exclusivo no poder político e (3) da sua interpretação estritamente individualista dos direitos constitucionais. Essa desconstrução permite enxergar as principais ameaças constitucionais colocadas pela digitalização – em particular, aquilo a que chamamos a dupla colonização do espaço digital – e para possíveis contra-estratégias inspiradas pelo constitucionalismo societal (seção III). Em seguida, delineamos o conteúdo das contribuições para aquele simpósio, agrupadas em quatro áreas: (1) reformulação da elaboração constitucional e legislativa; (2) economia digital; (3) instituições do constitucionalismo; (4) justiça digital (seção IV). Por fim, apontamos para desenvolvimentos futuros, bem como para as ligações a outras vertentes da literatura que focam na relação entre as tecnologias digitais e o direito (constitucional) (seção V).

I. Explorando o potencial transformativo do constitucionalismo digital através do constitucionalismo societal

O constitucionalismo estadocêntrico tradicional não consegue acompanhar os perigos inerentes à revolução digital. O código digital aumenta o frequentemente discutido potencial (auto)destrutivo da economia capitalista, do sistema político democrático, da ciência autónoma, da tecnologia e da religião militante. A digitalização está acelerando as tendências expansivas internas da diferenciação funcional: as simultâneas politização, monetização, cientifização e juridificação da sociedade. O capitalismo de vigilância (ZUBOFF, 2019), o poder informacional (ver *e.g.* KAPCZYNSKI, 2020; COHEN, 2019), a radicalização política e religiosa das mídias sociais (cf., entre outros, VAIDHYANATHAN, 2018; e, para uma análise empiricamente embasada dos efeitos das mídias sociais na coesão social e na democracia, ver GONZÁLEZ-BAILÓN; LELKES, 2023) são

apenas algumas das dinâmicas comunicativas irrestritas que são amplificadas pela aplicação do código digital.

Contra estas tendências, o constitucionalismo digital, uma vertente emergente do campo acadêmico constitucional, propõe questionar se os princípios fundamentais do constitucionalismo – nomeadamente, a separação de poderes, a democracia, os direitos fundamentais, o Estado de Direito – também podem ser estabelecidos no mundo digital (ver *e.g.* DE GREGORIO, 2022; CELESTE, 2019; KETTEMANN, 2020; SUZOR, 2019; GILL *et al.*, 2018). Tais princípios devem ser reformulados para que possam reagir ao potencial (auto)destrutivo da comunicação digital. O constitucionalismo digital, portanto, vai além do constitucionalismo estadocêntrico de duas maneiras: ele atravessa a divisão nacional/transnacional, bem como a divisão Estado/sociedade. Assim, combina diferentes perspectivas: a do Estado-nação, a global e a social (cf. DUARTE *et al.*, no prelo).

O constitucionalismo digital pode ser visto como parte do discurso sobre o constitucionalismo societal, que nas últimas duas décadas se desenvolveu no âmbito do universo mais amplo do constitucionalismo global (para dois tratamentos monográficos, ver TEUBNER, 2012; KJAER, 2014; para uma reformulação levando em conta as críticas e os debates, ver GOLIA; TEUBNER, 2021; sobre o constitucionalismo global, ver WIENER *et al.*, p. 7, 2012; WALKER, p. 97, 2014). Enquanto teoria do pluralismo jurídico *e* constitucional, o constitucionalismo societal tem sido objeto de um amplo debate (*e.g.* CHRISTODOULIDIS, 2021; WATT, 2018; MUNCK, 2016). É revelador o fato de uma das suas primeiras formulações abrangentes ter utilizado a esfera digital como estudo de caso (TEUBNER, 2004).

Até agora, o constitucionalismo societal tem sido utilizado principalmente como estrutura analítica para enquadrar questões do constitucionalismo digital (ver *e.g.* CELESTE, 2022; GRADONI, 2021; SHEFFI, 2020; GILL *et al.*, 2018; BASSINI, 2018). No entanto, as suas dimensões *normativa* e *transformativa* ainda têm de ser exploradas. De fato, a literatura relevante raramente desenvolveu propostas jurídicas concretas com base nesse quadro. O risco é tornar tanto o

constitucionalismo societal quanto o digital incapazes de uma crítica que se ocupe do poder societal na esfera digital e que estabeleça padrões normativos claros.

O principal objetivo deste número do simpósio é explorar o potencial transformativo do constitucionalismo digital através das lentes do constitucionalismo societal. Utilizando o constitucionalismo societal como teoria de fundo, um grupo de acadêmicos apresenta propostas concretas para um *direito constitucional digital*. Dessa forma, este número do simpósio procura responder a três questões inter-relacionadas: Qual é a mensagem do constitucionalismo societal para a emergente constituição digital? Como podem os princípios fundamentais das constituições dos Estados-nação ser generalizados e reespecificados para a digitalidade global com uma perspectiva transformativa? Como seriam os novos arranjos institucionais e práticas interpretativas?

Nesta introdução, pretendemos superar três tendências redutoras legadas pelo constitucionalismo tradicional (seção II). Argumentamos que o constitucionalismo digital deve olhar para além (1) do ainda dominante estadocentrismo dos princípios constitucionais, (2) do seu foco exclusivo no poder político e (3) da sua interpretação estritamente individualista dos direitos constitucionais. Essa desconstrução permite enxergar as principais ameaças constitucionais colocadas pela digitalização – em particular, aquilo a que chamamos a dupla colonização do espaço digital – e para possíveis contra-estratégias inspiradas pelo constitucionalismo societal (seção III). Em seguida, delineamos o conteúdo das contribuições para este simpósio, agrupadas em quatro áreas: (1) reformulação da elaboração constitucional e legislativa; (2) economia digital; (3) instituições do constitucionalismo; (4) justiça digital (seção IV). Por fim, apontamos para desenvolvimentos futuros, bem como para as ligações a outras vertentes da literatura que focam na relação entre as tecnologias digitais e o direito (constitucional) (seção V).

II. Constituições digitais para além da teoria constitucional tradicional

Contra o estadocentrismo. Sem dúvida, o constitucionalismo estatal tradicional ainda tem um potencial considerável de proteção contra o autoritarismo digital no sistema político. O "Sistema de Crédito Social" da China (ver *e.g.* MIOTTO; CHEN, 2022; JAKOB, 2021; BACKER, 2021), bem como o policiamento preditivo dos EUA (SOW, 2022; RENARD, 2022; BRAYNE, 2017), ambos os quais utilizam tecnologias digitais para suprimir potenciais ameaças ao poder do Estado, são casos exemplares. A fim de preservar o potencial democrático das tecnologias digitais contra uma política repressiva, as constituições dos Estados têm de estabelecer novas regras de proteção, *e.g.*, o livre e contínuo acesso à Internet e a preservação do anonimato em determinadas condições (ver, de duas perspectivas distintas, OKIDEGBE, 2022; LUCKNER, 2022; e, da perspectiva de um ativista envolvido na revolução egípcia pós-Primavera Árabe, EL-FATTAH, 2021). No entanto, é errado reduzir o constitucionalismo digital a um conjunto de direitos, normas de governança e limitações ao exercício do poder dos Estados na Internet. O constitucionalismo estadocêntrico não consegue abordar o poder (coletivo) exercido pelos agentes privados. Contra tendências repressivas em setores não estatais da sociedade, *i.e.*, em transações de mercado, organizações formais ou regimes transnacionais, a proteção constitucional tem de ir muito além das ameaças de poder do mundo estatal.

Atualmente, o espaço digital é o novo setor não estatal da sociedade global que demanda uma constitucionalização abrangente. Isso não requer apenas novas regras *constitutivas*, ou seja, estruturas institucionais complexas que sustentem o surgimento e a ação de agentes relevantes, incluindo textos normativos de nível superior (ver CELESTE, 2022) e redes intrincadas de organizações e procedimentos (cf., neste número do simpósio, PEREZ; WIMER, 2023; e SHEFFI, no prelo). Ainda mais urgente é a demanda por novas regras *limitativas*, produzidas tanto pelo direito estatal e quanto pelo não estatal, dirigidas contra o poder digital de agentes privados, notadamente as práticas

anticoncorrenciais do Vale do Silício e das "BigTechs" (ver STOLTON, 2022; BOROWSKA, 2020; TEACHOUT, 2020; PETIT, 2020).

Para além do poder (social). Há, no entanto, um segundo reducionismo, mais sutil. Embora os intermediários digitais, enquanto novos centros extraestatais de poder, sejam o alvo legítimo da crítica política, não é suficiente, nesse contexto, concentrar-se exclusivamente no poder.[12] A preocupação com o poder social obscurece os excessos de outros meios de comunicação expansivos (dinheiro, conhecimento, autoridade jurídica)[13] que – mesmo em situações em que os centros de poder social estão ausentes – exigem limitação constitucional (para esse argumento em maior detalhe, HENSEL; TEUBNER, 2016). As estratégias constitucionais devem buscar desenvolver regras limitativas não só contra as externalidades negativas produzidas pelo imperativo de poder da política, mas também – e particularmente – contra as externalidades do imperativo de lucro da economia, o imperativo de reputação da ciência, o imperativo de inovação da tecnologia, o imperativo de notícias dos meios de informação, o imperativo de saúde do sistema médico e o imperativo de juridificação do direito (ver, de forma mais geral, TEUBNER, 2020; e, especificamente com relação ao constitucionalismo digital, GOLIA, 2022).

A própria digitalidade é o novo meio de comunicação contra cujas externalidades é necessária proteção constitucional. Entre elas, a mais evidente é a tendência da tecnologia digital a criar as suas próprias realidades sociais. Essa "hiper-realidade" tem o potencial de monopolizar a comunicação em outros

[12] Aqui entendido não como coerção ou meramente como influência egoística no comportamento dos atores sociais, mas como um meio de comunicação específico (ver nota 2 *infra*) que torna provável a aceitação das ações de Alter como premissas das ações do Ego. Na sociedade funcionalmente diferenciada, o poder é o meio específico do sistema político. Ele também pode ser potencialmente realizado em outros sistemas, mas sem conseguir obter a sua capacidade de reprodução que tem na política. De fato, o poder se reproduz na forma de obediência a um comando. Em outras palavras, ele é realizado quando a sequência de ação comando-obediência é combinada com uma sequência de ameaça de sanção (se você não obedecer, eu o punirei): cf. BARALDI *et al.*, 2021).

[13] Entendidos como os "mecanismos de efeito" da sociedade funcionalmente diferenciada. Os meios de comunicação "[...] baseiam-se em símbolos que são considerados eficazes na comunicação – *e.g.* símbolos de dinheiro, poder, verdade ou amor – e que, como símbolos efetivamente eficazes, motivam outros atores sociais a fazer algo que não teriam feito sem esse uso eficaz de símbolos" (STICHWEH, 2011).

mundos (naturais), de totalizar a sua própria construção da realidade à custa de outras (cf. SOW, 2022; WANG, 2022). "Com o virtual, entramos não só na era da liquidação do real e do referencial, mas também na do extermínio do outro" (BALDWIN, 2015). Na sua relação com o direito, o código digital cria ordens normativas autônomas e tende a minar a ordem normativa do direito. Uma vez que os cálculos rígidos dos algoritmos induzem uma fusão entre a criação, a aplicação e a imposição unilaterais de regras, corre-se o risco de que tais ordens destruam os aspectos civilizantes e humanizantes do Estado de direito, nomeadamente a hermenêutica da argumentação jurídica.[14]

Para além dos direitos individuais. Aqui entra o terceiro reducionismo do constitucionalismo tradicional – a dimensão exclusivamente individualista dos direitos constitucionais. É claro que uma Declaração de Direitos para os usuários individuais das redes sociais é importante para combater os efeitos nocivos da digitalidade na privacidade, na saúde mental e no envolvimento político dos cidadãos.[15] "Vulnerabilidades digitais" refere-se a um projeto político que explora a forma como as tecnologias digitais exacerbam as vulnerabilidades humanas pré-existentes ou criam novas vulnerabilidades.[16] No entanto, "a verdadeira questão dos direitos fundamentais situa-se no *nível discursivo transindividual*. As plataformas são sistemas sociais expansivos, que podem frustrar a autorreprodução autônoma da sociedade" (GRABER, 2020; ver também RACHLITZ *et al.*, 2021). Assim, o constitucionalismo societal, indo além da dimensão individual, concentra-se na igualmente importante dimensão institucional dos direitos constitucionais. Isso significa proteger a integridade das formações sociais vulneráveis e dos agentes coletivos menos poderosos

[14] Ver DIVER, 2021; MARKOU; DEAKIN, 2020. Sobre essas questões, ver também LESSIG, 1999. Neste número do simpósio, ver, em especial, as contribuições de Tania Sourdin (2023); e Giovanni De Gregorio (2023).

[15] "A Social Network Users' Bill of Rights", Christina M. Gagnier e Gagnier Margossian (Conferência sobre Computadores, Liberdade e Privacidade), modificado por último em 26 de março de 2011, disponível em: https://www.w3.org/2011/track-privacy/papers/GagnierMargossian.pdf. Para um relato recente, ver, neste número do simpósio, CELESTE, 2023.

[16] O que Camilla Crea *et al.* definem como "vulnerabilidade digital": ver em https://www.dirittocomparato.org/wp-content/uploads/2022/07/7.-CALL-FOR-INTEREST_DiVE.pdf. Ver também DOMURATH, 2023.

(movimentos de protesto, sindicatos, meios de comunicação independentes, instituições de ensino e de pesquisa) contra a sua intromissão. Por exemplo, "enquanto direito fundamental, a liberdade acadêmica protege a autonomia individual do acadêmico, mas também facilita a diferenciação funcional dos sistemas societais, neste caso, protegendo a ciência contra intrusões indevidas da política, da economia ou da religião" (VERSCHRAEGEN, p. 164, 2018). E instituições igualmente vulneráveis estão surgindo também nos espaços sociodigitais, *e.g.*, a Wikipédia, o movimento do código aberto (*open-source movement*), os bens comuns digitais, os repositórios públicos de *software* e os movimentos sociais de trabalhadores das plataformas (ver HAIDAR; KEUNE, 2021; PAPADAKIS; MEXI, 2021), todos os quais, na sua ainda frágil autonomia, demandam proteção constitucional.

III. Dupla colonização, a nova economia política digital e contra-estratégias: resistibilidade e contestabilidade

Até aqui, concentramo-nos nos problemas constitucionais criados pela própria tecnologia digital. Além disso, o constitucionalismo societal identifica ameaças futuras que se escondem em outro lugar, ou seja, nos efeitos negativos da digitalização na estrutura *policontextural* da sociedade contemporânea.[17] Quando os dois sistemas funcionais dominantes – a política e a economia – são digitalizados de forma abrangente, as pressões das suas mais-valias, o lucro e o poder, são maciçamente reforçadas pelas igualmente fortes pressões da mais-valia da digitalidade.[18] Internamente, a digitalização intensifica a dinâmica de crescimento endógeno nos sistemas político e econômico. Externamente, ela agrava as tendências expansivas de tais sistemas em direção a outros sistemas sociais. Ambas as tendências resultam na dupla colonização do espaço digital (cf., de uma perspectiva habermasiana, WANG, 2022): o complexo poder-lucro

[17] Entendemos "policontexturalidade" como uma característica marcante das sociedades modernas: a pluralidade de perspectivas sociais mutuamente irredutíveis. Elas são incompatíveis entre si e só podem ser superadas com a rejeição de determinados valores, o que, por sua vez, leva a diferentes distinções binárias. Ver GÜNTHER, 1976.

[18] Para as primeiras advertências contra os perigos decorrentes do acoplamento dominante de "governo" e "comércio", ver LESSIG, 1999, p. 4 e seguintes.

produz um totalitarismo digital que impede a potencial evolução plural da digitalidade. Ele reduz a estrutura policontextural do espaço digital ao duopólio de poderosos setores: um "setor público" impulsionado pelo poder digitalizado e um "sector privado" impulsionado pelo lucro digitalizado. Esse duopólio dominante – que poderia ser designado como a nova "economia política digital"[19] – tem o potencial de corromper estruturalmente as novas mas ainda frágeis instituições sociodigitais[20] que estão emergindo nos outros domínios sociais: ciência, educação, saúde e arte. A nova distopia é a fusão do *homo oeconomicus* e do *homo politicus* no *homo digitalis*, em que a inclusão, a emancipação e a efetiva participação dos atores sociais em diferentes campos sociais se torna cada vez mais dependente de se e em que medida esses atores contribuem para a acumulação de poder e de lucro por meios digitais (cf. VESTING, esp. cap. 9, 2021). Em termos normativos, o combate a esse cenário distópico implica três estratégias constitucionais.

Uma primeira estratégia consiste em desenvolver restrições constitucionais à política digitalizada. Como já foi referido, quando a digitalização reforça o poder do Estado, o potencial repressivo dos sistemas políticos intensifica-se. Contra isso, o constitucionalismo estatal tradicional terá, de fato, de cumprir a sua promessa centenária: consolidar o Estado de direito, reforçar os direitos constitucionais e combater as práticas antidemocráticas. No entanto, para os novos perigos do poder estatal digitalizado, os princípios fundamentais do constitucionalismo estatal têm de ser transformados na sua contrapartida societal. São necessárias a sua generalização em estratégias constitucionais mais amplas e a sua reespecificação para o poder digital. O constitucionalismo digital terá de impor limites severos à vigilância biométrica

[19] Como ele é inspirado principalmente pelas características policontextuais das sociedades modernas, entendemos esse conceito de uma forma próxima a Fleur Johns (2021). Ver também COHEN, 2012; VILJOEN, 2021-2022; BURRELL; FOURCADE, 2021. Portanto, o conceito não está necessariamente alinhado às abordagens atuais de "*law and political economy*" (LPE): ver, entre muitas contribuições, PISTOR, 2019; KAPCZYNSKI, 2020. Ver também a seção V *infra*.

[20] Ver VERSCHRAEGEN, 2018, p. 179: "A intrusão da racionalidade econômica na ciência pode criar uma forma de 'corrupção estrutural' (em oposição à corrupção pessoal), não apenas exercendo pressões para a privatização e comercialização dos resultados da pesquisa, mas também afetando o processo de pesquisa e os próprios resultados."

(BRAYNE, 2017; BURRELL; FOURCADE, 2021, p. 221-226; CASTETS-RENARD, 2022), à tomada de decisões automatizada (ver ZALNIERIUTE *et al.*, 2019) e às tecnologias de "*hypernudge*" que utilizam Big Data para a regulação *by design* (ver YEUNG, 2017; e, mais genericamente, REICHMAN; SARTOR, 2022).

Uma segunda estratégia consiste em estabelecer limites constitucionais à utilização de algoritmos para maximizar o lucro. A economicização do meio digital é o ponto cego do constitucionalismo tradicional, que tenta apenas limitar o poder do Estado. As tecnologias digitais aumentaram as tendências de mercantilização do capitalismo global (COHEN, 2019). A combinação de mercados oligopolistas e modelos de negócio baseados em dados expandiu dramaticamente a possibilidade de os agentes econômicos afetarem a sociedade por meio do código de acumulação econômica. Em particular, as estratégias do capitalismo informacional combinam as pressões da maximização do lucro com as pressões da digitalidade para maximizar atenção. Estudos empíricos produziram "poderosas evidências observáveis de dinâmicas destrutivas, incluindo a rápida difusão de desinformação, campanhas de manipulação, (auto)segregação ideológica e extremismo" (ver GONZÁLEZ-BAILÓN; LELKES, 2023), as quais são produzidas pela maximização da atenção digital. Isso exige novas medidas constitucionais contra os protocolos de redes tecnológicas que se autorreforçam.

Atualmente, algumas contra-estratégias constitucionais estão lentamente surgindo. O *Digital Services Act* (DSA) adotado pela União Europeia[21] é um experimento regulatório extremamente significativo cujos efeitos concretos só surgirão no futuro. Ele proíbe a utilização de ajustes de experiência do usuário (*UX – user experience*) para manipular ou forçar o consentimento e exige que as plataformas ofereçam paridade nos fluxos de consentimento para recusar ou concordar em entregar dados (art. 25); a definição de perfis de menores (art. 28); a utilização de dados pessoais sensíveis (como origem racial ou étnica, filiação política ou religiosa, sexualidade ou dados de saúde) para a segmentação

[21] Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único de serviços digitais e que altera a Diretiva 2000/31/CE.

comportamental (*behavioral targetting*) (art. 26, par. 3). Um elemento adicional importante é o acesso aos dados e o controle das operações algorítmicas subjacentes, a fim de tornar transparente a forma como o objetivo de maximizar o lucro se sobrepõe a operações técnicas "inocentes". Nesse sentido, o DSA aproxima-se das restrições constitucionais da economia digitalizada quando exige que as "plataformas *online* de muito grande dimensão" realizem e publiquem periodicamente avaliações relativas a riscos sistémicos, em especial antes do lançamento de novos serviços (art. 34), com correspondentes obrigações de mitigação (art. 35); a supervisão regulatória dos seus algoritmos e o acesso de investigadores de interesse público aos dados para permitir o exame independente dos efeitos das plataformas (art. 40).

Para além das características de instrumentos específicos como o DSA, os órgãos de resolução de litígios têm de começar a rever os regulamentos "privados" dos "governantes digitais" (KLONICK, 2018) com controles de longo alcance, espelhando a revisão constitucional da legislação estatal realizada pelos tribunais estatais (cf. HOLZNAGEL, 2021). Nesse sentido, é crucial enquadrar os termos de uso das plataformas digitais não simplesmente como contratos padronizados, mas como formas de poder legislativo unilateral.[22] Com efeito, as plataformas exercem cada vez mais o seu poder "através de contratos de 'termos de serviço' não negociáveis, unilaterais e deliberadamente opacos" (ver *e.g.* BYGRAVE, 2015; HARTZOG *et al.*, 2013). Portanto, os tribunais têm de impor normas de escrutínio rigoroso aos regimes privados de governo digital. Mais importante ainda, eles devem basear-se em mais do que o consentimento legal dos indivíduos, porque este não leva em conta problemas de informação assimétrica, poder de negociação desigual ou externalidades negativas coletivas (cf. HUMMEL *et al.*, 2021; COFONE, 2021; TISNÉ; SCHAAKE, 2020). Assim, o direito privado que controla a equidade das disposições contratuais é – deve ser – transformado em um controle constitucional do direito não estatal emergente na economia digitalizada, um tipo novo e cada vez mais importante de controle

[22] Para um caso exemplar nessa direção, ver o caso recente *CasaPound v. Facebook*, Tribunal de Roma, sentença nº 17909/2022 de 5 de dezembro de 2022.

constitucional realizado por órgãos judiciais estatais e não estatais. Dessa perspectiva, a litigância estratégica, ativada por atores individuais e coletivos, baseada tanto em regras estatais quanto não estatais, é um precioso instrumento adicional para desencadear o surgimento de normas constitucionais constitutivas e limitativas na esfera digital (cf., no campo do direito público internacional, STROBEL, 2022; e, para o sistema normativo não estatal da Meta, GOLIA, 2023).

Além disso, o direito antitruste deve intervir e desenvolver regras constitucionais para proteger a integridade dos processos informacionais nas redes digitais, *e.g.* – novamente – proibindo "padrões obscuros" desleais e outras práticas digitais manipulativas (CARA, 2019). Outra proposta, inspirada nos modelos de direito societário do norte da Europa, estabeleceria formas de decisão conjunta com representantes externos de interesses coletivos (saúde, ciência, meio ambiente) nos conselhos de administração dos fornecedores de serviços digitais. Tudo isso equivaleria a um constitucionalismo societal "por procedimento", impondo um quadro procedimental obrigatório para a autolimitação dos processos digitais (WIELSCH, 2019). Também aqui, um outro instrumento no âmbito dos recentes esforços regulatórios da União Europeia, o *Digital Markets Act* (DMA)[23], apresenta desenvolvimentos interessantes, notavelmente as disposições que envolvem terceiros e concorrentes nas funções de monitoramento e *compliance* (arts. 27 e 28).

Uma terceira estratégia foca nas instituições de uma "sociedade civil digital". O seu objetivo é proteger os setores não estatais/sem fins lucrativos do espaço digital em termos constitucionais. Contra a dupla colonização pelo lucro e pelo poder, a integridade da ciência, do jornalismo, da educação, da medicina e da arte demanda proteção constitucional (para a proteção da ciência, especialmente da perspectiva do direito internacional dos direitos humanos, ver KUNZ, 2022; VERSCHRAEGEN, 2018). Assim, o terceiro setor digital demanda regras constitutivas para o desenvolvimento de instituições sociodigitais

[23] 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.

estáveis: comunidades de *hackers*, ONGs digitais, bens comuns digitais, Wikipédia, código aberto (*open source*). No entanto, a chamada tragédia dos bens comuns digitais revela tendências autodestrutivas mesmo no seio da sociedade civil digital (cf. SHARMA, 2023). O usuário médio das tecnologias da informação explora os recursos comuns até que estes não possam mais ser recuperados. Os usuários não prestam atenção às consequências do seu comportamento. A tragédia dos bens comuns digitais tem uma segunda consequência – a poluição da infosfera, *i.e.*, a utilização indiscriminada e incorreta da tecnologia e dos recursos digitais e a superprodução de dados. O excesso de informação conduz à corrupção da comunicação e à sobrecarga de informação. Ambas as tendências constituem o campo legítimo da autolimitação constitucional, que precisa ser apoiada por pressões externas da política e da sociedade civil.

Mas, mais importante ainda, o terceiro setor digital precisa de regras fortes contra as pressões externas de ambas as mais-valias do lucro e do poder. A integridade da ciência é afetada por externalidades negativas produzidas pela economia política digital à medida que a digitalização e a chamada reinterpretação econômica do acesso aberto (*open access*) aumentam as dinâmicas de publicar ou perecer (*publish or perish*), de procura de reputação e a publicação predatória, reforçando a posição dos agentes hegemônicos na ciência.[24] As grandes empresas editoriais, como Elsevier, Wiley e Springer, estão em posição de, invisível e estrategicamente, "exercerem controle sobre as principais decisões universitárias – desde a avaliação dos estudantes, até a integridade da pesquisa e o planeamento financeiro" (ASPESI, 2019, p. 5). Do mesmo modo, a integridade do jornalismo é ameaçada pela *web analytics* em tempo real, *clickbaits* e por bolhas de informação, dinâmicas que já conduziram a mudanças importantes: consolidação de grandes organizações noticiosas (MILANOVIC, 2020) e transformação das maneiras como o jornalismo concebe a si mesmo enquanto categoria profissional e como ele se auto-organiza (cf. PICKARD, 2022; BASTIAN *et al.*, 2021).

[24] Ver KUNZ, p. 43-45, 2021; e, de forma mais geral, o debate "Open/Closed", disponível em: https://verfassungsblog.de/category/debates/open-closed/.

As contra-estratégias constitucionais inspiradas no constitucionalismo societal são expressas por dois conceitos-chave: resistibilidade e contestabilidade. Estas representam duas faces de uma estratégia coerente contra a dupla colonização do espaço digital pelo complexo poder-lucro. Essa estratégia tem o potencial de transformar o constitucionalismo digital de um conceito acadêmico em um movimento sociopolítico.[25] A resistibilidade implica a defesa da sociedade civil contra a economia política da digitalidade. Contra as tendências colonizadoras da política digitalizada, ela terá de criar um contrapoder social, principalmente por meio de movimentos de protesto e grupos da sociedade civil. Isto não é apenas um desejo ilusório. De fato, "a utilização da governança algorítmica em contextos de risco cada vez mais elevado gerou uma onda de ativismo, militância e resistência" (BLOCH-WEHBA, 2022, ao apresentar três estudos de caso sobre como movimentos sociais e trabalhistas estão respondendo às dramáticas mudanças na governança digital). Contra a excessiva economicização do mundo digital, as estratégias de ameaça ao lucro são os instrumentos mais promissores que o direito e a política poderão impor. A contestabilidade implicará, internamente, a proteção da autocontestação. As plataformas digitais terão de permitir procedimentos de oposição interna e de denúncia de irregularidades. Externamente, é necessária a expansão do acesso à justiça, contra a política algorítmica e a economia digitalizada. Em última análise, este número do simpósio apela à "imaginação institucional" no sentido de Roberto Unger (1996), apresentando uma perspectiva crítica, normativa e transformadora e visando oferecer propostas concretas no contexto mais amplo do constitucionalismo digital.

[25] Neste número do simpósio, Celeste (2023) observa corretamente que as inúmeras propostas de Declarações de Direitos digitais que surgiram nos últimos anos são indicadores de um movimento social que produz contra-estratégias constitucionais.

IV. Contribuições do simpósio sobre quatro macrotemas: elaboração constitucional, economia digital, instituições do constitucionalismo, justiça digital

Passamos agora a descrever brevemente o conteúdo das contribuições individuais deste número do simpósio. Todos os autores já tinham se dedicado a questões de direito e política digitais. Expandindo os seus trabalhos anteriores, abordam questões cruciais do constitucionalismo digital através das lentes do constitucionalismo societal e apresentam propostas concretas. Em particular, os autores examinam abordagens experimentais. Por meio de estudos de casos em diferentes domínios, apontam deficiências e apresentam alternativas. Além disso, refletem criticamente sobre o impacto das novas soluções tanto nas posições hegemónicas e quanto nas subalternas afetadas pelas tecnologias digitais. Este número do simpósio está organizada em quatro seções, cada uma abordando problemas substantivos e procedimentais do constitucionalismo digital.

A primeira seção aborda a o processo de elaboração constitucional através do código digital. Edoardo Celeste analisa o potencial das chamadas "Declarações de Direitos da Internet". Estas generalizam e reespecificam as normas constitucionais na esfera digital, criando o potencial transformador do constitucionalismo societal (CELESTE, 2023). Em particular, Celeste salienta como tais declarações, apesar de não serem fontes juridicamente vinculantes, representam um instrumento flexível através do qual os seus promotores são livres para experimentar novas soluções jurídicas de forma gradual e mais democrática, incluindo atores para além dos mundos da política e dos negócios.

Giovanni De Gregorio se concentra no código digital como matriz de normatividade constitucional e aborda-o no quadro geral do constitucionalismo como projeto normativo (DE GREGORIO, 2023). Partindo da observação de que os sistemas de inteligência artificial (IA) criam as suas próprias normas ao definirem camadas geradoras de normatividade na sociedade algorítmica, o autor argumenta que os sistemas automatizados de tomada de decisões autonomamente desenvolvem normas por meio da experiência e da

aprendizagem em um espaço tecnológico opaco que tende a escapar à lógica do Estado de direito. Nesse contexto, ele discute o *Artificial Intelligence Act* proposto pela União Europeia[26] como um exemplo de como o Estado de direito pode limitar a delegação na era digital.

Oren Perez e Nurit Wimer também abordam o impacto constitucional da IA na regulação, mas focam na moderação de conteúdo das plataformas digitais. Os autores examinam o regime de moderação de conteúdo do Facebook, já parcialmente controlado por algoritmos. Partindo de uma crítica das abordagens atuais baseadas na engenharia ética, desenvolvem o "constitucionalismo algorítmico" como uma abordagem original à governança da IA. Demonstram como ele pode ser aplicado ao regime de moderação de conteúdo do Facebook e descrevem a diferença entre constitucionalismo societal e algorítmico. De fato – e paradoxalmente –, a tentativa de submeter o algoritmo de IA a um controle externo abre a porta para que o agente de IA intervenha nesse processo, potencialmente minando o seu próprio objetivo. Por fim, exploram as implicações do seu argumento para o DSA.

A segunda seção trata da política de propriedade de dados e do papel do direito na modelagem da interface entre economia e digitalidade. Dan Wielsch observa que, nos sistemas econômicos contemporâneos, os dados estão ocupando seu lugar ao lado do trabalho e do capital, o que levanta questões sobre a necessidade e a legitimidade da criação de direitos exclusivos sobre dados ou "propriedade de dados" (WIELSCH, 2023). Entretanto, a teoria jurídica não precisa apenas desenvolver um conceito adequado de "dados" e explicar as funções sociais dos direitos de propriedade relacionados. Ela também precisa alinhar uma possível propriedade de dados com a ideia mais ampla de ordenação social *por meio de* direitos de propriedade, levando em consideração a normatividade das ordens sociais constituídas por meio do exercício de direitos e garantindo que aqueles afetados por essas ordens possam participar de sua

[26] Proposta de Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e Altera Determinados Atos Legislativos da União, Com/2021/206 Final.

formação. Com relação à função dos direitos individuais para a prática social – ele argumenta –, surgem duas outras questões: as implicações da normatividade dessa prática para os direitos e, de forma correspondente, a participação dos titulares de direitos na prática social. Em última análise, e na medida em que os direitos privados permitiriam a mudança das regras da ordem social, eles se tornam direitos políticos.

Irina Domurath trata da criação de perfis algorítmicos como um exemplo de dataficação e colonização pelas máquinas. Ela examina o surgimento de uma constituição digital da UE a partir da perspectiva do constitucionalismo societal (DOMURATH, 2023). Por meio de uma crítica interna do constitucionalismo societal, ela questiona suas suposições sobre a capacidade dos atores societais e dos meios de comunicação não jurídicos, como a revolta e a litigância públicas, de exercer a pressão necessária para mudanças de dentro para fora. A autora recorre aos conhecimentos dos emergentes estudos da "*Law and Political Economy*" (LPE) (ver PISTOR, 2019, p. 183-204; KAPCZYNSKI, 2020) para entender o poder estrutural de empresas que inibem o aumento da pressão externa e para justificar a adoção de um contraconceito de vulnerabilidade digital estrutural.

Os estudos da LPE são um ponto de referência também para Roxana Vatanparast, que aborda ainda outro lado da relação entre as tecnologias digitais e a economia: a moeda digital (VATANPARAST, 2023). Concentrando-se em sua governança e seu potencial democrático, ela explora as oportunidades oferecidas pelo pluralismo da moeda digital e pela governança policêntrica para incorporar valores que, de outra forma, poderiam não ser valorizados nas sociedades de mercado. Em particular, ela faz referência a dois estudos de caso, a saber, a moeda digital criada por e para comunidades apátridas utilizando a tecnologia *blockchain*; e a moeda fiduciária digital que tem os atributos de preservação da privacidade do dinheiro e promove a inclusão financeira. Ela argumenta que o pluralismo das moedas digitais que utilizam arquiteturas institucionais públicas e sem fins lucrativos tem um potencial democrático maior do que as formas de moeda digital impulsionadas por fins lucrativos e extrativistas.

As contribuições da terceira seção exploram diferentes maneiras de reformular as instituições fundamentais do constitucionalismo (direitos, democracia, separação de poderes, procedimentos) na esfera digital. Usando a neutralidade da rede como um estudo de caso, Christoph Graber argumenta a favor de uma reconstrução dos direitos fundamentais como instituições. Eles devem incluir expectativas normativas relacionadas não apenas à proteção de posições individuais, mas também à defesa de autonomias institucionais contra as tendências autodestrutivas da sociedade (GRABER, 2023). A partir das garantias *legais* existentes de neutralidade da rede em determinadas jurisdições, ele defende o desenvolvimento de estruturas e processos *constitucionais* – a próxima etapa a ser esperada de acordo com a teoria do constitucionalismo societal. De uma perspectiva normativa, ele explora como a proteção da neutralidade da rede deve ser institucionalizada como um direito fundamental. Em particular, ele argumenta que duas questões preliminares precisam ser abordadas: primeiro, como conceituar adequadamente a relação entre o social e o tecnológico; segundo, como os direitos fundamentais devem ser concebidos para além do estadocentrismo. Ele conclui que uma reflexão sociológica dos direitos fundamentais como instituições da sociedade servirá como referência para a avaliação de futuros desenvolvimentos da doutrina jurídica constitucional.

Monika Zalnieriute segue um caminho diferente. Recorrendo aos estudos críticos e decoloniais, ela questiona as soluções procedimentalistas frequentemente oferecidas no campo do constitucionalismo digital. Ela critica o que chama de "fetichismo procedimental" (*procedural fetishism*) como uma estratégia do imperialismo digital para ocultar e reforçar o domínio dos EUA, a exploração colonial e a degradação ambiental (ZALNIERIUTE, 2023). Uma nova constituição digital – ela argumenta – teria que mudar seu foco de iniciativas procedimentais e de *soft law* para a responsabilidade substantiva e obrigações legais concretas das empresas de tecnologia. De forma ainda mais urgente, o constitucionalismo digital precisa reconhecer as práticas coloniais de extração e exploração, atentando-se às vozes das comunidades indígenas do "Sul Global".

Somente com esses esforços que se reforçam mutuamente é que uma nova constituição digital desmascarará as agendas corporativas e estatais de fetichismo procedimental e estabelecerá um novo contrato social para a era digital.

Raffaela Kunz aborda essas questões de uma outra perspectiva (KUNZ, 2023). Focando no *Open Science* como um estudo de caso, ela observa como a conscientização sobre os lados obscuros das tecnologias digitais tem aumentado nos últimos anos. Já faz tempo que as principais editoras acadêmicas começaram a entrar no negócio de análise de dados (*data analytics*), gerando consequências negativas para a consolidação de um oligopólio no setor de publicações acadêmicas e ampla influência das empresas sobre a ciência. Nesse contexto, ela argumenta que o constitucionalismo tradicional não é capaz de capturar os riscos sutis, embora sistêmicos, que a ciência enfrenta na era digital. O constitucionalismo societal não apenas serve como uma lente analítica útil, mas também ajuda a responder a essas ameaças. Ele fornece lições valiosas para debates sobre o constitucionalismo digital e a proteção efetiva dos direitos fundamentais na era digital.

A quarta e última seção examina a interface entre as tecnologias digitais e a adjudicação judicial, tanto na esfera privada quanto na pública. Tania Sourdin explora o impacto problemático da IA sobre as funções judiciais dos Estados (SOURDIN, 2023). Ela observa como as emergentes relações entre juízes, tribunais e tecnologias de IA desafiam a teoria de governança convencional, na medida em que exigem o foco na interação social para explorar como a capacidade de resposta judicial pode apoiar o desenvolvimento de abordagens éticas que cuidem de populações vulneráveis. A autora argumenta que o constitucionalismo social abre uma nova abordagem para a justiça, que promova o bem-estar humano, o que, por sua vez, dá suporte a tecnologias disruptivas no âmbito da justiça. Ela também reflete sobre os desafios apresentados por essa abordagem, imediatamente aparentes nas concepções de justiça que se concentram na prestação de justiça "rápida" e de "baixo custo", na ausência da própria justiça.

Na contribuição final, Angelo Jr Golia se concentra no *Oversight Board* (OB), o órgão adjudicativo independente criado pela Meta para tomar decisões consequentes de moderação de conteúdo que estabeleçam precedentes no Facebook e no Instagram. Ele propõe uma possível estratégia para fazer com que as plataformas digitais respondam às demandas externas relativas ao seu impacto social mais amplo (GOLIA, 2023). Começando com uma análise do sistema normativo da Meta a partir da perspectiva do constitucionalismo social, ele avalia a real extensão da juridificação e da constitucionalização. Com o objetivo de colocar o capitalismo informacional/vigilância "no banco dos réus", ele então delineia uma estratégia de litigância referente aos problemas de saúde mental dos jovens e, desse modo, acaba usando o sistema normativo da Meta para tematizar efeitos sistêmicos mais amplos das redes sociais em termos constitucionais.

V. Fios condutores: questões de definição, materialidade e conflito, abordagens regulatórias, teoria dos sistemas

Uma das tarefas mais importantes e desafiadoras do constitucionalismo digital é tornar visível a convergência de diferentes vertentes acadêmicas que lidam com o impacto das tecnologias digitais sobre os direitos fundamentais, a democracia e o Estado de direito. Essa convergência é possível especialmente com as abordagens que não falam – pelo menos, não explicitamente – a linguagem do constitucionalismo. Isso abre debates mais amplos, tanto dentro quanto fora dos estudos constitucionais. Nesse contexto, nesta seção final, destacamos alguns fios condutores e os vinculamos a debates paralelos. Em particular, quatro fios condutores estão surgindo, relacionados a questões de definição, materialidade e conflito digitais, abordagens regulatórias e teoria dos sistemas.

Um primeiro fio condutor diz respeito à identidade do constitucionalismo digital. De fato, sua complexidade interna está bem refletida em sua própria (falta de consenso sobre sua) definição (para uma visão geral das questões de definição, ver CELESTE, 2019). As contribuições para este simpósio revelam uma variedade

de sentidos e orientações normativas na definição de "constituição digital" e "constitucionalismo digital" (ver especialmente as contribuições de De Gregorio (2023), Zalnieriute (2023) e Perez e Wimer (2023)). Em contraste com a crítica apressada (COSTELLO, 2023; PEREIRA; KELLER, 2022), essas nuances – essa ambiguidade interna, se se preferir – não são necessariamente negativas. Tampouco se trata de um instrumento para cooptar o capital simbólico do constitucionalismo. Em vez disso, ela permite que vários discursos com uma perspectiva normativa compartilhada coexistam, interajam e potencialmente compensem os limites uns dos outros. Essa variedade interna também facilita os engajamentos críticos e contribui para desmascarar as tentativas de cooptação.[27] O que importa é a ambição compartilhada de criar instrumentos jurídicos que protejam *e* restrinjam a dinâmica do código digital em sua relação com o poder, o dinheiro, a fé e a autoridade jurídica. Colocando em termos mais usuais: o objetivo é a tradução e a implementação de princípios constitucionais em diferentes campos sociais recém-surgidos. Entretanto, o horizonte normativo de qualquer constitucionalismo, seja ele estadocêntrico, global ou societal, define o projeto (ver DUARTE *et al.*, no prelo).

O projeto pode ser visto tanto como uma conceitualmente ambiciosa "constituição digital" quanto como um mais modesto "constitucionalismo para o digital". Um envolvimento sério com as tecnologias digitais pressupõe levar-se em conta uma pluralidade de normatividades, as quais, de forma variável, interagem, sobrepõem-se, entram em conflito e influenciam umas às outras. Somente dentro desse processo *poderá* uma "constituição digital" surgir. Mas – e isto é importante – esse surgimento é contingente e de forma alguma necessário. Ele deve ser ativamente buscado por diferentes atores estratégicos, incluindo acadêmicos engajados. Qualquer conceito de constitucionalismo digital transformativo terá como objetivo estabelecer as precondições analíticas e normativas para esse surgimento.

[27] Cf. ZALNIERIUTE, 2023; e, de forma mais geral, GOLIA, 2021. Na mesma direção, com observações precisas em relação ao DSA da UE, ver MARONI, no prelo.

Há um segundo fio condutor: materialidade e conflito (digitais). Com efeito, pensar a digitalidade pelas lentes do constitucionalismo societal permite o estabelecimento de vínculos com as precondições materiais da constituição digital, em dois sentidos. Primeiro, o substrato sociotécnico das tecnologias digitais influencia seus efeitos constritivos, as possibilidades reais de transformação e a contestação de normas e soluções de políticas públicas. Assim, a tecnologia facilita e também dificulta o surgimento de normas constitucionais (GRABER, 2023; ver também GRABER, 2021). Em segundo lugar, o constitucionalismo societal exige que se observem as relações socioeconômicas concretas – efetivamente materiais – sustentadas pela infraestrutura jurídica do ecossistema digital. Processos de extração de valor amplificados pela digitalidade, efeitos redistributivos em níveis nacionais e globais, a capacidade da política, da ciência e do direito como campos sociais distintos de resistir à colonização pela racionalidade econômica – todos esses são pontos de contato com os estudos da LPE, como mostram várias das contribuições deste número do simpósio (ver, em especial, VATANPARAST, 2023; WIELSCH, 2023; DOMURATH, 2023; KUNZ, 2023. Para uma excelente contribuição que vincula a LPE e o constitucionalismo societal, ver KAMPOURAKIS, 2021). Conforme mencionado acima, combater os efeitos negativos da fusão entre um "setor público" dirigido pelo poder digitalizado e um "setor privado" dirigido pelo lucro digitalizado – o que chamamos de nova "economia política digital" – deve ser uma das metas transformativas de um direito digital baseado no constitucionalismo social.

Aqui, afirmamos que a contribuição específica do constitucionalismo societal está na policontexturalidade como um de seus pontos de partida analíticos (ver GÜNTHER, 1976). De fato, contra o risco de se concentrar exclusivamente na interface economia/política, o constitucionalismo societal insiste na multiplicidade de perspectivas sociais mutuamente irredutíveis reproduzidas pela digitalidade e suas colisões. Em termos normativos, isso exige abordagens refinadas que levem em conta a dinâmica específica dos diferentes sistemas sociais – entre eles, o direito, a ciência, a religião –, de forma a orientar

as soluções normativas e políticas para a reflexividade *específica* de cada campo social (ver, em especial, KUNZ, 2023; GRABER, 2023. Para uma aplicação recente de abordagens de direito reflexivo a criptomoedas, ver MOTSI-OMOIJIADE, 2022).

Isso nos leva a um terceiro fio condutor, a saber, a contribuição ao campo acadêmico da regulação (para uma significativa contribuição para esse debate, ver TÖRNBERG, 2023). Este simpósio ajuda a dissipar algumas caracterizações equivocadas do constitucionalismo societal (GÜNTHER, 2020; GOLDMANN, 2016; BOGDANDY; DELLAVALLE, 2013). É plenamente incorreto dizer que o constitucionalismo societal se concentra apenas no ordenamento privado para o surgimento da normatividade constitucional. Da mesma forma, é errado afirmar que ele é inspirado por uma ideologia neoliberal que legitima poderes privados e apoia exclusivamente a autorregulação privada e a retração da regulação estatal. Em contraste, o constitucionalismo societal demanda a inclusão de normatividades provenientes de todos os campos sociais, *incluindo* a política baseada no Estado (cf. GOLIA; TEUBNER, 2021, p. 388). É importante ressaltar que isso não significa necessariamente "menos governo". Em vez disso, mesmo a regulação estatal, se orientada para a *efetiva* constitucionalização, deve ser traduzida em *auto*constitucionalização. A fim de desempenhar suas funções constitutivas e limitativas, as constituições digitais precisam responder às estruturas/processos comunicativos específicos da digitalidade. De forma mais concreta, as regras jurídico-políticas precisam ser reconstruídas pelo código digital. Em outras palavras, as estratégias regulatórias que visam a uma efetiva constitucionalização da esfera digital podem exigir mais ou menos regulação estatal. No entanto, essa constitucionalização não pode se basear exclusivamente em normas politicamente legitimadas, mesmo quando elas derivam de processos deliberativos autênticos. Ao final das contas, o constitucionalismo social pede uma interação estratégica de tipos de normas qualitativamente diferentes (cf. GOLIA; TEUBNER, 2021, p. 388-395), conforme afetadas pelo código digital (cf. CELESTE, 2023; DE GREGORIO, 2023; PEREZ; WIMER, 2023; GOLIA, 2023). A partir dessa perspectiva, não surpreende o fato de que vários dos colaboradores

– adotando percepções provenientes do constitucionalismo societal – tenham defendido um papel mais significativo para os Estados, desde a expansão de suas obrigações positivas (cf. KUNZ, 2023) até o estabelecimento de proibições mais claras e "rígidas" (cf. DE GREGORIO, 2023; ZALNIERIUTE, 2023). Da mesma forma, a problematização do Estado de direito – um princípio clássico do constitucionalismo moderno –, formulada por várias das contribuições a este simpósio (cf. DE GREGORIO, 2023; ZALNIERIUTE, 2023; PEREZ; WIMER, 2023), e as estratégias para sua reespecificação em diferentes contextos são outro exemplo de como o constitucionalismo societal contribui para combinar distintas normatividades, princípios de legitimidade e abordagens regulatórias. Conforme mencionado acima, os efeitos normativos decorrentes de tecnologias digitais e dos algoritmos precisam ser reconciliados com o Estado de direito de uma maneira diferente daquela que ocorreu no constitucionalismo "analógico" (ver, em especial, PEREZ; WIMER, 2023). Em termos positivos, tais contribuições mostram a importância de se buscar soluções que vinculem os efeitos coercitivos da tecnologia (COHEN, 2012, cap. 10) com as estruturas e processos normativos específicos do direito (nessa direção, ver GRABER, 2021; HILDEBRANDT, 2020; VESTING, 2018, com foco nos aspectos culturais e de mídia da normatividade do código) e suas características humanas.[28]

O quarto e último foi condutor derivado deste simpósio diz respeito à relação com a teoria dos sistemas. A teoria dos sistemas fornece uma estrutura analítica adequada para uma constituição digital (cf., para os termos desse debate, BAECKER, 2020)? O constitucionalismo social – conforme desenvolvido nas duas últimas décadas – baseia-se na teoria dos sistemas sociais de Luhmann e, ao mesmo tempo, pensa nos termos normativos do constitucionalismo. Algumas das contribuições deste simpósio mostram que a teoria da diferenciação funcional de Luhmann abre novas perspectivas para uma reconstrução transformativa da digitalidade (ver KUNZ, 2023; GRABER, 2023). Tais

[28] Na literatura mais recente, cf. TASIOULAS, 2023; CATANNZARITI, 2022, enfatizando o papel dos profissionais jurídicos humanos nas burocracias públicas. Esses aspectos são perdidos, por exemplo, em abordagens voltadas para a eficiência, como COGLIANESE; LAI, 2022.

contribuições revelam um outro aspecto da teoria dos sistemas que tematiza os riscos da dataficação (ver, em especial, DOMURATH, 2023; KUNZ, 2023; GRABER, 2023). Aqui, uma questão em aberto é se a teoria constitucional deveria se concentrar apenas nos efeitos que a dataficação tem sobre os meios de comunicação já existentes (ver nota 2 *supra*) ou no efeito que tem sobre o próprio código digital, como um *novo* meio de comunicação. Essa é a perspectiva do "constitucionalismo por etapas", que identifica os processos constitucionais na própria arquitetura digital (SHEFFI, no prelo). De uma perspectiva mais especulativa, este simpósio convoca a pesquisa sociojurídica a investigar se o impacto da digitalização é tão significativo que irá desencadear um afastamento da diferenciação funcional como a principal forma de organização social.[29] Em outras palavras, processos sociais orientados por dados, como a ressocialização do poder – a capacidade de atores coletivos não políticos e não estatais de aumentar a probabilidade de aceitação de Alter como premissa das ações de Ego – podem chegar ao ponto de provocar o surgimento de formas novas e sem precedentes de diferenciação social.[30] Essas perguntas certamente não podem ser respondidas apenas pela teoria constitucional. Entretanto, essa ampliação do horizonte é necessária para qualquer constitucionalismo que pretenda atingir o nível de complexidade exigido pelas questões envolvidas e, potencialmente, oferecer soluções normativas para uma constituição digital. Talvez este simpósio contribua para esse debate.

Referências

ASPESI, Claudio, *et al.* SPARC Landscape Analysis: the changing academic publishing industry – implications for academic institutions. **LIS Scholarship Archive**, 29 de mar. de 2019. Disponível em: https://osf.io/preprints/lissa/58yhb.

[29] O que substituiu a segmentação e a estratificação nas sociedades modernas: ver BARALDI *et al.*, 2021, p. 65-70.

[30] Por exemplo, as ideias de Dirk Baecker sobre a próxima sociedade: ver BAECKER, 2014; BAECKER, 2007.

BACKER, Larry Catá. And an algorithm to entangle them all? *In:* KRISCH, Nico (ed.). **Entangled legalities beyond the state.** New York: Cambridge University Press, p. 79-106, 2021.

BAECKER, Dirk. The network synthesis of social action I: towards a sociological theory of next society. **Cybernetics & Human Knowing**, v. 14, p. 9-42, 2007.

BAECKER, Dirk. Layers, flows, and switches: individuals in next society. *In:* GEISSLER, Beate *et al.* (eds.). **Volatile Smile.** Nürnberg: Verlag für modern Kunst, p. 90-97, 2014.

BAECKER, Dirk. **Digitization as calculus:** a prospect. 2020. Disponível em: https://www.researchgate.net/publication/344263318_Digitization_as_Calculus_A_Prospect.

BALDWIN, Jon. 'Self-immolation by technology': Jean Braudillard and the posthuman in film and television. In: HAUSKELLER, Michael *et al.* (eds.). **The Palgrave handbook of Posthumanism in film and television.** London: Palgrave Macmillan, p. 19-27, 2015.

BARALDI, Claudio *et al.* **Unlocking Luhmann:** a keyword introduction to systems theory. Bielefeld: Bielefeld University Press, p. 175, 2021.

BASSINI, Marco. Fundamental rights and private enforcement in the digital age. **European Law Journal**, v. 25, n. 2, p. 182-197, 2018.

BASTIAN, Mariella *et al.* Safeguarding the journalistic DNA: attitudes towards the role of professional values in algorithmic news recommender designs. **Digital Journalism**, v. 9, n. 6, p. 835-863, 2021.

BLOCH-WEHBA, Hannah. Algorithmic governance from the bottom up. **Brigham Young University Law Review**, v. 48, n. 1, p. 69-136, 2022.

BOGDANDY, Armin von; DELLAVALLE, Sergio. The lex mercatoria of systems theory: localisation, reconstruction and criticism from a public law perspective. **Transnational Legal Theory**, v. 4, n. 1, p. 59-82, 2013.

BOROWSKA, Kasia. The monopoly on technology and how to defeat it. **Forbes**, 15 de dez. de 2020. Disponível em: https://www.forbes.com/sites/kasiaborowska/2020/12/15/the-monopoly-on-technology-and-how-to-defeat-it/?sh=55d48b521af7.

BRAYNE, Sarah. Big Data surveillance: the case of policing. **American Sociological Review**, v. 82, n. 5, p. 977-1008, 2017.

BURRELL, Jenna; FOURCADE, Marion. The society of algorithms. **Annual Review of Sociology**, v. 47, n. 1, p. 213-237, 2021.

BYGRAVE, Lee A. **Internet governance by contract**. Oxford: Oxford University Press, p. 85-103, 2015.

CARA, Corina. Dark patterns in the media: a systematic review. **Network Intelligence Studies**, v. 7, n. 14, p. 105-113, 2019.

CASTETS-RENARD, Céline. Human rights and algorithmic impact assessment for predictive policing. *In:* MICKLITZ, Hans-W. *et al.* **Constitutional challenges in the algorithmic society.** Cambridge: Cambridge University Press, p. 93-110, 2022.

CATANZARITI, Mariavittoria. Algorithmic law: law production by data or data production by law? *In:* MICKLITZ, Hans-W. *et al.* **Constitutional challenges in the algorithmic society.** Cambridge: Cambridge University Press, p. 78-92, 2022.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorization. **International Review of Law, Computers & Technology**, v. 33, n. 1, p. 76-99, 2019.

CELESTE, Edoardo. **Digital constitutionalism:** the role of internet bills of rights. New York: Routledge, 2022.

CELESTE, Edoardo. Internet bills of rights: generalization and re-especification towards a digital constitution. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 25-54, 2023.

CHRISTODOULIDIS, Emilios A. **The redress of law:** globalisation, constitutionalism and market capture. Cambridge: Cambridge University Press, cap. 4.2, 2021.

COFONE, Ignacio. Beyond data ownership. **Cardozo Law Review**, v. 43, n. 2, p. 501-573, 2021.

COGLIANESE, Cary; LAI, Alicia. Algorithm v. algorithm. **Duke Law Journal**, v. 71, p. 1281-1340, 2022.

COHEN, Julie E. **Configuring the networked self:** law, code, and the play of everyday practice. New Haven: Yale University Press, cap. 1, 2012.

COHEN, Julie E. **Between truth and power:** the legal constructions of informational capitalism. Oxford: Oxford University Press, 2019.

COSTELLO, Róisín Á. Faux ami? Interrogating the normative coherence of 'digital constitutionalism', **Global Constitutionalism**, v. 12, n. 2, p. 326-249, 2023.

DE GREGORIO, Giovanni. **Digital Constitutionalism in Europe:** reframing rights and powers in the algorithmic society. Cambridge: Cambridge University Press, 2022.

DE GREGORIO, Giovanni. The normative power of artificial intelligence. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 55-80, 2023.

DIVER, Laurence. Digisprudence: the design of legitimate code. **Law, Innovation & Technology**, v. 13, n. 2, p. 325-354, 2021.

DOMURATH, Irina. Rage against the machine: profiling and power inn the data economy. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 131-164, 2023.

DUARTE, Francisco De Abreu Duarte *et al.* **Perspectives on digital constitutionalism.** No prelo.

EL-FATTAH, Alaa Abd. Keynote speech to Rightscon 2011. *In:* EL-FATTAH, Alaa Abd. **You have not yet been defeated.** London: Fitzcarraldo, p. 76-82, 2021).

GILL, Lex *et al.* Towards digital constitutionalism? Mapping attempts to craft an internet bill of rights. **The International Communication Gazette**, v. 80, p. 302, 2018.

GOLDMANN, Matthias. A matter of perspective: global governance and the distinction between public and private authority (and not law). **Global Constitutionalism**, v. 5, p. 48, 2016.

GOLIA, Angelo Jr. **Beyond Oversight: advancing societal constitutionalism in the age of surveillance capitalism.** 2021.

GOLIA, Angelo Jr. The Critique of Digital Constitutionalism. **MPIL Research Paper Series**, n. 2022-13, p. 1-31, 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4145813.

GOLIA, Angelo Jr. The transformative potential of Meta's Oversight Board: strategic litigation within the digital constitution? *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 325-361, 2023.

GOLIA, Angelo Jr; TEUBNER, Gunther. Societal constitutionalism: background, theory, debates. **ICL – Vienna Journal of International Constitutional Law**, v. 15, n. 4, p. 357-411, 2021.

GONZÁLEZ-BAILÓN, Sandra; LELKES, Yphtach. Do social media undermine social cohesion? A critical review. **Social Issues Policy Review**, v. 17, p. 155, 2023.

GRABER, Christoph B. Artificial Intelligence, Affordances and Fundamental Rights. *In:* HILDEBRANDT, Mireille; O'HARA, Kieran (eds.). **Life and the law in the era of data-driven agency.** Cheltenham: Edward Elgar, seção 1, 2020.

GRABER, Christoph B. How the law learns in the digital society. **Law, Technology and Humans**, v. 3, p. 12, 2021.

GRABER, Christoph B. Net neutrality: a fundamental right in the digital constitution? *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 197-226, 2023.

GRADONI, Lorenzo. Constitutional review via Facebook's Oversight Board: how platform governance had its Marbury v Madison. **VerfBlog**, 10 de fev. de 2021. Disponível em: https://verfassungsblog.de/fob-marbury-v-madison/.

GÜNTHER, Gotthard. Life as poly-contexturality. *In:* GÜNTHER, Gotthard (ed.). **Beiträge zur Grundlegung einer operationsfähigen Dialektik.** Hamburg: Meiner, p. 283-306, 1976.

GÜNTHER, Klaus. Normative legal pluralism: a critique. *In:* FABRA-ZAMORA, Jorge L. (ed.). **Jurisprudence in a globalized world.** Cheltenham: Edward Elgar, p. 84-99, 2020.

HAIDAR, Julieta; KEUNE, Marteen (eds.). **Work and labour relations in global platform capitalism.** Cheltenham: Edward Elgar, 2021.

HARTZOG, Woodrow *et al.* Fighting Facebook: A Campaign for a Peoples Terms of Service. **The Nation**, 22 de mai. de 2013. Disponível em: https://www.thenation.com/article/archive/fighting-facebook-campaign-peoples-terms-service/.

HENSEL, Isabell; TEUBNER, Gunther. Horizontal fundamental rights as conflict of law rules: how transnational pharma groups manipulate scientific publications. *In:* BLOME, Kerstin *et al.* (eds.). **Contested regime collisions:** norm fragmentation in world society. Cambridge: Cambridge University Press, p. 139-168, 2016.

HILDEBRANDT, Mireille. Code-driven law: freezing the future and scaling the past. *In:* DEAKIN, Simon; MARKOU, Christopher (eds.). **Is law computable?** Critical perspectives on law and artificial intelligence. Oxford: Bloomsburry Publishing, p. 67-84, 2020.

HOLZNAGEL, Daniel. Enforcing the rule of law in online content moderation: how European high court decisions might invite reinterpretation of CDA § 230. **Business Law Today**, 9 de dez. de 2021. Disponível em: https://businesslawtoday.org/2021/12/rule-of-law-in-online-content-moderation-european-high-court-decisions-reinterpretation-cda-section-230/.

HUMMEL, Patrik *et al.* Own data? Ethical reflections on data ownership. **Philosophy & Technology**, v. 34, p. 545-572, 2021.

JAKOB, Sarah. The corporate social credit system in China and its transnational impact. **Transnational Legal Theory**, v. 12, p. 294-314, 2021.

JOHNS, Fleur. Governance by data. **Annual Review of Law and Social Science**, v. 17, n. 1, p. 53-71, seção 4.1, 2021.

KAMPOURAKIS, Ioannis. Bound by the economic constitution: notes for "Law and Political Economy" in Europe. **Journal of Law and Political Economy**, v. 1, n. 2, p. 301-332, 2021.

KAPCZYNSKI, Amy. The law of informational capitalism. **The Yale Law Journal**, v. 129, p. 1460-1515, 2020.

KETTEMANN, Matthias. **The normative order of the internet:** a theory of rule and regulation online. Oxford: Oxford University Press, 2020.

KJAER, Poul F. **Constitutionalism in the global realm:** a sociological approach. Abingdon: Routledge 2014.

KLONICK, Kate. The new governors: the people, rules, and processes governing online speech. **Harvard Law Review**, v. 131, n. 6, p. 1598-1670, 2018.

KUNZ, Raffaela. Opening access, closing the knowledge gap? **Heidelberg Journal of International Law**, v. 81, n. 1, p. 23-46, 2021.

KUNZ, Raffaela. Threats to academic freedom under the guise of Open Access. **VerfBlog**, 18 de mar. de 2022. Disponível em: https://verfassungsblog.de/threats-to-academic-freedom-under-the-guise-of-open-access/.

KUNZ, Raffaela. Tackling threats to academic freedom beyond the state: the potential of societal constitutionalism in protecting the autonomy of science in the digital era. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 265-292, 2023.

LESSIG, Lawrence. **Code and other laws of cyberspace.** New York: Basic Books, 1999.

LUCKNER, Katharina. #WhoseLawIsItAnyway: how the internet augments civil society participation in international law making. *In:* GOLIA, Angelo Jr *et al.* (eds.). **Digital transformations in public international law.** Baden-Baden: Nomos, p. 235-260, 2022.

MARONI, Marta. 'Mediated transparency': the digital service act and the legitimisation of platform power. *In:* LEINO-SANDBERG, Päivi *et al.* (eds.).

(In)visible European government: critical approaches to transparency as an ideal and a practice. No prelo.

MARKOU, Christopher; DEAKIN, Simon. Is law computable? From the rule of law to legal singularity. *In:* DEAKIN, Simon; MARKOU, Christopher (eds.). **Is law computable?** Critical perspectives on law and artificial intelligence. Oxford: Bloomsburry Publishing, 2020.

MILANOVIC, Nik. We need new business models to burst old media filter bubbles. **TechCrunch**, 28 de out. de 2020. Disponível em: https://techcrunch.com/2020/10/28/we-need-new-business-models-to-burst-old-media-filter-bubbles/.

MIOTTO, Lucas; CHEN, Jiahong. Manipulation, real-time profiling, and their wrongs. *In:* JONGEPIER, Fleur; KLENK, Michael (eds.). **The philosophy of online manipulation.** New York: Routledge, 2022.

MUNK, Jean De. From orthodox to societal constitutionalism. *In:* ROBÉ, Jean-Philippe *et al.* (eds.). **Multinationals and the constitutionalization of the world power system.** Abingdon: Routledge, 2016.

OKIDEGBE, Ngozi. The democratizing potential of algorithms? **Connecticut Law Review**, v. 53, p. 739, 2022.

MOTSI-OMOIJIADE, Immaculate D. **Cryptocurrency regulation:** a reflexive law approach. Abingdon: Routledge, 2022.

PAPADAKIS, Konstantinos; MEXI, Maria. Managing complexity in the platform economy: self-regulation and the cross-border social dialogue route. **Geneva Graduate Institute**, 16 de jun. de 2021. Disponível em: https://www.graduateinstitute.ch/communications/news/managing-complexity-platform-economy-self-regulation-and-cross-border-social.

PEREIRA, Jane Reis Gonçalves; KELLER, Clara Iglesias. Constitucionalismo digital: contradições de um conceito impreciso. **Revista Direito e Práxis**, v. 13, n. 4, p. 2648-2689, 2022.

PEREZ, Oren; WIMER, Nurit. Algorithmic constitutionalism. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative

potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 81-114, 2023.

PETIT, Nicolas. **Big tech and the digital economy:** the moligopoly scenario. Oxford: Oxford University Press, 2020.

PICKARD, Victor. Can journalism survive in the age of platform monopolies? Confronting Facebook's negative externalities. *In:* FLEW, Terry; MARTIN, Fiona R. (eds.). **Digital platform regulation:** global perspectives on internet governance. Cham: Springer Nature, p. 23-42, 2022.

PISTOR, Katharina. **The code of capital:** how the law creates wealth and inequality. Princeton: Princeton University Press, p. 183-204, 2019.

RACHLITZ, Kurt *et al.* Digitale Platformen als soziale Systeme? Vorarbeiten zu einer allgemeinen Theorie. **Soziale Systeme**, v. 26, p. 54-94, 2021.

REICHMAN; Amnon; SARTOR, Giovanni. Algorithms and regulation. *In:* MICKLITZ, Hans-W. *et al.* **Constitutional challenges in the algorithmic society.** Cambridge: Cambridge University Press, p. 131-181, 2022.

SHARMA, Chinmayi. Tragedy of the digital commons. **North Carolina Law Review**, v. 101, p. 1129-1228, 2023. Disponível em: https://ssrn.com/abstract=4245266.

SHEFFI, Nofar. We accept: the constitution of Airbnb. **Transnational Legal Theory**, v. 11, p. 484-520, 2020.

SHEFFI, Nofar. **We accept:** bit-by-bit constitution. No prelo.

SOURDIN, Tania. Robo justice: constitutional issues with judge AI. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 293-324, 2023.

SOW, Amadou Korbinian. On reaching a crime scene ahead of the criminal: dreams of police and technology from the 1970s to today. **German Law Journal**, v. 23, p. 597-624, 2022.

STICHWEH, Rudolf. Systems theory. *In:* BADIE, Bertrand *et al.* (eds.). **International encyclopedia of political science.** Thousand Oaks: Sage Publications, p. 2579-2588, 2011.

STOLTON, Samuel. EU braces for Big Tech's legal backlash against new digital rulebook. **Politico**, 10 de ago. de 2022. Disponível em: https://www.politico.eu/article/eu-brace-legal-assault-against-digital-clampdown/.

STROBEL, Vera. Strategic litigation and international internet law. *In:* GOLIA, Angelo Jr *et al.* (eds.). **Digital transformations in public international law.** Baden-Baden: Nomos, p. 261-284, 2022.

SUZOR, Nicolas. **Lawless:** the secret rules that govern our digital lives. Cambridge: Cambridge University Press, 2019.

TASIOULAS, John. The rule of algorithm and the rule of law. **Vienna Lectures on Legal Philosophy**, 2023.

TEACHOUT, Zephyr. **Break 'em up:** recovering our freedom from big ag, big tech, and big money. New York: Macmillan, 2020.

TISNÉ, Martin; SCHAAKE, Marietje. The data delusion: protecting individual data isn't enough when the harm is collective. **Luminate**, jul. de 2020. Disponível em: https://luminategroup.com/storage/1023/The-Data-Delusion---July-2020.pdf.

TEUBNER, Gunther. Societal constitutionalism: alternatives to state-centered constitutional theory? *In:* JOERGES, Christian *et al.* (eds.). **Transnational governance and constitutionalism.** Portland: Hart Publishing, p. 3-28, 2004.

TEUBNER, Gunther. **Constitutional fragments:** societal constitutionalism and globalization. Oxford: Oxford University Press, 2012.

TEUBNER, Gunther. The constitution of non-monetary surplus values. **Social and Legal Studies**, v. 30, p. 501, 2020.

TÖRNBERG, Petter. How platforms govern: social regulation in digital capitalism. **Big Data & Society**, v. 10, n. 1, 2023.

UNGER, Roberto Mangabeira. Legal analysis as institutional imagination. **Modern Law Review**, v. 59, n. 1, 1996.

VAIDHYANATHAN, Siva. **Antisocial media:** how Facebook disconnects us and undermines democracy. Oxford: Oxford University Press, 2018.

VATANPARAST, Roxana. Digital monetary constitutionalism: the democratic potential of monetary pluralism and polycentric governance. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 165-196, 2023.

VERSCHRAEGEN, Gert. Regulating scientific research: a constitutional moment? **Journal of Law and Society**, v. 45, n. 1, p. 163-184, 2018.

VESTING, Thomas. **Legal theory and the media of law.** Cheltenham: Edward Elgar, 2018.

VESTING, Thomas. **Gentleman, Manager, Homo Digitalis:** der Wandel der Rechtssubjektivität in der Moderne. Weilerswist: Velbrück, 2021.

VILJOEN, Salomé. A relational theory of data governance. **Yale Law Journal**, v. 131, n. 2, p. 573-654, 2021-2022.

WALKER, Neil. **Intimations of Global Law.** Cambridge: Cambridge University Press, 2014.

WANG, Hao. **Algorithmic colonization:** automating love and trust in the age of Big Data. 2022. Tese (Doutorado em Direito) – University of Amsterdam, 2022.

WATT, Horatia Muir. When societal constitutionalism encounters private international law: of pluralism, distribution, and 'chronotopes'. **Journal of Law and Society**, v. 45, n. 1, p. 185-203, 2018.

WIELSCH, Dan. Private law regulation of digital intermediaries. **European Review of Private Law**, v. 27, n. 2, p. 197-220, 2019.

WIELSCH, Dan. Political autonomy in the digital world: from data ownership to digital constitutionalism. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 115-130, 2023.

WIENER, Antje Wiener *et al.* Global constitutionalism: human rights, democracy and the rule of law. **Global Constitutionalism**, v. 1, n. 1, p. 1-15, 2012.

YEUNG, Karen. 'Hypernudge': Big Data as a mode of regulation by design. **Information, Communication & Society**, v. 20, n. 1, p. 118-136, 2017.

ZALNIERIUTE, Monika *et al.* The rule of law and automation of government decision- making. **Modern Law Review**, v. 82, n. 3, p. 425, 2019.

ZALNIERIUTE, Monika. Against procedural fetishism: a call for a new digital constitution. *In:* GOLIA, Angelo Jr; TEUBNER, Gunther (eds.). **Digital constitution:** on the transformative potential of societal constitutionalism. Simpósio: Indiana Journal of Global Legal Studies, v. 30, n. 2, p. 227-264, 2023.

ZUBOFF, Shoshana. **The age of surveillance capitalism:** the fight for a human future at the new frontier of power. London: Public Affairs, 2019.

4. Regulação para o mercado? Reflexões sobre direito e inovação na era das tecnologias disruptivas a partir de aportes schumpeterianos

Marco Antonio Loschiavo Leme de Barros[31]

Julia Tosatto[32]

Introdução

No campo do Direito Econômico, especialmente no que se refere à regulação dos setores, importante questão é encontrar o equilíbrio adequado entre a proteção proporcionada pela regulação e os impactos que essa intervenção pode ter sobre a competitividade econômica. Este dilema é multifacetado, influenciado por diversos aspectos da economia, desde a inovação até a estrutura de mercado e a proteção dos consumidores.[33]

Considerando o desenvolvimento tecnológico envolvido nos setores, a regulação de serviços e produtos inovadores enfrenta o problema da rápida evolução tecnológica, que frequentemente supera a capacidade das autoridades de desenvolver e atualizar leis em tempo hábil. Esse descompasso cria lacunas,

[31] Professor da Faculdade de Direito da Universidade Presbiteriana Mackenzie e da Pontifícia Universidade Católica de São Paulo. Doutor em direito pela Universidade de São Paulo com apoio da FAPESP. Mestre em Direito e Desenvolvimento pela Fundação Getúlio Vargas de São Paulo. Realizou estágio de pós-dourado em Economia Política Internacional pela Universidade de São Paulo, com apoio da CAPES. Foi visiting researcher no Instituo Internacional de Sociologia Jurídica de Oñati (Espanha) e fez estágio doutoral "sanduíche" na Faculdade de Direito da Universidade da Califórnia em Los Angeles (EUA). É coordenador no grupo de pesquisa Direito & Regulação da Sociedade, cadastrado no diretório do CNPq.

[32] Advogada e mestranda em Direito Político e Econômico na Universidade Presbiteriana Mackenzie. Possui pós-graduação em Compliance Digital pela mesma universidade. É membro do "Grupo de Pesquisa Estado e Economia" vinculado ao Programa de Pós-Graduação da Universidade Presbiteriana Mackenzie.

[33] Nas últimas décadas, inovações surgiram e cresceram, permitindo que indivíduos compartilhassem interesses comuns, ganhassem produtividade e se beneficiassem do uso da tecnologia em indústrias importantes como a medicina. Com sua presença difundida e intrínseca na vida das pessoas, influenciam significativamente a psicologia e a identidade de seus usuários, transformando a maneira como pensam, agem e interagem, impactando profundamente a sociedade (Fisher, 2023).

permitindo que novos modelos de negócios operem sem a devida regulamentação. Como resultado, surgem questões críticas de responsabilidade e segurança, exigindo uma abordagem mais ágil e adaptativa por parte dos reguladores.

Excessiva regulação pode criar barreiras à entrada para novos competidores, protegendo as empresas incumbentes e reduzindo a competitividade do mercado. Do outro lado, mercados competitivos e menos regulados incentivam as empresas a inovarem e melhorar a eficiência para se destacar. Isso pode resultar em melhores produtos e serviços a preços mais baixos para os consumidores e avanço tecnológico.

No Brasil, alguns casos de sucessos em mercados regulados podem ser apontados sobre o equilíbrio entre regulação e inovação. No setor financeiro a história do Pix, sistema de pagamentos instantâneos desenvolvido pelo Banco Central,[34] é exemplo de como a inovação, quando bem regulada, pode transformar um setor inteiro e beneficiar milhões de pessoas. Desde sua concepção até sua implementação e crescimento contínuo, estabelecendo um novo padrão de conveniência, acessibilidade e eficiência financeira. O sucesso do Pix é em grande parte atribuído à regulação eficiente do Banco Central, que estabeleceu diretrizes claras para as instituições financeiras participantes e também atendeu os interesses do setor – rivalizando com as Big Techs.[35]

[34] A ideia do Pix surgiu da necessidade de modernizar o sistema de pagamentos no Brasil, tornando-o mais ágil, eficiente e inclusivo. O Banco Central começou a estudar e planejar um sistema de pagamentos instantâneos em 2018, inspirado em iniciativas similares de outros países. O objetivo era criar uma solução que permitisse a transferência de fundos em tempo real, com baixo custo para os usuários. Além disso, o Pix buscava promover a inclusão financeira, permitindo que pessoas sem conta bancária tradicional ou com acesso limitado a serviços financeiros pudessem realizar transações de maneira simples e acessível (Duarte et al., 2022).

[35] Numa perspectiva política e institucional, importante conclusão: "our account takes a political approach to understand the development of PIX, underscoring the complementarity of three factors. First, the BCB's historically constructed institutional preference for preserving its regulatory perimeter and power. Second, the ideas about states' roles in instant payment systems, especially in the face of Big-techs, formulated and shared through transnational regulatory networks. Third, the non-opposition of the largest banks in Brazil, whose interests have not been severely affected. By examining these factors, the article describes PIX as a political-institutional construct, highlighting the critical role of states in the architecture of digital financialization. It also clarifies that the state's role in digital finance is context-specific, which may vary according to local politicaleconomic issues" (Schapiro et al., 2023, p. 890).

A regulação focou em segurança,[36] interoperabilidade e inclusão, garantindo que o sistema fosse seguro para os usuários e acessível para a maioria da população. A regulação também promoveu a competitividade no setor financeiro. O Pix reduziu a dependência de intermediários tradicionais e permitiu que *fintechs* e outras empresas de tecnologia financeira entrassem no mercado de pagamentos, aumentando a concorrência e beneficiando os consumidores com melhores serviços e tarifas mais baixas.

Para alguns autores (Duarte et al., 2022), esta regulação também produziu importantes impactos sociais como a inclusão financeira, permitindo que pessoas sem acesso a serviços bancários tradicionais realizassem transações de maneira fácil e gratuita. Da mesma forma, o sistema instantâneo impulsionou a digitalização da economia, reduzindo a dependência do dinheiro em espécie e aumentando a transparência nas transações financeiras.

Embora o advento de tecnologias inovadoras tenha inegavelmente trazido benefícios significativos, como maior conectividade e eficiência, também introduziu desafios complexos especialmente no âmbito regulatório. No caso do Pix, a rapidez das transações e a facilidade de uso exigem que as instituições financeiras mantenham vigilância constante para evitar fraudes e garantir a segurança dos usuários – destaque para as questões relativas à proteção de dados pessoais. Além disso, a adaptação de comerciantes e consumidores a um novo sistema de pagamento também é um processo contínuo que requer educação e suporte das autoridades. Tais situações exigem novas formas de compliance e adequações legais por parte dos entes reguladores. Como compreender estar novas formas de comportamento da atividade reguladora diante do desafio de promover inovação em setores fortemente regulados?

De maneira exploratória, este texto promove um debate a partir da ideia de regulação para o mercado. De maneira homóloga à ideia de concorrência pelo mercado (*competition for the market*), que se refere à disputa entre empresas para

[36] Uma das principais preocupações foi a segurança das transações. O Banco Central implementou diversas camadas de segurança para proteger os dados dos usuários e prevenir fraudes. As instituições financeiras foram obrigadas a aderir a padrões rigorosos de segurança, o que ajudou a construir a confiança no sistema (Duarte et al., 2022).

se tornarem o fornecedor exclusivo de um determinado bem ou serviço, em vez de competirem por uma participação de mercado (*competition in the market*), a regulação pelo mercado está focada na implementação de novas abordagens regulatórias em setores caracterizados por grandes economias de escala e alta dependência de investimentos em novas tecnologias.

Essas abordagens buscam promover um ambiente competitivo em setores regulados, incentivando a inovação e garantindo que novos entrantes possam desafiar incumbentes estabelecidos, mantendo a dinâmica do mercado ativa e benéfica para os consumidores. Este conceito é particularmente relevante em mercados digitais e de alta tecnologia, onde características como efeitos de rede, economias de escala e altos custos fixos de entrada podem levar a uma situação em que um ou poucos jogadores dominam o mercado.

Uma importante base teórica que possibilita compreender a regulação econômica a partir da questão da inovação é a obra de Joseph Schumpeter, que oferece fundamentos para entender como a inovação impulsiona o crescimento econômico e como a regulação pode influenciar esse processo. Em uma leitura schumpeteriana, reguladores podem criar um ambiente favorável à inovação ao reduzir barreiras à entrada, proteger a propriedade intelectual e fornecer incentivos para pesquisa e desenvolvimento.

Para explorar essa relação, o capítulo é dividido em três partes. Primeira parte, os conceitos e teorias de Joseph Schumpeter são abordados, destacando como a inovação e a destruição criativa desempenham papéis cruciais no avanço tecnológico e no crescimento econômico. Em seguida, é apresentada uma análise da dificuldade regulatória de serviços e produtos inovadores - evidenciando os desafios de equilibrar a promoção da inovação com a necessidade de regulamentação adequada. Na última parte, para ilustrar a ideia de regulação para o mercado, discutem-se casos de aplicação de *sandboxes* regulatórios no Brasil – instrumentos que permitem a experimentação controlada de inovações sob supervisão. No final, o texto explora como os princípios schumpeterianos podem informar práticas regulatórias que incentivem a inovação e promovam o desenvolvimento econômico sustentável.

1. Inovação, Schumpeter e o avanço tecnológico

Há diversos conceitos de inovação. Vale mencionar a Lei n. 10.973/2004[37], que visa incentivar tal conceito, por exemplo, o caracteriza como o artigo 2º, IV[38] ou a importante Lei n. 9.279/1996 que estabelece as bases da propriedade industrial considerando a inventividade.[39]

Entretanto, o presente artigo encontra nas teorias de Schumpeter uma base sólida para entender a dinâmica da inovação. O autor é conhecido por introduzir conceitos que o distinguiam dos economistas neoclássicos, sendo um destes, o destaque dado ao dinamismo e à inovação. Em sua obra "Teoria do Desenvolvimento Econômico", é destacado o papel crucial do empresário inovador, cuja função é fundamental para o desenvolvimento econômico ao superar riscos e resistências a fim de criar produções. como um motor essencial do progresso (Balbino et. al., 2020).

Para o autor, o desenvolvimento econômico, em sua essência, é impulsionado pela criatividade e inovação dos produtores. Estes agentes, ao introduzirem novas combinações de meios produtivos, alteram o curso da economia, desafiando a visão tradicional de que o desenvolvimento é meramente resultado do acúmulo de capital e força de trabalho (Schumpeter, 1934). Estas novas combinações englobam a introdução de novos bens, métodos de produção, mercados e formas de organização industrial. Isto, por sua vez, demonstra como a esfera da produção, e não do consumo, é o motor propulsor da econômica, uma vez que "é o produtor que, via de regra, inicia a mudança econômica, e os consumidores são educados por ele" (Schumpeter, 1934, p. 76).

---

[37] BRASIL. Lei nº 10.973, de 2 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm. Acesso em: 08 jun. 2024.

[38] Art. 2º, IV, da Lei n. 10.973/2004: introdução de novidade ou aperfeiçoamento no ambiente produtivo e social que resulte em novos produtos, serviços ou processos ou que compreenda a agregação de novas funcionalidades ou características a produto, serviço ou processo já existente que possa resultar em melhorias e em efetivo ganho de qualidade ou desempenho.

[39] Art. 8º, da Lei n. 9.279/1996: É patenteável a invenção que atenda aos requisitos de novidade, atividade inventiva e aplicação industrial.

A figura do empreendedor emerge como central nesse processo. Não se trata de meros gerentes ou tomadores de risco, mas de indivíduos que realizam novas combinações, impulsionando a inovação e a mudança (Schumpeter, 1934). Tal função transcende a simples administração de negócios, focando na criação de algo novo, seja um produto, processo ou mercado. Essa distinção é fundamental para compreender o papel do empreendedor no desenvolvimento econômico, diferenciando-o de outras figuras como o capitalista, independentemente de sua relação com o capital (*ibidem*). A teoria schumpeteriana, ao enfatizar a inovação e a ruptura com o equilíbrio existente, oferece uma perspectiva inovadora sobre o empreendedor, destacando sua importância como agente de mudança e impulsionador do progresso.

No panorama atual, é possível encontrar diversos exemplos da referida teoria em empresários, em sua grande parte do Vale do Silício, cultuados como figuras míticas do desenvolvimento econômico. Steve Jobs, por exemplo, é conhecido por introduzir produtos revolucionários como o iPhone, iPad e o iPod, além de transformar o mercado de computadores pessoais com o Macintosh. Jeff Bezos, por sua vez, é visto como um revolucionário do comércio eletrônico e da logística com a Amazon, criando um ecossistema que mudou o hábito de compra e de consumo. Reed Hastings, através da Netflix, é reconhecido por transformar a indústria do entretenimento ao introduzir um modelo de *streaming* que mudou a maneira de consumo de mídia. Juntos, esses empresários exemplificam a teoria de Schumpeter e demonstram que a inovação pode impulsionar o crescimento econômico e transformar indústrias inteiras.

Complementando o referido conceito que coloca os produtores como peça central no desenvolvimento econômico, a teoria da destruição criativa também é importante para compreender o presente cenário tecnológico. Schumpeter descreve que o sistema capitalista não possui um caráter estacionário – assim, em razão do dinamismo, a produção de bens e serviços alimentam a estrutura econômica (Schumpeter, 1942). Ele destacou a introdução de novas tecnologias substitui as antigas, alterando a cadeia produtiva de bens e serviços (Schumpeter, 1942). A teoria da destruição criativa de Schumpeter postula que o capitalismo

depende da constante inovação e renovação, com empreendedores desempenhando um papel crucial ao introduzir novas combinações produtivas (Takada, 2016).

De acordo com a teoria schumpeteriana, o sistema capitalista passa por transformações complexas e não lineares ao longo do tempo. Em vez de um simples crescimento, ocorre uma série de revoluções tecnológicas e organizacionais. Por exemplo, a agricultura evoluiu de práticas rudimentares para uma mecanização avançada, assim como a indústria do ferro e aço e a produção de eletricidade evoluíram de métodos primitivos para tecnologias modernas (Schumpeter, 1942). Esse processo é contínuo e se caracteriza por destruição e criação incessantes dentro da estrutura econômica. A destruição criativa, portanto, é um processo contínuo em que antigas indústrias e tecnologias são substituídas por novas, mais eficientes e inovadoras, impulsionando o progresso econômico (*ibidem*).

Um exemplo mais tangível se dá com o advento do *smartphone*, que substituiu diversas indústrias. Mapas físicos, outrora essenciais para dirigir, foram substituídos por aplicativos de GPS. Calculadoras, antes dispositivos físicos, agora estão a um clique de distância. Além disso, a digitalização transformou o setor bancário, com bancos digitais substituindo muitas funções dos bancos tradicionais. Esses exemplos ilustram como a destruição criativa reformula indústrias e altera significativamente a sociedade.

Estas teorias são importantes para compreender o cenário de inovação e avanço tecnológico atual com a ressalva de que este processo se encontra cada vez mais rápido. Há diversas métricas que podem ser utilizadas para tentar compreender tal fenômeno - a clássica é a Lei de Moore, inicialmente proposta por Gordon Moore, que tem sido um conceito fundamental na indústria de semicondutores, servindo como um indicador preditivo para avanços tecnológicos. Ela prevê que as capacidades da eletrônica digital dobrem aproximadamente a cada dois anos (Lundstrom; Alam, 2022).

A lei desempenhou um papel significativo no impulsionamento do crescimento exponencial da indústria, especialmente na fabricação de *chips* de

semicondutores, que é considerada a base do setor de tecnologia da informação eletrônica.[40] Assim, a teoria de Moore não apenas fundamentou indústria, mas também virou um símbolo da aceleração do avanço tecnológico, evidenciando como a inovação e o desenvolvimento tecnológico estão ocorrendo em um ritmo cada vez mais rápido

Isto é corroborado também pelo relatório "Data Never Sleeps 11.0" da DOMO[41] que destaca o aumento significativo na atividade em várias plataformas *online*. Através de um infográfico anual, a pesquisa oferece uma visão do volume imenso de dados gerados na *internet* a cada minuto, demonstrando como os dados estão em constante evolução à medida que mais pessoas interagem com plataformas e serviços digitais. O infográfico demonstra que a cada minuto de cada dia, espectadores assistem a 43 anos de conteúdo em plataformas de *streaming*, pessoas mandam 241 milhões de *e-mails* e usuários do ChatGPT mandam 6.944 *prompts*.

Estas mudanças também causam um impacto significativo na regulação. Com a constante transformação do sistema capitalista, conforme abarcado por Schumpeter, e com a rapidez do avanço tecnológico a qual a sociedade se encontra agora, é necessário compreender o impacto que este "novo mundo" causa na regulação. Um exemplo disso é o texto inicial do regulamento de Inteligência Artificial na Europa (*EU AI Act*) que não previu o lançamento de modelos generativos. Isso é relevante porque ferramentas como ChatGPT demonstram que a IA pode gerar conteúdo em um nível semelhante ao que os humanos podem alcançar, o que não estava amplamente antecipado quando a referida lei estava sendo desenvolvida. A rápida evolução da IA, coloca em voga o debate sobre a necessidade de regulamentações flexíveis e adaptáveis para lidar

[40] É importante notar que há um debate de que Lei de Moore está começando a falhar, Apesar dos desafios, seu impacto histórico no progresso tecnológico é inegável, impulsionando a revolução dos computadores e o crescimento tecnológico global. Ver: DeBenedictis, E. P. "Moore's Law: A Hard Act to Follow." IEE Computer, v. 52, n. 12, p. 114-117, dez. 2019. DOI: 10.1109/MC.2019.2941719

[41] Domo. Infographic: Data Never Sleeps 11.0. 2023. Disponível em: <https://www.domo.com/learn/infographic/data-never-sleeps-11>. Acesso em 07 jun. 2024.

com esses avanços inesperados. Com isso em mente, é necessário compreender, primeiramente, quais são de fato os desafios enfrentados pela tecnologia.

2. Dificuldade regulatória de serviços e produtos inovadores

Conforme apresentado na primeira etapa, o primeiro desafio que a regulação enfrenta é a constante introdução de inovação no mercado. O exemplo do *EU AI Act* demonstra o que ocorre quando as leis existentes não conseguem acompanhar a velocidade da inovação tecnológica. Um fator que agrava tal situação é a resposta legislativa demasiadamente lenta. Um levantamento exploratório do Aprovômetro do JOTA,[42] demonstra que a aprovação de emendas constitucionais e leis ordinárias no Brasil entre os anos 1990 e 2019, pode levar mais de três anos, criando um vácuo regulatório que pode ser explorado por novos modelos de negócios antes que a regulação apropriada esteja em vigor.

O acima exposto, por sua vez, propicia a criação de vazios regulatórios, ou seja, quando serviços disruptivos desafiam as regulações existentes por não se encaixarem nas categorias tradicionais de regulação. Um exemplo é o Uber, que se autodenomina uma empresa de tecnologia conectando motoristas e passageiros, mas opera essencialmente como um serviço de transporte. Isso criou desafios para reguladores em todo o mundo, que precisam decidir como aplicar as leis existentes ou desenvolver novas leis para acomodar esses serviços. Da mesma forma, o Airbnb permite que proprietários aluguem suas propriedades a curto prazo, desafiando as regulamentações de hospedagem tradicionais. Em muitas cidades, isso resultou em debates sobre regulamentação de ocupação, segurança, impostos e impacto no mercado imobiliário (Nohara, 2022)

Para evitar essa assimetria regulatória, busca-se aplicar a regra de que serviços iguais devem ser submetidos às mesmas regulamentações. No entanto, esses novos serviços geralmente não se enquadram nos moldes dos serviços existentes, pois utilizam plataformas tecnológicas que conectam usuários de maneiras inovadoras, exigindo uma abordagem regulatória que leve em conta a

[42] JOTA, Brasília, 25 maio 2020. Disponível em: <https://www.jota.info/legislativo/congresso-tramitacao-aprovometro-25052020?non-beta=1>. Acesso em: 7 jun. 2024.

complexidade e a peculiaridade desses serviços. Em casos envolvendo o Uber, por exemplo, a regulação enfrenta o desafio de equilibrar os interesses dos consumidores, que se beneficiam de um serviço de transporte mais barato e eficiente, com a necessidade de proteger os interesses dos taxistas tradicionais que operam sob um regime regulatório mais rigoroso. Assim, a discussão não é apenas sobre a necessidade de novas regulações, mas também sobre a revisão das antigas, considerando se os critérios existentes são justos e eficazes para a realidade atual dos novos modelos de negócios. (Nohara, 2022)

Um outro desafio também relacionado ao vazio regulatório é o que Elizabeth Pollman e Jordan M. Barry chamam de "empreendedorismo regulatório"[43], ou seja, quando empresas – normalmente de tecnologia - fazem da mudança das leis uma parte fundamental de seus planos de negócios ("empreendedores regulatórios"). Para os autores, empresas como a Uber são construídas com base em um plano para mudar as leis e, em alguns casos, até mesmo violá-las enquanto isso não acontece. Para essas empresas, a atividade política tornou-se uma parte crucial da estratégia de negócios. Entretanto, estas se diferem das atividades tradicionais de lobby corporativo, que buscam influenciar leis aplicáveis a negócios legais já estabelecidos. Isto porque "o empreendedorismo regulatório" envolve a criação de negócios sabendo que mudar a lei é uma parte essencial do plano de negócios.

Ademais, a pesquisa aponta que enquanto o lobby corporativo tradicional envolve acesso discreto a autoridades, os "empreendedores regulatórios" tornam suas questões altamente visíveis ao público, mobilizando-a a seu favor e utilizando esse apoio popular como alavanca para conseguir mudanças. O artigo, por sua vez, tem corroboração no Brasil quando o PL 2630/2020 – popularmente conhecido como PL das *Fake News* – estava sendo discutido em plenário. A empresa Telegram, dona de um aplicativo de mensagens instantâneas, disparou avisos a seus usuários mencionando que o projeto de lei iria "acabar com a

[43] POLLMAN, Elizabeth; BARRY, Jordan M. Regulatory Entrepreneurship. Loyola Law School, Los Angeles **Legal Studies Research Paper** No. 2017-29, 90 S. Cal. L. Rev. 383 (2017). Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732521>. Acesso em: 07 de jun. 2024.

liberdade de expressão"[44]. Essas ações levantam questões sobre a influência desproporcional dessas empresas no processo legislativo. Assim, o empreendedorismo regulatório revela uma faceta complexa da interação entre tecnologia, negócios e legislação, onde a capacidade de moldar as normas jurídicas se torna um diferencial competitivo e estratégico para essas empresas.

Destaca-se também um fenômeno descrito por David Collingridge (Kudina; Verbeek, 2019), no qual, em períodos de disrupção, os reguladores enfrentam um dilema: regular precocemente, ou seja, sem evidências suficientes - o que pode prejudicar a inovação - ou, por outro lado, optar por não intervir, o que pode resultar, entre outros problemas, em violações de direitos fundamentais. É evidente que encontrar um equilíbrio que garanta a segurança dos usuários desses serviços e promova a inovação não é tarefa fácil. Entretanto, em um período de transição tecnológica contínua, a incapacidade de abordar essas questões regulatórias cria um ambiente de incerteza e insegurança, além de acarretar riscos para a sociedade.

Por fim, como destacado no início, setores que exigem altos investimentos tecnológicos, particularmente os mercados digitais, são frequentemente caracterizados por dinâmicas que favorecem a formação de monopólios. Essas dinâmicas incluem economias de escala, efeitos de rede e proteção por direitos de propriedade intelectual, entre outras. Compreender essas características é crucial para desenvolver abordagens regulatórias eficazes que promovam a concorrência (*competition for the market*).

Grandes economias de escala significam que a produção em grande volume reduz significativamente os custos unitários. Em setores como o de tecnologia, onde os custos fixos (como P&D e infraestrutura) são altos, empresas estabelecidas podem operar a custos muito mais baixos que novos entrantes. Intervenções regulatórias podem ser necessárias para evitar que uma empresa

[44] TORTELLADA, Tiago. Telegram dispara mensagem contra o PL das Fake News. CNN Brasil, São Paulo, 09 maio 2023. Disponível em: <https://www.cnnbrasil.com.br/politica/telegram-dispara-mensagem-contra-o-pl-das-fake-news/#:~:text=O%20Telegram%20disparou%20mensagens%20contra,com%20a%20liberdade%20de%20express%C3%A3o>. Acesso em: 07 jun. 2024.

dominante abuse de sua posição de mercado, impondo preços excessivos ou reduzindo a qualidade dos serviços. Reguladores podem impor controles de preços ou exigências de acesso a infraestruturas essenciais para novos entrantes.[45]

Vale resgatar e diferenciar a ideia de concorrência no mercado para a concorrência pelo mercado para compreender o desafio para a regulação diante de práticas disruptivas. A concorrência no mercado ocorre quando várias empresas competem simultaneamente por uma participação de mercado. Isso significa que cada empresa está tentando atrair consumidores dos seus concorrentes, buscando aumentar sua própria fatia de mercado em termos de vendas, contratos e relações com clientes. Por outro lado, a concorrência pelo mercado refere-se a um cenário em que as empresas competem para se tornar o fornecedor dominante ou único de um determinado mercado de produto ou serviço. Nesse tipo de concorrência, a luta é pela captura e dominação do mercado como um todo, em vez de apenas uma parte dele. A competição se concentra na captura do mercado inteiro. Empresas inovam agressivamente e implementam estratégias para se tornarem a opção preferida ou exclusiva dos consumidores.

A partir dessas distinções o texto, de forma similar, sugere a ideia de regulação para o mercado, que pode ser contrastada em relação à regulação no mercado e a seguir sistematizada:

[45] Plataformas digitais frequentemente beneficiam-se de efeitos de rede, onde o valor do serviço aumenta com o número de usuários. Esses efeitos podem criar barreiras significativas à entrada de novos concorrentes. As autoridades podem precisar impor medidas para garantir a interoperabilidade entre plataformas, prevenir práticas anticompetitivas (como bloqueio de acesso a concorrentes) e promover a portabilidade de dados dos usuários para permitir a movimentação entre diferentes serviços.

Tabela 01: Regulação no mercado vis-à-vis regulação para o mercado

Elemento comparativo	Regulação no Mercado	Regulação para o Mercado
Definição	Intervenção direta do Estado para controlar práticas em determinados setores por força de lei.	Criação de condições para que a própria dinâmica de mercado regule o comportamento das empresas, sob a supervisão do Estado.
Objetivo	Proteger os consumidores e garantir qualidade e segurança dos serviço.	Promover a concorrência e a inovação contínua.
Métodos	Controle de qualidade, regulamentação de tarifas, restrições de entrada, requisitos de licenciamento.	Redução de barreiras à entrada, promoção de interoperabilidade, incentivos à inovação.
Requisitos para Eficácia	Supervisão contínua, conformidade com regulamentos específicos, atualização regulatória constante.	Ambiente legal que permita entrada fácil, medidas que incentivem a competição e a inovação.
Relação com a Inovação	Pode ser conservadora, priorizando estabilidade sobre inovação.	Estimula a inovação ao permitir que novas empresas entrem e desafiem incumbentes.
Desempenho em Setores Dinâmicos	Frequentemente lento para se adaptar a mudanças rápidas.	Melhor desempenho em setores tecnológicos e dinâmicos devido à flexibilidade e adaptabilidade.
Exemplos	Mercado financeiro (regulação de bancos), saúde pública (controle de medicamentos).	Plataformas digitais (eg. Google, Amazon), fintechs (criação de novos serviços financeiros).

Fonte: Autores

Por trás deste debate, a ideia de contestação é relevante. Introduzida pelos economistas William Baumol, John Panzar e Robert Willig em seu livro *Contestable Markets and the Theory of Industry Structure* (1982), a teoria dos mercados contestáveis sugere que um mercado pode ser competitivo mesmo com

um número pequeno de empresas, desde que as barreiras à entrada e saída sejam baixas e os custos de investimento sejam reversíveis. A inovação pode ser uma forma eficaz de competir em mercados contestáveis. Empresas que introduzem novos produtos, serviços ou modelos de negócios podem rapidamente capturar participação de mercado, mesmo em ambientes dominados por poucos jogadores.

Em setores regulados, a implementação de medidas que diminuam as barreiras à entrada e saída pode aumentar a contestabilidade do mercado. Isso pode incluir simplificação de licenças, redução de custos regulatórios e eliminação de monopólios legais desnecessários. Da mesma forma, é possível refletir sobre a facilitação do acesso à infraestrutura essencial já que entes reguladores podem garantir que novos entrantes tenham acesso justo e não discriminatório a infraestruturas essenciais controladas por incumbentes, como redes de telecomunicações ou serviços de utilidade pública.

Desta forma, para enfrentar os desafios apresentados pelos serviços disruptivos, busca-se caminhos em que a regulação seja flexível e adaptativa. Ademais aponta-se que a colaboração entre o setor público e o privado é vital para uma regulação eficaz. A participação de empresas inovadoras, sociedade civil e reguladores em processos colaborativos pode ajudar a identificar riscos e desenvolver soluções justas e eficientes. Isso envolve a criação de estruturas que possam se ajustar rapidamente às mudanças no mercado e nas tecnologias. Modelos de regulação adaptativa, como os *sandboxes*, surgem como mecanismos que permitirem a experimentação controlada e ajustes baseados em dados empíricos. Desta forma, se mostra imprescindível compreender a adoção deste fenômeno e suas aplicações práticas quando se fala na regulação de tecnologias inovadoras.

3. Desenvolvimento experimental: o impacto dos *sandboxes* regulatórios no ecossistema de inovação

No artigo "Innovation-Friendly Regulation: The Sunset of Regulation, The Sunrise of Innovation"[46], Sofia Ranchordás, discute como a regulação e a governança podem incentivar ou atrasar a introdução de novas tecnologias, dependendo dos mecanismos adotados. Reconhecendo a inovação como uma prioridade para muitos governos em busca de crescimento econômico e desenvolvimento, ela argumenta a favor de práticas regulatórias mais receptivas ao progresso tecnológico. Propõe-se, então, o uso de uma regulação mais flexível e adaptável, sem comprometer a responsabilidade e segurança.

Desta forma, deve ser encontrado uma maneira em que a regulação e o desenvolvimento coexistam (Handrlica, Sharp e Nešpor, 2023). Um dos mecanismos empregados para tentar alcançar este objetivo é o caminho dos *sandboxes* regulatórios (Ranchordás, 2021). Adotado a partir da experiência do Reino Unido, através do Financial Conduct Authority (FCA)[47], tal mecanismo experimental, de acordo com o Parlamento Europeu[48], ainda não possui uma definição consensual. No entanto, são geralmente vistos como ferramentas regulatórias que permitem às empresas testar e experimentar novos produtos, serviços ou modelos de negócios sob supervisão regulatória por um período limitado.

Esse mecanismo promove o aprendizado empresarial, facilitando o desenvolvimento e teste de inovações em um ambiente real. Além disso, apoiam o aprendizado regulatório, auxiliando na formulação de regimes legais experimentais que orientam e suportam as atividades de inovação das empresas sob a supervisão de uma autoridade reguladora. Na prática, essa abordagem

---

[46] RANCHORDAS, Sofia. Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation. **Jurimetrics**, v. 55, n. 2, 2015.

[47] FINANCIAL CONDUCT AUTHORITY (United Kingdom). Regulatory Sandbox. 2022. Disponível em: https://www.fca.org.uk/firms/innovation/regulatory-sandbox. Acesso em: 6 jun. 2024.

[48] PARLAMENTO EUROPEU. Regulatory Sandboxes and Innovation Hubs for Fintech. Bruxelas: Serviço de Estudos do Parlamento Europeu, 2022. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733544 Acesso em: 15 maio 2024

possibilita a inovação experimental dentro de um contexto de riscos controlados e supervisão, além de melhorar a compreensão dos reguladores sobre novas tecnologias.[49]

Embora seja um fenômeno novo, já há um impacto no Brasil. A ANPD abriu uma consulta à sociedade sobre *sandbox* regulatório de inteligência artificial e proteção de dados pessoais[50]. Além disso, o fenômeno em questão tem previsão expressa no artigo 11 lei das Startups (Lei Complementar n.182/2021). Ademais, diversas cidades e estados têm adotado o modelo de *sandbox* regulatório para fomentar a inovação. Foz do Iguaçu, por exemplo, implementou um programa de ambiente regulatório experimental, antes mesmo da entrada em vigor do Marco Legal das Startups (TCU, 2023).

O *sandbox* de Foz do Iguaçu focou no desenvolvimento de *smart cities*, ao transformar o bairro "Vila A" em um bairro inteligente. Isso envolveu a instalação de semáforos e luminárias inteligentes, pontos de ônibus tecnológicos e um Centro de Controle e Operações (CCO). Para implementar essas medidas, a Prefeitura Municipal contou com o apoio de várias entidades, incluindo a Agência Brasileira de Desenvolvimento Industrial (ABDI) e a Itaipu Binacional (*ibidem*).

A governança do programa foi realizada através de um Comitê Gestor plural, incluindo a participação de diversos atores no processo de tomada de decisão. Essa abordagem buscou integrar as iniciativas do *sandbox* com as políticas municipais de inovação, assegurando que as experimentações atendessem às necessidades da população e contribuíssem para a coletividade (ABIDI, 2021).

---

[49] Para Irene Nohara (2023, p. 38):o sandbox regulatório se estabelece como uma alegoria de 'caixa de areia' necessária para testagem de novos produtos e serviços em uma ambiência real e, ao mesmo tempo, controlada, com a devida flexibilidade e segurança imprescindível para que a regulação tradicional de serviços não seja fator que barre o desenvolvimento das atividades de fato disruptivas, abrindo um espaço relevante à indispensável adaptação às inovações, que se tornam a tônica dos tempos atuais.

[50] Aberta consulta à sociedade sobre sandbox regulatório de inteligência artificial e proteção de dados pessoais no Brasil. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-a-sociedade-sobre-sandbox-regulatorio-de-inteligencia-artificial-e-protecao-de-dados-pessoais-no-brasil>. Acesso em 28 mar. 2024.

A inciativa se deu através de um Decreto Municipal[51] que regulamentou o mecanismo experimental. Este arcabouço permitiu a suspensão temporária da legislação municipal pelo Comitê Gestor, desde que fosse comprovado, de maneira clara e inequívoca, o caráter inovador do teste[52]. Outro parâmetro interessante de mencionar foi o prazo de cada ciclo experimental - podendo durar de seis a doze meses[53].

A partir dessa experiência, a cidade lançou o programa "Smart Vitrine", um mecanismo contínuo de avaliação e validação de tecnologias no ambiente do *sandbox*. Segundo dados da Itaipu[54] foram realizados quatro ciclos de convocação, visando encontrar soluções em diversas áreas, como meio ambiente, urbanismo, saúde e educação. No total, mais de 65 empresas e startups se inscreveram, incluindo duas empresas internacionais. Até 2022, os investimentos já ultrapassavam seiscentos mil reais em Foz do Iguaçu, demonstrando o potencial dos *sandboxes* para contribuir com o desenvolvimento econômico da região.

Outro caso de destaque do uso de *sandbox* regulatório no Brasil ocorreu de forma semelhante à experiência inicial britânica, que visava implantar um modelo para o desenvolvimento de produtos e serviços no mercado financeiro. Em 2019, a Susep, a CVM e o Banco Central anunciaram conjuntamente a intenção de estabelecer programas de *sandbox* regulatório em resposta à transformação tecnológica dos setores[55]. Esse intuito se tornou realidade: a primeiro destas instituições a lançar um programa de *sandbox* foi a Susep através

---

[51] FOZ DO IGUAÇU. Decreto nº 28.244, de 23 de junho de 2020. Regulamenta no âmbito do Município de Foz do Iguaçu, a instituição de ambientes experimentais de inovação científica, tecnológica e empreendedora, sob o formato de Bancos de Testes Regulatórios e Tecnológicos - "Programa Sandbox - Foz do Iguaçu". Foz do Iguaçu: Prefeitura Municipal, 2020.

[52] Art. 3º, *caput*, Decreto nº 28.244, de 23 de junho de 2020.

[53] Art. 6º, *caput*, Decreto nº 28.244, de 23 de junho de 2020.

[54] PARQUE TECNOLÓGICO DE ITAIPU. Novas instalações de tecnologias no sandbox "Vila A Inteligente" consolidam sucesso do Smart Vitrine para Foz do Iguaçu. Disponível em: <https://www.pti.org.br/novas-instalacoes-de-tecnologias-no-sandbox-vila-a-inteligente-consolidam-sucesso-do-smart-vitrine-para-foz-do-iguacu/.> Acesso em: 26 jun. 2024

[55] BANCO CENTRAL DO BRASIL. Comunicado Conjunto Ministério da Economia, Banco Central, CVM e Susep: divulga ação coordenada para implantação de regime de sandbox regulatório nos mercados financeiro, securitário e de capitais brasileiros. Disponível em: <https://www.bcb.gov.br/detalhenoticia/16776/nota>. Acesso em: 26 jun. 2024

da Resolução CNSP n.º 381, de março de 2020[56] que definiu as regras gerais para a atuação da autarquia na criação e gestão do *sandbox* regulatório e a Circular Susep nº 598/2020[57] que complementou a resolução, detalhando procedimentos como a solicitação de autorização e os documentos necessários.

Em 2021, a Susep lançou um relatório de projeto estratégico[58] para destacar os objetivos e resultados de sua primeira experiência experimental. Segundo a autarquia, a adoção desse mecanismo foi crucial devido à penetração limitada do mercado de seguros no Brasil. Desta forma, ao introduzir o *sandbox*, buscava-se alcançar vantagens significativas, como a melhoria da qualidade do serviço ao consumidor, aumento da eficiência operacional, redução de custos e expansão do mercado de seguros. Com isso em mente, a Susep concebeu o modelo baseado em três pilares fundamentais: (i) gestão controlada de riscos, (ii) fomento à inovação e (iii) foco no consumidor. A regulamentação também contemplou medidas para facilitar a entrada de novas empresas, como a redução do capital inicial exigido e a simplificação das normas regulatórias.

Consequentemente, a Susep relata que muitos consumidores utilizaram serviços de empresas aprovadas no programa pela primeira vez. Isso se deve a diversos fatores, incluindo a aplicação de tecnologias como inteligência artificial, internet das coisas (IoT) e contratos inteligentes. Além disso, foram adotadas

---

[56] *SUPERINTENDÊNCIA DE SEGUROS PRIVADOS* - SUSEP - Resolução CNSP nº 381, de 04 de março de 2020. Estabelece as condições para autorização e funcionamento, por tempo determinado, de sociedades seguradoras participantes exclusivamente de ambiente regulatório experimental (Sandbox Regulatório) que desenvolvam projeto inovador mediante o cumprimento de critérios e limites previamente estabelecidos e dá outras providências. Disponível em: <https://www.susep.gov.br/menu/atos-normativos/normativos/normativos-emitidos-pela-susep>. Acesso em: 26 jun. 2024

[57] *SUPERINTENDÊNCIA DE SEGUROS PRIVADOS* - SUSEP. Circular SUSEP nº 598, de 19 de março de 2020. Dispõe sobre autorização, funcionamento por tempo determinado, regras e critérios para operação de produtos, transferência de carteira e envio de informações das sociedades seguradoras participantes exclusivamente de ambiente regulatório experimental (Sandbox Regulatório) que desenvolvam projeto inovador mediante o cumprimento de critérios e limites previamente estabelecidos. Disponível em: https://www.susep.gov.br/menu/atos-normativos/normativos/circular-susep. Acesso em: 26 jun. 2024.

[58] *SUPERINTENDÊNCIA DE SEGUROS PRIVADOS* - SUSEP. Relatório do Projeto Estratégico – Sandbox Regulatório. Rio de Janeiro: SUSEP, dezembro, 2021. Disponível em: <https://www.gov.br/susep/pt-br/arquivos/arquivos-transparencia/arquivos-pei/Arquivos_projetos_estrategicos/RELATORIO_FINAL_PROJETO_SANDBOX_REGULATORIO_20211.pdf> Acesso em: 26 jun. 2024.

estratégias inovadoras, como a personalização de coberturas e o uso de *cashback*, com precificação baseada no comportamento do consumidor. Essas iniciativas mostram potencial para a redução de preços e a ampliação do mercado de seguros.

Por outro lado, observa-se que o próprio regulador, a Susep, também colheu benefícios com essa experiência, como a redução da burocracia, a flexibilização das normas com base na experiência adquirida e melhorias tecnológicas. Dessa forma, conclui-se que os resultados são promissores. No entanto, é importante ressaltar que esta é apenas uma experiência inicial, sendo crucial monitorar continuamente os resultados para entender o impacto de longo prazo dessas iniciativas.

O *sandbox* do Banco Central, por sua vez, foi lançado com o objetivo de fomentar a concorrência no setor bancário e de pagamentos, incentivando a entrada de agentes com soluções inovadoras como parte de uma estratégia para estimular a inovação tecnológica e garantir segurança jurídica para novos produtos e serviços (Amato; Missagia, 2023).

As prioridades estratégicas estabelecidas para o ambiente experimental[59] refletem os desafios e oportunidades do sistema financeiro brasileiro. O fomento ao mercado de capitais, o crédito para micro e pequenas empresas, a integração com o Open Banking e o Pix, o desenvolvimento do mercado de crédito rural e a promoção de finanças sustentáveis são alguns dos focos do programa[60]. Com um prazo inicial de um ano, prorrogável por igual período, o projeto buscou garantir a qualidade dos projetos selecionados, visando alcançar os objetivos do programa.

[59] BANCO CENTRAL DO BRASIL. Resolução BCB nº 50, de 16 de dezembro de 2020. Dispõe sobre os requisitos para instauração e execução pelo Banco Central do Brasil do Ambiente Controlado de Testes para Inovações Financeiras e de Pagamento (Sandbox Regulatório) – Ciclo 1, bem como sobre os procedimentos e requisitos aplicáveis à classificação e à autorização para participação nesse ambiente. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=50>. Acesso em: 26 jun. 2024.

[60] Art. 7º, Resolução BCB nº 50, de 16 de dezembro de 2020.

Por fim, aponta-se a experiência da CVM, que através da Instrução CVM 29, de maio de 2021[61], instituiu que o Comitê de Sandbox, composto por servidores da CVM, é responsável por conduzir as atividades estipuladas pela instrução, garantindo um ambiente propício para a inovação no mercado financeiro. Ademais, possui como principais objetivos fomentar a inovação, orientar os participantes sobre questões regulatórias, reduzir custos e o tempo de desenvolvimento de novos produtos e serviços, além de ampliar a visibilidade e atração para investimentos de capital de risco. Também visa aumentar a competição entre fornecedores de serviços financeiros, promover a inclusão financeira com produtos mais acessíveis e aprimorar o arcabouço regulatório aplicável.

A autarquia aprovou quatro empresas que receberam permissão temporária para trabalhar com diferentes tipos de valores mobiliários. A Basement, por exemplo, obteve a permissão de atuar como escriturador para sociedades que estão ou vão fazer ofertas públicas de valores mobiliários, especialmente sociedades pequenas. Outros projetos como Beegin, CIP e Finchain trabalham com valores mobiliários de pequenas e médias empresas, enquanto o projeto da Vórtx tem relação com debêntures e cotas de fundos fechados, usando regras específicas para suas ofertas.

O que estes exemplos demonstram, portanto, é como os *sandboxes* regulatórios podem ser adaptados para diferentes setores e necessidades locais, promovendo a inovação enquanto asseguram a proteção dos consumidores e a integridade do mercado. Esses mecanismos surgem - não apenas para proporcionar um ambiente seguro para o desenvolvimento de novas tecnologias - mas também para fortalecer a capacidade dos reguladores de compreender e responder às mudanças rápidas e disruptivas no cenário econômico e tecnológico global. Ao facilitar o teste de soluções inovadoras em condições controladas, os *sandboxes* podem incentivam o empreendedorismo e a competitividade, além de

[61] É importante notar que esta instrução revogou uma anterior (Resolução CVM N. 29). COMISSÃO DE VALORES MOBILIÁRIOS - CVM. Instrução CVM nº 626, de 15 de maio de 2020. Dispõe sobre as regras para constituição e funcionamento de ambiente regulatório experimental (sandbox regulatório). Disponível em: <http://www.cvm.gov.br/>. Acesso em: 26 jun.

colocarem as instituições que os adotam em uma posição mais adaptável às demandas da era digital.

Por fim, vale destacar que a regulação sandbox tem ganhado destaque como um modelo de regulação "para o mercado". Ao permitir a experimentação e a inovação, ela ajuda a moldar mercados futuros, incentivando práticas de negócios que podem ser benéficas para consumidores e empresas a longo prazo. A abordagem sandbox é projetada para criar um ambiente competitivo onde as inovações podem desenvolver. Reguladores trabalham em parceria com empresas para garantir que as inovações não só atendam aos requisitos de segurança e proteção ao consumidor, mas também que contribuam para um mercado mais dinâmico e eficiente.

Considerações Finais

Conforme apresentado neste texto, a regulação de serviços e produtos inovadores é um desafio complexo que, em face do presente cenário, exige uma abordagem adaptativa. As evoluções tecnológicas, impulsionadas pela inovação e pela destruição criativa descritas por Schumpeter, estão transformando rapidamente a sociedade e a economia. Essas mudanças, por sua vez, estão desafiando os modelos regulatórios existentes, que muitas vezes não conseguem acompanhar o ritmo da inovação. A rapidez com que novas tecnologias são introduzidas no mercado, muitas vezes sem uma regulamentação adequada, cria vazios regulatórios que podem ser explorados por empresas inovadoras, mas também podem representar riscos para os consumidores e a sociedade em geral. A resposta legislativa tradicional se mostra muitas vezes lenta e reativa, não sendo suficiente para lidar com esses desafios.

A regulação para o mercado de forma similar a discussão sobre competição pelo mercado é uma chave de análise para esta situação. Como apontado, os entes reguladores hoje possuem o desafio de garantir que a regulação não apenas proteja os consumidores, mas também estimule o desenvolvimento de tecnologias mais inclusivas e de alta qualidade, contribuindo para um crescimento econômico sustentável.

Diante desse cenário, os *sandboxes* regulatórios surgem como uma abordagem para lidar com a regulação de serviços e produtos inovadores. Esses mecanismos permitem que empresas testem e experimentem novas tecnologias sob supervisão regulatória, facilitando a inovação enquanto se protege os consumidores e se mantém a integridade do mercado. No Brasil tal ambiente experimental se encontra implementado em diferentes setores, como demonstrado pelo caso de Foz do Iguaçu, da Susep, da CVM e do Bacen. Essas iniciativas um potencial de promover a inovação de forma responsável, criando um ambiente que estimula o desenvolvimento de produtos e serviços mais inclusivos e de maior qualidade.

Percebe-se, portanto que os serviços disruptivos apresentam desafios significativos para os reguladores, mas também oferecem oportunidades para desenvolver modelos regulatórios mais flexíveis e adaptativos. Através do uso inteligente de ferramentas como os *sandboxes* regulatórios, é possível garantir que a regulação acompanhe o ritmo da inovação, promovendo um desenvolvimento sustentável e equilibrado das novas tecnologias.

Referências

AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL. **Guia Sandbox para Cidades Inteligentes**. São Paulo, setembro de 2021. Disponível em: <https://sandbox.abdi.com.br/page/index2.html.> Acesso em: 27 jun. 2024.

AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Ambientes regulatórios experimentais: O sandbox no sistema financeiro brasileiro. **RBSD – Revista Brasileira de Sociologia do Direito**, v. 10, n. 3, p. 143-171, set./dez. 2023. Disponível em: https://revista.abrasd.com.br/index.php/rbsd/article/view/747 . Acesso em 23 set. 2024.

BALBINO, Carlos Marcelo; SILVINO, Zenith Rosa; JOAQUIM, Fabiana Lopes; SOUZA, Cláudio José de; SANTOS, Lucimere Maria dos. Inovação tecnológica: perspectiva dialógica sob a ótica do Joseph Schumpeter. **Research, Society and**

Development, v. 9, n. 6, e198963593, 2020. DOI: http://dx.doi.org/10.33448/rsd-v9i6.3593. Disponível em: https://orcid.org/0000-0003-0763-3620 . Acesso em: 07 jun. 2024.

BANCO CENTRAL DO BRASIL. **Comunicado Conjunto Ministério da Economia, Banco Central, CVM e Susep: divulga ação coordenada para implantação de regime de sandbox regulatório nos mercados financeiro, securitário e de capitais brasileiros**. Disponível em: <https://www.bcb.gov.br/detalhenoticia/16776/nota>. Acesso em: 26 jun. 2024

BANCO CENTRAL DO BRASIL. Resolução BCB nº 50, de 16 de dezembro de 2020. **Dispõe sobre os requisitos para instauração e execução pelo Banco Central do Brasil do Ambiente Controlado de Testes para Inovações Financeiras e de Pagamento (Sandbox Regulatório) – Ciclo 1, bem como sobre os procedimentos e requisitos aplicáveis à classificação e à autorização para participação nesse ambiente**. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=50>. Acesso em: 26 jun. 2024.

BAUMOL, William; PANZAR, John; WILLIG, Robert. **Contestable Markets and the Theory of Industry Structure**. Nova Iorque: Harcourt Brace Jovanovich, 1982.

BRASIL. Lei nº 10.973, de 2 de dezembro de 2004. **Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm>. Acesso em: 07 jun. 2024.

COMISSÃO DE VALORES MOBILIÁRIOS - CVM. Instrução CVM nº 626, de 15 de maio de 2020. **Dispõe sobre as regras para constituição e funcionamento de ambiente regulatório experimental (sandbox regulatório)**. Disponível em: <http://www.cvm.gov.br/>. Acesso em: 26 jun.

DEBENEDICTIS, E. P. Moore's Law: A Hard Act to Follow. **Computer**, v. 52, n. 12, p. 114-117, dez. 2019. DOI: 10.1109/MC.2019.2941719

DOMO. **Infographic**: Data Never Sleeps 11.0. 2023. Disponível em: <https://www.domo.com/learn/infographic/data-never-sleeps-11>. Acesso em 07 jun. 2024.

DUARTE, Angelo et al. Central banks, the monetary system and public payment infrastructures: lessons from Brazil's Pix. **BIS Bulletin**, n. 52, 2022.

FISHER, Max. **A máquina do caos**: Como as redes sociais reprogramaram nossa mente e nosso mundo. Tradução de Érico Assis. 1. ed. São Paulo: Todavia, 2023.

FINANCIAL CONDUCT AUTHORITY (United Kingdom). **Regulatory Sandbox**. 2022. Disponível em: <https://www.fca.org.uk/firms/innovation/regulatory-sandbox>. Acesso em: 6 jun. 2024.

FOZ DO IGUAÇU. Decreto nº 28.244, de 23 de junho de 2020. **Regulamenta no âmbito do Município de Foz do Iguaçu, a instituição de ambientes experimentais de inovação científica, tecnológica e empreendedora, sob o formato de Bancos de Testes Regulatórios e Tecnológicos - "Programa Sandbox - Foz do Iguaçu"**. Foz do Iguaçu: Prefeitura Municipal, 2020.

HANDRLICA, J; SHARP, V.; NEŠPOR, J. Forum shopping in regulatory sandboxes and the perils of experimental law-making. **Juridical Tribune**, v. 13, n. 3, 1 nov. 2023.

KUDINA, Olya; VERBEEK, Peter-Paul. Ethics from Within: Google Glass, the Collingridge Dilemma, and the Mediated Value of Privacy. **Science, Technology, & Human Values**, v. 44, n. 2, p. 291-314, 2019. DOI: 10.1177/0162243918793711.

LUNDSTROM, Mark S.; ALAM, Muhammad A. Moore's law: The journey ahead. **Science**, [S.l.], v. 378, n. 6621, p. 722-723, 17 nov. 2022. DOI: 10.1126/science.ade2191.

MARCUS, J. Scott. Adapting the European Union AI Act to deal with generative artificial intelligence. **Bruelgel Analysis**, 19 jul. 2023. Disponível em: https://www.bruegel.org/analysis/adapting-european-union-ai-act-deal-generative-artificial-intelligence . Acesso em: 07 de jun. 2024.

MARCELINO, Daniel. Congresso: tempo de tramitação cai de mais de mil dias para apenas 15 dias. Dados fazem parte do Aprovômetro, a ferramenta preditiva

do JOTA. **JOTA**, Brasília, 25 maio 2020. Disponível em: https://www.jota.info/legislativo/congresso-tramitacao-aprovometro-25052020?non-beta=1 . Acesso em: 7 jun. 2024.

NOHARA, Irene Patrícia. Inovação e Experimentação em Sandbox Regulatório: Testagem de Impactos de Serviços Disruptivos pela Administração Pública. In: BITENCOURT, Caroline Müller; GABARDO, Emerson; BARRERA, Teresita Rendón Hurta (Orgs.). **Administração Pública, Novas Tecnologias e Políticas Públicas.** Curitiba: Íthala, 2023. p. 37-49.

BITENCOURT, Caroline Müller. Desafios de regulação dos serviços disruptivos: equilíbrio nas fronteiras da inovação. In: ZOCKUN, Maurício; GABARDO, Emerson (Coords.). **Direito Administrativo e Inovação**: crises e soluções. Curitiba: Íthala Ltda., 2022. p. 307-321.

PARLAMENTO EUROPEU. **Regulatory Sandboxes and Innovation Hubs for Fintech**. Bruxelas: Serviço de Estudos do Parlamento Europeu, 2022. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733544 . Acesso em: 7 jun. 2024.

PARQUE TECNOLÓGICO DE ITAIPU. **Novas instalações de tecnologias no sandbox "Vila A Inteligente" consolidam sucesso do Smart Vitrine para Foz do Iguaçu**. Disponível em: https://www.pti.org.br/novas-instalacoes-de-tecnologias-no-sandbox-vila-a-inteligente-consolidam-sucesso-do-smart-vitrine-para-foz-do-iguacu/ Acesso em: 26 jun. 2024

POLLMAN, Elizabeth; BARRY, Jordan M. Regulatory Entrepreneurship. Loyola Law School, **Los Angeles Legal Studies Research Paper** No. 2017-29, 90 S. Cal. L. Rev. 383 (2017). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732521 . Acesso em: 07 de jun. 2024.

RANCHORDAS, Sofia. Experimental lawmaking in the EU: Regulatory Sandboxes. EU Law Live, Weekend Edition, **University of Groningen Faculty of Law Research Paper** N. 12, out. 2021.

RANCHORDAS, Sofia. Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation. **Jurimetrics**, v. 55, n. 2, 2015.

SCHAPIRO, Mario G. et al. PIX: explaining a state-owned Fintech. **Brazilian Journal of Political Economy**, v. 43, p. 874-892, 2023.

SCHUMPETER, Joseph Alois. **Capitalismo, Socialismo e Democracia**. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2022.

SCHUMPETER, Joseph Alois. **Teoria do desenvolvimento econômico:** uma investigação sobre lucros, capital, crédito, juro e o ciclo econômico. Tradução de Maria Sílvia Possas. São Paulo: Nova Cultural, 1997.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS – SUSEP. Resolução CNSP nº 381, de 04 de março de 2020. **Estabelece as condições para autorização e funcionamento, por tempo determinado, de sociedades seguradoras participantes exclusivamente de ambiente regulatório experimental (Sandbox Regulatório) que desenvolvam projeto inovador mediante o cumprimento de critérios e limites previamente estabelecidos e dá outras providências**. Disponível em: https://www.susep.gov.br/menu/atos-normativos/normativos/normativos-emitidos-pela-susep . Acesso em: 26 jun. 2024

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS - SUSEP. Circular SUSEP nº 598, de 19 de março de 2020. **Dispõe sobre autorização, funcionamento por tempo determinado, regras e critérios para operação de produtos, transferência de carteira e envio de informações das sociedades seguradoras participantes exclusivamente de ambiente regulatório experimental (Sandbox Regulatório) que desenvolvam projeto inovador mediante o cumprimento de critérios e limites previamente estabelecidos**. Disponível em: https://www.susep.gov.br/menu/atos-normativos/normativos/circular-susep . Acesso em: 26 jun. 2024.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS - SUSEP. **Relatório do Projeto Estratégico – Sandbox Regulatório**. Rio de Janeiro: SUSEP, dezembro, 2021. Disponível em: https://www.gov.br/susep/pt-br/arquivos/arquivos-transparencia/arquivos-

pei/Arquivos_projetos_estrategicos/RELATORIO_FINAL_PROJETO_SANDBOX_REGULATORIO_20211.pdf . Acesso em: 26 jun. 2024.

TAKADA, Thalles Alexandre. Joseph Alois Schumpeter e a destruição criadora. **Revista Direito Mackenzie**, v. 10, n. 1, p. 188-200, 2016.

TRIBUNAL DE CONTAS DA UNIÃO. **Sandbox Regulatório no Marco Legal das Startups**. Brasília: TCU, Laboratório de Inovação, 2023.

5. Inovações regulatórias para tecnologias disruptivas: o *sandbox* de inteligência artificial

Caio Rezende Missagia[62]

Introdução

O debate sobre a relação entre regulação e inovação, embora esteja em alta com os recentes avanços da inteligência artificial, não é de hoje. A tensão entre essas duas forças frequentemente tidas como antagônicas se fez presente desde meados do século XX, em discussões sobre a regulação de tecnologias como energia nuclear, campos eletromagnéticos, emissões de gases de efeito estufa e alimentos geneticamente modificados (Wiener, 2004, p. 483).

No entanto, há algo que qualifica o debate na atualidade em relação a períodos passados: hoje, e a cada dia que passa, a velocidade com que novas tecnologias disruptivas são introduzidas nos mercados é cada vez maior. Certamente, a bola da vez é a inteligência artificial (IA). Apesar de ter surgido enquanto campo do conhecimento ainda na década de 1950[63], a IA tem passado por uma evolução frenética nos últimos anos. Um dos episódios mais marcantes dessa evolução foi o lançamento pela OpenAI, no final de 2022, do ChatGPT, um *chatbot* baseado em IA generativa. É sintomático o fato de o lançamento do ChatGPT ter obrigado a União Europeia a rever todo o projeto de regulação da IA então discutido para que pudesse comportar a IA generativa, que, até então, era desconhecida da sociedade em geral. Esse fato ilustra como o processo de

[62] Mestrando em Filosofia e Teoria Geral do Direito pela Faculdade de Direito da Universidade de São Paulo (USP). Graduado em Direito pela USP e pela *Université Jean-Monnet Saint-Etienne (licence en Droit)* e pós-graduado em Administração de Empresas pela Fundação Getúlio Vargas (FGV EAESP).

[63] "Na década de 1950, no âmbito dos esforços científico-tecnológicos de criar modelos de simulação da mente humana, surgiu o campo da inteligência artificial. O termo apareceu pela primeira vez no título do evento *Dartmouth Summer Research Project on Artificial Intelligence* (Projeto de Pesquisa de Verão de Dartmouth sobre Inteligência Artificial), realizado no Dartmouth College em Hanover, New Hampshire, EUA, no verão de 1956 (...)" (Kaufman, 2019, p. 21).

inovação tecnológica é fortemente atrelado à incerteza, trazendo consequências absolutamente imprevisíveis para a sociedade.

No debate sobre a regulação da IA, enquanto se apontam muitos riscos graves relacionados à tecnologia, reconhece-se, por outro lado, que seus benefícios em muitos domínios da sociedade também são extremamente positivos. Isso leva a uma questão já repetida muitas vezes: como equilibrar regulação e inovação, mitigando os riscos sem inibir os benefícios da tecnologia?

Nota-se que a ideia largamente reproduzida de se "equilibrar" regulação e inovação carrega, implícito, o pressuposto de que regulação e inovação seriam necessariamente dois pesos contrários: se um é excessivo, o outro fica suspenso. No entanto, em vez de concebê-las como fatores antagônicos, é preciso enxergá-las como forças complementares e indissociáveis. Não como pesos contrários em uma balança, mas como duas faces de uma mesma moeda.

Contextualizado em reflexões dessa natureza, o presente capítulo tem por objetivo explorar a relação entre o Estado (em suas dimensões empreendedora e regulatória) e a inovação tecnológica, apresentando um contraponto às visões que, por um lado, não reconhecem a função empreendedora do Estado e, por outro, enxergam a função regulatória estatal como um fator inerentemente inibidor da inovação tecnológica.

Para isso, em um primeiro momento, sobretudo com base na teoria do desenvolvimento de Schumpeter e na obra *O Estado Empreendedor*, de Mariana Mazzucato, será questionado o mito do "setor público ineficiente *vs.* setor privado inovador", apresentando-se uma visão do Estado como agente fundamental na história da inovação, sem o qual muitas das "inovações revolucionárias" geralmente atribuídas à iniciativa privada jamais teriam se concretizado.

Em seguida, será explorada a relação entre regulação e inovação, argumentando-se que a concepção dogmática que enxerga a regulação unicamente a partir do modelo de comando e controle, rígido e repressivo, cria a falsa ideia de que a regulação necessariamente seria incompatível com a dinâmica das novas tecnologias, as quais demandariam celeridade, flexibilidade

e colaboração por parte do regulador. Quando se rompe com essa concepção "monoinstitucionalista" da regulação, percebe-se que o Estado, no desempenho de sua função regulatória, pode contar com (e imaginar) inúmeras abordagens e ferramentas mais adequadas para lidar com a realidade acelerada de tecnologias disruptivas como a IA.

Por fim, para que as reflexões desenvolvidas não careçam de aplicação sobre um caso concreto, será feita uma breve análise do instituto do *sandbox* regulatório e sua aplicação no âmbito da regulação da IA. Tendo em vista que essa inovação regulatória foi originalmente pensada para o setor financeiro, é relevante buscar compreender se sua aplicação no caso da IA manteria a mesma finalidade do regulador financeiro – qual seja, reduzir barreiras à entrada e estimular a inovação e a concorrência no mercado. Ainda, serão sugeridos outros exemplos e modelos regulatórios que poderão servir de inspiração para o regulador da IA no Brasil, tendo em vista um objetivo de construção de um ecossistema favorável à inovação baseada em IA no país.

1. Estado e inovação

Na história do pensamento econômico, a ideia de inovação ganha centralidade na teoria do desenvolvimento econômico do austríaco Joseph A. Schumpeter (1883-1950). Para Schumpeter (2017 [1942], p. 119), o capitalismo deve ser compreendido como um processo evolucionário não linear, em constante mudança "de dentro para fora". Essa dinâmica, por sua vez, seria impulsionada pelas inovações criadas por uma figura central no processo de desenvolvimento capitalista: o empreendedor (Backhouse, 2002, p. 208).

O empreendedor, diferentemente de um mero administrador ou especulador, é aquele que efetivamente *inova*, isto é, introduz novos produtos ou métodos de produção, abre novos mercados, conquista novas fontes de matéria-prima ou desenvolve novas formas de organização (Schumpeter, 1983 [1934], p. 66). Com isso, o empreendedor desbrava oportunidades inéditas de lucro, antes inexistentes, levando as tecnologias anteriores à obsolescência e rompendo o equilíbrio do mercado. Após essa ruptura, porém, os demais empresários tendem

a copiar a inovação introduzida, passando a concorrer com aquele empresário inovador, de forma a, gradualmente, reestabelecer-se o equilíbrio do sistema, até que a concorrência chegue a um ponto de exaustão e mais um empreendedor venha inovar e revolucionar o mercado.

A economia capitalista, assim, seria marcada por ciclos sucessivos de (i) inovação (em que o empreendedor introduz uma inovação e passa a dominar o mercado, auferindo lucro de monopólio); e (ii) concorrência (em que, após abandonarem as tecnologias antigas e imitarem a nova, os empresários concorrem entre si mediante o corte de custos de produção e a redução de preços) (Backhouse, 2002, p. 183, 208). Quando não é mais possível cortar custos, o ciclo de concorrência atinge um ponto de saturação. A partir daí, ou algum empreendedor introduz uma nova tecnologia que irá revolucionar o mercado, reiniciando o ciclo de inovação, ou as empresas quebram.

A esse processo de constante revolução da estrutura capitalista "de dentro para fora" Schumpeter (2017 [1942], p. 120) deu o nome de "destruição criativa". Em sua teoria, portanto, o progresso econômico capitalista seria movido, fundamentalmente, pelas iniciativas inovadoras dos empreendedores privados, causadores do processo de destruição criativa.

Em *O Estado Empreendedor*, a influente economista italiana Mariana Mazzucato[64] (2014, p. 26), ao investigar a história da inovação, questiona esse protagonismo atribuído à iniciativa privada no desenvolvimento econômico, demonstrando, a partir de exemplos históricos, como, na realidade, o Estado é que foi a verdadeira força por trás das inovações tecnológicas mais revolucionárias, tais como as ferrovias, a internet, a nanotecnologia e a farmacêutica.[65]

---

[64] Ver reportagem da BBC News Brasil de 8 de agosto de 2020: "A economista que defende uma mudança radical do capitalismo para o mundo pós-pandemia". Disponível em: https://www.bbc.com/portuguese/internacional-53686431 .

[65] Vale destacar que Mazzucato não se opõe à teoria de Schumpeter. Pelo contrário, sua análise é baseada sobretudo nas ideias de Keynes e Schumpeter. A autora, no entanto, embora não negue a importância da iniciativa privada e a genialidade de alguns empreendedores, propõe que a história da inovação tem sido contada como se apenas o setor privado fosse responsável pelas tecnologias disruptivas que dão base para o progresso econômico, enquanto o Estado seria um "intruso". Ela questiona essa narrativa e demonstra como muitas das tecnologias mais

Segundo Mazzucato (2014, p. 94), a inovação tecnológica é um processo marcado por um alto grau de incerteza e que demanda estratégias pacientes de longo prazo. Por essa razão, as empresas privadas, que têm como foco a maximização dos lucros no curto prazo, não têm interesse, por exemplo, em investir em pesquisas de base para o desenvolvimento de projetos tecnológicos revolucionários, cujos retornos são altamente incertos. Em vez disso, quando "inovam", preferem focar no desenvolvimento de produtos e processos *marginalmente* novos, cujos riscos são relativamente calculáveis. Os investimentos empresariais em tecnologias revolucionárias, assim, são limitados não apenas pela ausência de recursos, mas também pela falta de coragem do empreendedor para "apostar" em uma iniciativa extremamente incerta (Mazzucato, 2014, p. 52).

O setor público, ao contrário, por não ter de atender a interesses imediatos de acionistas (mas sim ao interesse público) e poder focar em estratégias de desenvolvimento de longo prazo, toma iniciativas audaciosas para, em meio à incerteza, conceber e desenvolver tecnologias revolucionárias e criar novos mercados, dinamizando a economia, impulsionando a evolução tecnológica e difundindo o conhecimento por toda a sociedade (Mazzucato, 2014, p. 39).

Apesar de essa ser a "verdadeira história da inovação", a autora (2014, p. 104-105) aponta que ainda prevalece um mito, baseado na ideologia fundamentalista de mercado, de que o setor privado seria o verdadeiro responsável pela assunção de riscos, pelo empreendedorismo, pela inovação, pela criação de novos mercados e pelo desenvolvimento econômico, ao passo que o Estado seria um intruso, um ator econômico secundário, um gigantesco leviatã burocrático e ineficiente que apenas atrapalha as corajosas iniciativas dos empreendedores inovadores. De acordo com essa visão, caberia ao Estado tão somente corrigir as "falhas de mercado" porventura existentes, deixando a iniciativa econômica a cargo dos empresários individuais.

revolucionárias (como a internet, o GPS e a nanotecnologia) foram pacientemente concebidas e desenvolvidas pela iniciativa do Estado. É uma questão, portanto, de reconhecer também o papel crucial do Estado na história da inovação e do progresso econômico (Mazzucato, 2014, p. 47).

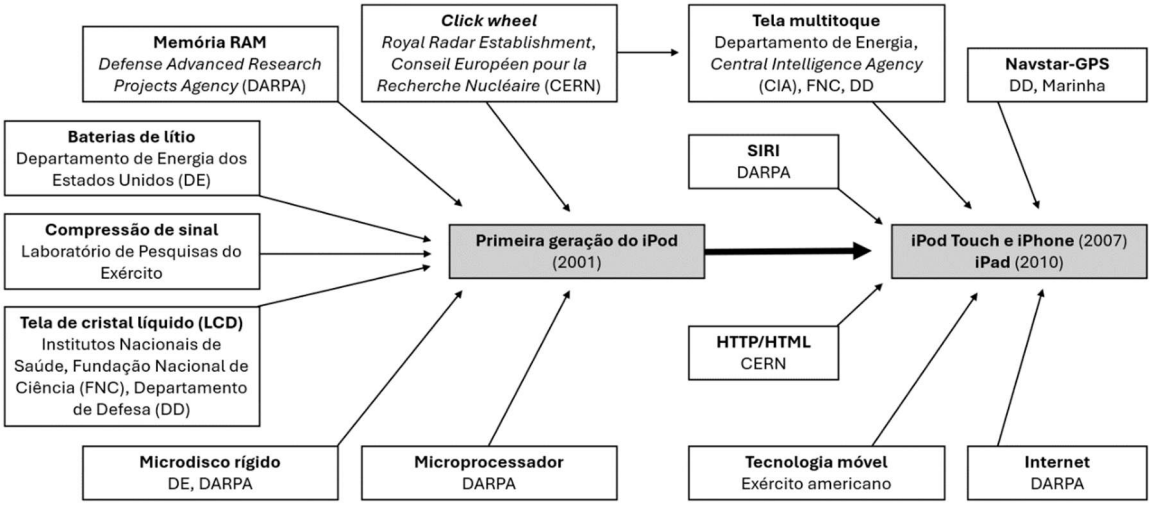
Uma manifestação categórica desse "mito do setor público *vs.* setor privado" explorada por Mazzucato (2014, cap. 5) é a narrativa que se conta sobre a Apple, tida como um dos principais modelos de empresa inovadora do Vale do Silício, a qual, graças à genialidade de seu fundador, Steve Jobs, revolucionou o mundo da tecnologia e a história dos computadores pessoais e dos *smartphones*, mudando para sempre a forma como as pessoas trabalham e se comunicam.

Entretanto, embora não se negue a genialidade de Steve Jobs e a importância da Apple na criação de produtos marcados por um *design* único e revolucionário, é preciso reconhecer que, no que se refere à inovação tecnológica em si, o mérito da Apple se restringe à mera *integração, em uma arquitetura nova, de tecnologias já existentes* (Mazzucato, 2014, p. 133).

No caso, conforme se vê no Gráfico 1 abaixo, a maioria das tecnologias por trás do iPod, do iPhone e do iPad, que fazem deles produtos fascinantes, foram pacientemente concebidas e desenvolvidas não pela iniciativa privada, mas pelo Estado. Sem tecnologias como a tela LCD, a tela *touch*, o GPS, a tecnologia móvel (celular) e a internet, o que seria dos "inovadores" produtos Apple? Até mesmo a SIRI, assistente virtual baseada em inteligência artificial, tem sua origem em um projeto de pesquisa e financiamento conduzido pelo governo dos Estados Unidos[66] – país ironicamente tido como o modelo da criação de riqueza liderada pelo setor privado (Mazzucato, 2014, p. 109).

[66] "O recurso mais recente do iPhone é um assistente pessoal virtual conhecido como SIRI. E, como a maioria dos outros recursos tecnológicos dos produtos iOS da Apple, o SIRI tem sua origem na pesquisa e no financiamento federal. O SIRI é um programa de inteligência artificial que consiste em aprendizagem de máquina, processamento de linguagem natural e um algoritmo de busca de web (Roush, 2010). Em 2000, a DARPA [*Defense Advanced Research Projects Agency* – Agência de Projetos de Pesquisa Avançada de Defesa] pediu ao Stanford Research Institute (SRI) para assumir a liderança em um projeto para desenvolver uma espécie de 'assistente virtual' para auxiliar o pessoal militar. O SRI ficou encarregado de coordenar o projeto 'Cognitive Assistant that Learns and Organizes' (CALO) [Assistente Cognitivo que Aprende e Organiza], que incluía vinte universidades americanas trabalhando para o desenvolvimento da tecnologia básica. Quando o iPhone foi lançado em 2007, o SRI reconheceu uma oportunidade para que o CALO fosse usado como um aplicativo de smartphone e decidiu comercializar a tecnologia criando uma start-up financiada com capital de risco nesse mesmo ano, a SIRI. Em 2010 a SIRI foi adquirida pela Apple por uma quantia não revelada." (Mazzucato, 2014, p. 149)

Gráfico 1. Origem dos produtos populares da Apple



Fonte: Mazzucato, 2014, p. 153.

Assim, é preciso superar os mitos existentes sobre a origem do empreendedorismo e da inovação e reconhecer que o Estado efetivamente cumpre uma função fundamental de inovação tecnológica, isto é, uma função *empreendedora*. A partir da compreensão de como as economias *realmente funcionam*, será possível formular políticas públicas alinhadas à realidade, em vez de simplesmente se perpetuar a reprodução de mitos e estereótipos sobre o papel do Estado na economia (Mazzucato, 2014, p. 39).

É nesse sentido que Lucas Amato (2022, p. 240-248) aponta cinco funções exercidas pelo Estado em uma economia de mercado:

(i) Função de garantia: função clássica de manutenção da ordem de mercado, mediante a garantia, pelo Estado, de uma competição regrada e da proteção jurídica dos direitos contratuais e de propriedade, por meio de uma organização centralizada de ameaça e imposição de sanções;

(ii) Função de regulação: disciplina administrativa ou quase-judicial do mercado, dividida em (a) regulação setorial (*ex ante*, baseada em agências reguladoras); e (b) regulação antitruste (*ex post*, voltada para o controle da concentração econômica e a defesa da concorrência);

(iii) Função de compensação: políticas contracíclicas e gasto público na forma de direitos e programas sociais;

(iv) Função de exceção direta ao mercado: pelos mecanismos de planejamento, monopólios estatais e empresas estatais; e

(v) Função de inovação do mercado: atuação positiva e proativa do Estado em relação à economia no processo de desenvolvimento econômico, aprofundando e abrindo novos mercados.

É essa quinta função do Estado na economia – de inovação do mercado – que corresponde ao "Estado empreendedor" descrito por Mazzucato. É o Estado visto não como intruso ou interventor, mas, sim, como arquiteto de novos mercados e agente catalisador de mudanças tecnológicas disruptivas, proporcionando oportunidades que virão a ser exploradas pela iniciativa privada – tal como a Apple, ao integrar em seus dispositivos as tecnologias revolucionárias concebidas e desenvolvidas pelo Estado.

2. Regulação e inovação

Se, a despeito das evidências históricas, o mito do "setor público ineficiente *vs.* setor privado inovador" ainda predomina no senso comum e na mentalidade dos formuladores de políticas públicas conservadores, observa-se também a prevalência de narrativa semelhante quando se trata da específica relação entre regulação e inovação.

Regulação e inovação são frequentemente concebidas como adversárias: a regulação representando o governo, burocracia e limites ao empreendedorismo; e a inovação associada aos mercados, à iniciativa privada e ao crescimento econômico (Wiener, 2004, p. 483). No entanto, é possível identificar duas falácias principais que sustentam essa falsa oposição necessária entre regulação e inovação.

Em primeiro lugar, o mito da "regulação *vs.* inovação" se apoia sobre uma visão da função regulatória do Estado como uma mera "correção de falhas de mercado". Essa visão deriva da ideia criticada por Mazzucato de que a inovação seria tarefa exclusiva da iniciativa privada, cabendo ao Estado intervir apenas na medida estritamente necessária para corrigir ou mitigar efeitos nocivos

decorrentes de "anomalias" (como monopólios naturais nos setores de energia elétrica e telecomunicações) ou riscos próprios de determinados setores da economia (como o risco sistêmico do setor bancário). Ir além da mera correção de falhas de mercado, assim, significaria uma intervenção indevida do Estado regulador na economia, uma intromissão que apenas prejudicaria a dinâmica do mercado que, naturalmente, sob a condução da "mão invisível", levaria à eficiência, à inovação e ao progresso econômico. A regulação, portanto, deve ser mínima, para não impedir a inovação supostamente capitaneada pelo setor privado, na forma dos agentes daquele setor regulado.

Mas há uma segunda falácia que ajuda a sustentar o falso antagonismo entre regulação e inovação – dessa vez, uma falácia própria não do pensamento econômico, mas do pensamento jurídico: trata-se da concepção da regulação sob a forma de um único modelo institucional possível (Wiener, 2004, p. 484).

Pode-se dizer que essa visão "monoinstitucionalista" da regulação corresponde a uma manifestação do que Roberto Mangabeira Unger (2004 [1996], p. 17) denomina o "fetichismo institucional": "a crença de que concepções institucionais abstratas, como a democracia política, a economia de mercado e uma sociedade civil livre, têm uma expressão institucional única, natural e necessária".

No caso, o modelo da regulação estatal tido como "natural" tende a ser identificado com uma forma de regulação direta, hierarquizada, minudente, inflexível e unilateral, "de cima para baixo" (*top down*), em que as regras estabelecidas pela agência reguladora valem universalmente para todos os agentes do setor regulado (Amato; Missagia, 2023, p. 144, 166).

Esse modelo regulatório mais repressivo – frequentemente tido como a forma "padrão" da regulação – corresponde à estratégia regulatória denominada "comando e controle". Segundo Baldwin, Cave e Lodge (2012, p. 106-107):

> The essence of command and control (C & C) regulation is the exercise of influence by imposing standards backed by criminal sanctions. Thus, the Health and Safety Executive may bring criminal prosecutions against occupiers who breach health and safety regulations. The force of law is used to prohibit certain forms of conduct, to demand some positive actions, or to lay down conditions for entry into a sector. […]

> The strengths of C & C regulation (as compared to techniques based, say, on the use of economic incentives such as taxes or subsidies) are that the force of law can be used to impose fixed standards with immediacy and to prohibit activity not conforming to such standards. In political terms, the regulator or government is seen to be acting forcefully and to be taking a clear stand: by designating some forms of behaviour as unacceptable; by excluding dangerous parties from relevant areas; by protecting the public; and establishing penalties for those engaging in offensive conduct. Som forms of behaviour can thus be outlawed completely and the ill-qualified can be stopped from practicing activities likely to produce harms. The public, as a result, can be assured that the might of the law is being used both practically and symbolically in their aid.

Muitas vezes, alega-se que "a regulação" (de comando e controle) é incompatível com os processos de inovação tecnológica por ser excessivamente rígida, unilateral, autoritária e lenta, ao passo que as novas tecnologias demandariam abertura para diálogo, experimentalismo, dinamismo e flexibilidade por parte do regulador. Mas, como "a regulação" não apresenta esses atributos, se o objetivo é estimular a inovação, a única alternativa disponível seria, simplesmente, não regular.

Hoje, esse falso dilema entre regular (sob o modelo de comando e controle) ou abster-se de regular frequentemente se faz presente nos debates nacionais e internacionais sobre a regulação da inteligência artificial. Representantes da indústria e *big techs* se opõem às propostas de regulação da tecnologia (ou tentam postergá-las ao máximo), sob a justificativa de que "a regulação" irá impedir a inovação.

Chama a atenção o caso do presidente da Argentina, o libertário Javier Milei, que quer transformar a Argentina no "quarto centro mundial de IA", prometendo uma regulamentação mínima para atrair os presidentes de companhias americanas de tecnologia, como uma forma de proteção contra os "crescentes riscos regulatórios" nos Estados Unidos e na Europa.[67] Esse posicionamento evidencia sua concepção da regulação estatal como um fator necessariamente inibidor da inovação, como se o mero fato de não regular (ou

[67] Ver reportagem do Financial Times de 11 de junho de 2024: "Javier Milei pitches Argentina as low-regulation AI hub". Disponível em: https://www.ft.com/content/90090232-7a68-4ef5-9f53-27a6bc1260cc .

regular minimamente) a tecnologia fosse por si só suficiente para atrair empresas estrangeiras para o país. Pelo contrário, conforme demonstra Mazzucato (2014), a participação proativa do Estado no desenvolvimento tecnológico e na abertura de novos mercados é que se configura como fator de avanço da inovação e do empreendedorismo (privado e público).[68]

Há, porém, uma forma de escapar desse falso dilema e superar o mito da "regulação *vs.* inovação": reconhecendo que a função regulatória do Estado não se resume a um único formato (de comando e controle), mas, ao contrário, conta com diversos modelos, estratégias e ferramentas regulatórias – já estabelecidas ou ainda por imaginar e experimentar – a serem articuladas visando o atingimento de determinado(s) objetivo(s) – incluindo o próprio objetivo de preservar ou estimular a inovação, considerado central quando se trata da regulação das inovações disruptivas (Baptista; Keller, 2016, p. 141-142).

A partir de um conceito amplo de tecnologia como "um dispositivo ou sistema para conversão de entradas (*inputs*) em saídas (*outputs*)", Wiener (2004, p. 484) propõe que a própria regulação seja compreendida como uma forma de tecnologia: "um conjunto de técnicas para alterar as funções da produção visando à geração menor de alguns resultados, como a poluição, ou maior de outros". Nesse sentido, o impacto da regulação sobre a tecnologia depende do próprio conjunto das *tecnologias regulatórias* desenvolvidas e aplicadas pelo regulador.

A questão fundamental, portanto, é compreender que não há um único modelo regulatório ideal para lidar com qualquer tecnologia em qualquer situação. As estratégias e tecnologias regulatórias apropriadas a serem utilizadas pelo regulador irão depender, em primeiro lugar, dos objetivos estipulados pelo regulador (por exemplo, reduzir a poluição, prevenir riscos bancários sistêmicos ou estimular a inovação no setor em questão), mas, também, do contexto

[68] É curioso comparar o posicionamento de Milei com um questionamento posto por Mariana Mazzucato (2014, p. 32): "Por acaso a Pfizer saiu de Sandwich, Kent (Reino Unido), e se mudou para Boston, nos Estados Unidos, devido à redução da carga tributária e à legislação mais flexível? Ou isso ocorreu porque o National Institutes of Health (NIH), do setor público, tem desembolsado cerca de 30,9 bilhões de dólares por ano nos Estados Unidos no financiamento da base de conhecimento sobre a qual empresas farmacêuticas privadas prosperam?"

econômico, social, institucional e cultural em que se está inserido (Wiener, 2004, p. 495).

Quando se trata da regulação de tecnologias disruptivas, essa abordagem regulatória dinâmica, criativa e experimental se revela ainda mais necessária, pois a inovação tecnológica é imersa em incerteza (Mazzucato, 2014, p. 66). Como os efeitos sociais, ambientais e econômicos das tecnologias disruptivas são, por natureza, imprevisíveis, é fundamental que, diante delas, o regulador tenha flexibilidade suficiente para, no momento que julgar mais adequado, aplicar os instrumentos regulatórios que façam sentido para a mitigação dos riscos decorrentes da tecnologia, sem, no entanto, inibir a inovação e seus efeitos benéficos para a sociedade.

Em linha com essas ideias, Patrícia Baptista e Clara Iglesias Keller (2016, p. 157) sugerem que

> um bom modelo de disciplina [das novas tecnologias] dependerá da combinação de mais de uma estratégia regulatória. O cardápio de ferramentas regulatórias hoje à disposição do formulador de políticas públicas é extenso. O regulador tradicional, aferrado aos padrões mais usuais do direito público (ordens, tributação, sanções), provavelmente não será bem-sucedido. É preciso inovar – também aqui – e combinar os instrumentos tradicionais com lógicas de incentivo, imposição de padrões de desempenho, autorregulação, experimentalismo etc. Enfim, regulará melhor aquele que tiver êxito em combinar melhor o *mix* de estratégias existentes de acordo com os fins regulatórios perseguidos em cada caso. Eis o desafio aos reguladores nessa área de rápidas e grandes evoluções.

Portanto, assim como Mazzucato fala em um "Estado empreendedor", devemos também reconhecer e defender a existência de um "regulador inovador"[69]: um regulador que não se deixa aprisionar em modelos arcaicos do século passado, mas que se dispõe a imaginar e implementar alternativas regulatórias criativas, construindo arranjos jurídico-institucionais dinâmicos que permitam o experimentalismo e a constante aprendizagem regulatória como forma de lidar com a complexidade inerente às tecnologias disruptivas, como a inteligência artificial.

[69] Expressão de Paixão; Aguiar; Freire, 2021.

Em linha com esse espírito experimentalista, um exemplo concreto de como o Estado também pode desempenhar sua função regulatória de forma inovadora é o recente instituto do *sandbox* regulatório.

Apesar de ter sido originalmente concebido para o setor financeiro, o *sandbox* regulatório também tem sido invocado como instrumento de apoio à inovação no âmbito da regulação da inteligência artificial. No entanto, não basta simplesmente transplantar irrefletidamente o instituto do setor financeiro para o campo da IA como se isso fosse suficiente para garantir o estímulo à inovação. Diante disso, deve-se, primeiro, buscar compreender qual seria o específico sentido de se aplicar a abordagem do *sandbox* regulatório no âmbito da regulação da IA, em comparação com a sua aplicação no setor financeiro.

3. *Sandbox* de inteligência artificial

Conforme originalmente concebido no âmbito do setor financeiro, o *sandbox* regulatório consiste em uma abordagem regulatória experimental baseada na concessão, pelo regulador ao regulado, de uma autorização especial voltada para o teste de produtos e serviços inovadores no setor. Por meio do *sandbox*,

> as regras postas podem ser mitigadas ou afastadas pelo regulador, a pedido do ente regulado participante do programa do *sandbox*, para que tal ente possa testar um produto ou serviço inovador cuja aplicação era antes impedida, dificultada ou considerada arriscada em razão das regras regulatórias vigentes. Assim, em contrapartida à flexibilização regulatória concedida pela agência reguladora para um agente regulado específico, o teste do projeto inovador ocorre em um ambiente estritamente limitado, controlado e monitorado pelo ente regulador [...]. (Amato; Missagia, 2023, p. 144)

Nesse sentido, o *sandbox* regulatório permite, por um lado, o teste de produtos inovadores em um ambiente controlado e, por outro, uma melhor comunicação e um processo de aprendizado mútuo entre regulador e regulado. Dessa forma, especialmente em setores econômicos que demandam estímulos à inovação e à concorrência, essa abordagem configura uma interessante alternativa ao modelo regulatório "tradicional" de comando e controle, cuja

lógica se baseia mais na repressão de condutas ilícitas e menos na comunicação colaborativa entre regulador e regulado.

O *sandbox* foi originalmente implementado em 2015 pela *Financial Conduct Authority* (FCA), autoridade reguladora do sistema financeiro do Reino Unido, tendo por objetivos prover um ambiente controlado em que empresas do setor financeiro possam testar seus produtos e serviços, reduzir os tempos e custos de colocação do produto no mercado, facilitar o acesso ao financiamento e dar proteção adequada aos consumidores (Financial Conduct Authority, 2022).

No Brasil, inspiradas pela experiência britânica, as três agências reguladoras do setor financeiro também instituíram seus próprios programas de *sandbox*: em 2020, a Superintendência de Seguros Privados (Susep) e o Banco Central do Brasil; e, em 2021, a Comissão de Valores Mobiliários (CVM). Posteriormente, foi introduzida a Lei Complementar nº 182, de 1º de junho de 2021, que instituiu o "marco legal das *startups* e do empreendedorismo inovador", trazendo as fundações do regime jurídico do *sandbox* regulatório no país, bem como regras gerais a serem observadas pelas agências reguladoras que desejem implementar o programa em seus respectivos setores regulados (ou seja, sua aplicação não é limitada ao setor financeiro).

Assim, desde a pioneira implementação do instituto pela FCA, o *sandbox* regulatório tem sido aplicado por reguladores de todo o mundo, sobretudo no âmbito da regulação financeira.[70] No entanto, há também muitos casos de aplicações em outros domínios. No Brasil, por exemplo, as agências reguladoras dos setores de telecomunicações, saúde a transporte já tomaram iniciativas no sentido de implementar *sandboxes* regulatórios (Moraes, 2023, p. 306). Mais do que isso, também já foram realizados experimentos para além das regulações setoriais. Marco Barros e Julia Tosatto, em capítulo desta obra, trazem o caso do *sandbox* de Foz do Iguaçu, voltado para o desenvolvimento de um bairro

[70] De acordo com relatório do Banco Mundial (World Bank, 2020), até novembro de 2020, 73 *sandboxes* regulatórios já haviam sido implementados em todo o mundo, espalhados em 57 jurisdições.

inteligente na cidade, o que ilustra a aplicação do instituto a nível da administração pública.

Tendo em vista a afinidade existente entre o *sandbox* regulatório e a inovação tecnológica, não surpreende que a sua aplicação também venha sendo invocada no âmbito da incipiente regulação da inteligência artificial. Como exemplo, na União Europeia (UE), o instituto é previsto no *AI Act*, vigente desde 1º de agosto de 2024, e, no Brasil, ele consta do ainda discutido[71] Projeto de Lei nº 2.338/2023[72]. Destaca-se que, tanto no caso da UE quanto no caso do Brasil (inspirado na UE), a abordagem geral para a regulação da IA parte do modelo denominado "regulação baseada em riscos".

Sendo assim, limitando-nos ao modelo de regulação baseada em riscos adotado na UE e atualmente discutido no Brasil, cabe indagar qual seria o específico objetivo pretendido com a aplicação do *sandbox* regulatório no âmbito da regulação da IA. É conveniente, portanto, comparar alguns aspectos da IA (e sua regulação) frente ao setor financeiro (e sua regulação), para que se possa compreender se os objetivos do *sandbox* financeiro e do *sandbox* de IA seriam os mesmos, ou se estaríamos diante de objetivos distintos.

Nesse sentido, uma diferença fundamental entre a regulação financeira e a regulação da IA (baseada em riscos) é o fato de que, na regulação financeira (como em outras regulações de caráter setorial), para que um agente possa ingressar no setor e começar a operar no mercado, oferecendo produtos ou serviços para consumidores, é necessária a obtenção de uma autorização prévia concedida pelo regulador (no caso do setor financeiro brasileiro, o Banco Central, a CVM ou a Susep). Trata-se, portanto, de uma regulação baseada na concessão de autorizações prévias para que os entes regulados possam, licitamente, atuar no setor econômico em questão (Moraes, 2023, p. 308-313).

[71] O presente capítulo foi escrito em agosto de 2024.
[72] O presente capítulo toma como referência o relatório publicado no dia 07 de junho de 2024 pela Comissão Temporária Interna sobre Inteligência Artificial no Brasil (CTIA) com uma nova proposta de texto substitutivo para o PL 2.338/2023. Disponível em: https://legis.senado.leg.br/atividade/comissoes/comissao/2629/.

Ao contrário dessa abordagem, o modelo de regulação baseada em riscos, empregado no *AI Act* e no PL 2.338/2023, não envolve a concessão de autorizações prévias pelo regulador para que os entes regulados possam atuar no mercado em questão. Não há, portanto, um controle prévio de quem pode ou não fazer parte do "setor" de IA. Em vez disso, nessa abordagem, são previstas diversas categorias de riscos relacionados a diferentes usos da IA, que variam desde riscos mais baixos até riscos excessivos e inaceitáveis, às quais correspondem diferentes níveis de obrigações a serem observadas pelo regulado. Assim, demanda-se que, antes do lançamento no mercado, o próprio ente regulado faça uma avaliação preliminar da sua tecnologia, a fim de enquadrá-la em alguma daquelas categorias. A depender da classificação de risco imputada ao sistema de IA em questão, o regulado deverá observar um ou outro conjunto de regras aplicáveis ao seu produto.

É preciso levar em conta, portanto, essa diferença fundamental entre a regulação financeira e a regulação da IA: enquanto a primeira envolve a necessidade de obtenção de uma autorização prévia para atuar no setor, a segunda dispensa qualquer licença prévia, requerendo, porém, que os próprios agentes façam uma autoavaliação preliminar sobre a categoria de risco em que sua tecnologia se enquadra.

Essa diferença em relação ao setor financeiro não é arbitrária ou acidental, mas decorre da própria natureza da IA. Diferentemente dos setores financeiro, de energia, saúde, telecomunicações, transportes ou saneamento básico, a IA não constitui propriamente um *setor econômico*. Trata-se, na verdade, de uma tecnologia *transetorial*, aplicável a todo e qualquer domínio. Ela é, nesse sentido, o que se chama de "tecnologia de propósito geral" (*general purpose technology – GPT*): "tecnologias-chave, [que] moldam toda uma era e reorientam as inovações nos setores de aplicação, como a máquina a vapor, a eletricidade e o computador" (Kaufman, 2022, p. 22).

Essa constatação já é suficiente para se concluir que não faz sentido que um *sandbox* de IA vise à redução de barreiras à entrada no mercado, objetivo do *sandbox* financeiro.

Isso porque essas "barreiras à entrada no mercado" são, por assim dizer, uma espécie de externalidade negativa gerada pelo próprio modelo regulatório baseado em autorizações. Na medida em que se impõe uma série de condições rigorosas para que uma instituição financeira possa obter uma autorização para se instalar no mercado, muitas vezes, agentes com propostas inovadoras se veem impossibilitados de beneficiar os consumidores pelo fato de não conseguirem atender àquelas condições prévias para operar no setor.

Com o regime do *sandbox* regulatório, essa externalidade negativa gerada pela regulação (tradicional) é mitigada pela própria regulação (alternativa), na medida em que o regulador concede ao regulado uma autorização temporária, de caráter precário, voltada tão somente para o teste do produto ou serviço inovador dentro das condições experimentais estabelecidas pelo regulador. O *sandbox* regulatório no setor financeiro, portanto, consiste basicamente na concessão de uma autorização especial para se testar alguma inovação. Ao final do teste, se bem-sucedido, o regulador poderá converter a licença temporária em licença definitiva, permitindo ao regulado oferecer seu produto ou serviço ao mercado em geral.

Ora, conforme mencionado, a abordagem regulatória baseada em riscos, aplicada na regulação da IA tanto no *AI Act* quanto no PL 2.338/2023, não envolve qualquer concessão de autorização prévia por parte do regulador para que um agente possa atuar no mercado. Sendo assim, um *sandbox* de IA não poderia ter como função "reduzir barreiras regulatórias à entrada de agentes no mercado", porque, no caso da IA, essas barreiras regulatórias (consistentes nas condições exigidas para a obtenção da autorização regulatória) sequer existem.

Se o *sandbox* regulatório, conforme concebido para a regulação do setor financeiro, não cumpre sua função original quando transplantando para a regulação da IA, qual seria um possível sentido para a implementação de *sandboxes* regulatórios de IA? Por que um desenvolvedor de IA teria interesse em se candidatar a um programa de *sandbox*, já que não ele depende de autorizações para testar seu produto?

Em setembro de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) divulgou estudo técnico para subsidiar a implementação, pela ANPD, de *sandbox* relacionado à regulação de tecnologias emergentes, em especial a inteligência artificial. No referido estudo, são apontados exemplos de "*sandboxes* de privacidade" desenvolvidos por autoridades de proteção de dados de diferentes países, tais como a *Information Commissioner's Office* do Reino Unido, a *Datatilsynet* da Noruega, a *Superintendencia de Industria y Comercio* da Colômbia e a *Personal Data Protection Commission* de Singapura.

Assim como o modelo regulatório adotado no *AI Act* e proposto no PL 2.338/2023, as legislações de proteção de dados são normalmente baseadas em categorias de riscos (Moraes, 2023, p. 311). O estudo da ANPD, assim, destaca que, em contraste com *sandboxes* financeiros, os referidos programas de *sandbox* de privacidade "não realizaram a suspensão temporária de sanções", sugerindo-se que "o afastamento de normas para fins de sanção nem sempre é necessário [para um programa de *sandbox*], uma vez que o foco do programa se concentra na implementação do princípio da responsabilidade e prestação de contas (...) e no fomento do *privacy by design* (...)", conceito que remonta a uma abordagem para o desenvolvimento de tecnologias por meio da qual "a privacidade deve ser incorporada diretamente ao projeto e à operação de tecnologias da informação, práticas comerciais e infraestruturas de rede" (Moraes 2023, p. 311).

Nesse sentido, do ponto de vista do regulado, o interesse por um *sandbox* de IA decorre do fato de que, em um modelo de regulação baseada em riscos, uma das principais preocupações do agente de mercado é, justamente, identificar os riscos associados ao produto desenvolvido e tomar medidas assertivas para mitigá-los. Cabe a ele próprio realizar essa avaliação para que saiba quais medidas tomar e qual conjunto de regras observar. Frequentemente, porém, não é fácil identificar os efeitos da tecnologia com clareza. Aliás, não é exagero dizer que a era da IA está apenas começando. Muitos dos impactos decorrentes de diferentes aplicações da IA ainda são incertos e só serão descobertos no longo prazo.

Não bastasse essa dificuldade de prever os riscos decorrentes de diferentes aplicações da IA, é agravante o fato de que, muitas vezes, esses riscos representam ameaças a direitos humanos fundamentais. Kaufman, Junquilho e Reis (2023) sugerem que alguns desses riscos são *intrínsecos* à tecnologia, demonstrando como a IA, por sua própria natureza, afeta os direitos fundamentais à explicabilidade[73] (derivado do direito ao devido processo legal), à não discriminação[74] (derivado da igualdade perante a lei) e à privacidade[75]. Segundo as autoras, como tais riscos decorrem de características inerentes à tecnologia, os esforços regulatórios pela eliminação desses riscos muitas vezes esbarram nos limites da própria técnica. Não obstante, mesmo que sistemas de IA não cheguem a ser plenamente interpretáveis, transparentes, não enviesados ou respeitadores da privacidade dos usuários, é preciso persistir na mitigação desses efeitos nocivos, tanto quanto possível. Essa é uma exigência não só dos reguladores, mas da própria sociedade civil (Smuha, 2021, p. 73).

Um *sandbox* de IA, assim, ao possibilitar que regulador e regulado mantenham uma comunicação colaborativa constante em torno do teste controlado de alguma inovação pelo ente regulado, permite que este tenha uma

---

[73] O risco da IA ao direito à explicabilidade decorre do chamado problema da "interpretabilidade": o processo como os algoritmos correlacionam os dados e definem os parâmetros é de uma complexidade tão grande que a cognição humana é incapaz de compreendê-lo. Em outras palavras, não é possível saber ao certo as "razões" do algoritmo pelas quais determinados *inputs* (entradas) geraram determinado *output* (resultado). Nesse sentido, o algoritmo é opaco – é o que se chama de "*black box*". Esse processo de transformação de *inputs* em *outputs* é muito abstrato, e essa complexidade tende a crescer com os avanços da capacidade computacional e do *big data*. Para agravar, existe um *trade-off* entre precisão e transparência, de forma que medidas voltadas para aumentar a interpretabilidade dos processos do algoritmo tendem a ter como efeito uma queda na precisão dos seus resultados (Kaufman; Junquilho; Reis, 2023, p. 52-54).

[74] Há várias origens possíveis para o risco da IA ao direito à não discriminação. Vieses discriminatórios presentes nos *outputs* da IA podem decorrer dos próprios dados de treinamento, quando não representam adequadamente a população-alvo (ex.: mais imagens de homens brancos, quando a população de um país é majoritariamente de mulheres negras), do processo de coleta de dados, da preparação das bases de dados, além da própria subjetividade humana ao longo do desenvolvimento e uso do sistema de IA, dentre outras possíveis origens. Os vieses algorítmicos, seja qual for a sua origem do ponto de vista técnico, reforçam preconceitos sociais e mantêm minorias sociais em situação de injustiça (Kaufman; Junquilho; Reis, 2023, p. 56-58).

[75] O limite ao direito à privacidade não é estritamente técnico, diferentemente dos outros casos. Afinal, os algoritmos não são inerentemente processadores de dados pessoais. Porém, fato é que sistemas baseados em IA têm sido largamente usados para processamento de dados pessoais, muitas vezes sem o devido consentimento dos usuários (Kaufman; Junquilho; Reis, 2023, p. 61-62).

espécie de "consultoria regulatória" sobre os padrões éticos e legais a serem observados e implementados na tecnologia ao longo de seu desenvolvimento. Com isso, o regulado tem o apoio do próprio regulador acerca de medidas a serem tomadas para que o sistema de IA seja desde o início concebido como um produto aderente aos padrões éticos e legais exigidos não só pela regulação, mas também pela sociedade.

Mas o escopo de um *sandbox* de IA não se limita apenas ao *privacy by design* e ao fomento à inovação responsável em IA. Em outubro de 2023, a ANPD abriu consulta pública propondo a implementação do *sandbox* de IA no Brasil, elencando ainda outros objetivos: (i) promover a transparência algorítmica, buscando tornar o funcionamento interno dos sistemas de IA e seus processos de tomada de decisão compreensíveis e explicáveis; (ii) estabelecer um ambiente multissetorial, reunindo agentes interessados de vários setores da sociedade, como pesquisadores, desenvolvedores, representantes da indústria, organizações da sociedade civil e órgãos reguladores, a fim de se promoverem diálogos multissetoriais que poderão ajudar no constante aprimoramento da regulação e das práticas de mercado; e (iii) auxiliar no desenvolvimento de parâmetros para intervenção humana em processos de decisão automatizados, especificamente para sistemas de IA classificados como de alto risco.

Em suma, nota-se que, diferentemente do caso do *sandbox* financeiro, o objetivo principal do regulador de IA não seria estimular a concorrência mediante a flexibilização regulatória, mas, sim, fomentar o *privacy by design* e a inovação responsável (Moraes, 2023, p. 310-313). Na medida em que sistemas de IA éticos, legal e socialmente responsáveis são mais bem aceitos pelo mercado e pela sociedade, cria-se um incentivo para que agentes desenvolvedores da tecnologia tenham interesse em participar de programas de *sandbox* de IA, tendo a oportunidade de receber o apoio do regulador para o desenvolvimento de sistemas menos propensos a gerar aqueles riscos que a regulação procura inibir.

Com a breve análise feita até aqui acerca dos objetivos de um *sandbox* de IA, espera-se, enfim, ter demonstrado, a partir de um exemplo prático, como o Estado pode assumir uma postura de estímulo à inovação tecnológica

(responsável) até mesmo no exercício de sua função regulatória. Para isso, porém, precisa também o regulador inovar nas técnicas regulatórias empregadas, pois os modelos regulatórios tradicionais, em especial a abordagem de comando e controle, de fato não foram pensados para lidar com dinâmicas tão aceleradas, incertas e complexas como é o caso da IA. O *sandbox* regulatório, técnica regulatória inovadora, experimental e criativa, poderá conferir segurança jurídica para o teste de novos produtos e serviços baseados em IA ao mesmo tempo em que estimula a inovação ética e socialmente responsável, tudo isso em um ambiente de mútua colaboração e constante aprendizagem regulatória.

Todavia, a colaboração entre o regulador e a iniciativa privada no processo de inovação tecnológica não deve se reduzir apenas a essa ferramenta, até porque *sandboxes* regulatórios são muito intensivos no uso de recursos humanos do regulador, de forma que sua aplicação deve ser planejada com cautela (Paixão; Aguiar; Ragazzo, 2021, p. 35). Há diversas outras iniciativas regulatórias que podem e devem ser tomadas para se fomentar a construção de um profícuo ecossistema de inovação de IA no país.

4. Outras inovações regulatórias

O regulador da IA poderá se inspirar em outras inovações regulatórias já experimentadas em outros setores regulados, tanto dentro quanto fora do país.

O Banco Central do Brasil, no âmbito da Agenda BC#, tem tomado nos últimos anos uma série de ações estratégicas visando o estímulo à inovação tecnológica e a construção de um ecossistema descentralizado de inovação financeira no Brasil. Além do próprio *sandbox* regulatório do Banco Central, instituído em outubro de 2020, Paixão, Aguiar e Ragazzo (2021, p. 39-48) discorrem sobre a iniciativa do *sandbox* setorial, na forma do Laboratório de Inovações Financeiras e Tecnológicas (LIFT).

Segundo os autores, um *sandbox* setorial diferencia-se de um *sandbox* regulatório nos seguintes aspectos:

Tabela 1 – Diferenças entre *sandbox* setorial e *sandbox* regulatório

Sandbox setorial da indústria financeira	*Sandbox* regulatória
Tem objetivo de criar um espaço para *fintechs*, empresas estabelecidas (financeiras, tecnologia) e regulador colaborarem em novos produtos financeiros da fase de concepção até protótipo num ambiente virtual de testes fora de mercado e sem consumidores. Não há implicações regulatórias em testes fora de mercado, portanto não há necessidade de uma estrutura regulatória customizada.	A *sandbox* regulatória cria um espaço seguro onde *fintechs* (ou mesmo iniciativas de empresas licenciadas, como bancos) e um número limitado de consumidores reais interagem num teste de mercado. Alguns requerimentos regulatórios podem ser atenuados para criar um ambiente customizado pela duração do teste onde determinadas exigências regulatórias não se aplicam.
O acesso em geral não possui um processo regulado e restrito, onde a entrada ocorre pela aderência da proposta ao sistema financeiro local e ao interesse dos demais participantes do arranjo.	O acesso é baseado em um procedimento regulado e bem definido. As firmas devem atender aos critérios de eligibilidade do regulador, e aquelas ainda não autorizadas precisarão de licença prévia (mesmo precária) para teste.
Os recursos necessários (humanos, tecnológicos) à execução de um projeto – são compartilhados entre os participantes, tornando a iniciativa inerentemente escalável.	Os recursos das iniciativas de *sandboxes* regulatórias vêm unicamente dos reguladores respectivos e dos proponentes da iniciativa. O regulador em geral aloca recursos humanos para acompanhar e monitorar a iniciativa. Os recursos financeiros e tecnológicos necessários cabem ao proponente da iniciativa.

Fonte: Paixão; Aguiar; Ragazzo, 2021, p. 41.

Nota-se que o *sandbox* setorial não envolve flexibilização regulatória, mas, sim, a criação de um ambiente colaborativo que estimule o diálogo, experimentação e amadurecimento de ideias entre diversos atores do setor financeiro. O Laboratório de Inovações Financeiras e Tecnológicas (LIFT), anunciado pelo Banco Central em maio de 2018, é um exemplo de *sandbox* setorial aplicado no setor financeiro brasileiro – o qual, aliás, ganhou em 2019 o *Central Banking Award* de melhor iniciativa de *sandbox* do mundo (mesmo se tratando de um *sandbox* setorial, e não regulatório) (Paixão, 2019).

Considerando que um dos principais problemas enfrentados por reguladores no Brasil é a falta de recursos financeiros e humanos, o *sandbox* setorial se apresenta como ferramenta interessante na medida em que se baseia sobretudo na colaboração entre os próprios participantes do ambiente, não requerendo a utilização de recursos do regulado (Paixão; Aguiar; Ragazzo, 2021, p. 42).

Se concebido também para a regulação da IA, o *sandbox* setorial poderá vir a constituir, ao lado de outras ferramentas regulatórias a serem empregadas,

> mais um dos componentes em um ecossistema de inovação que permite a experimentação de modelos de negócios, o uso avançado de tecnologia e a apreciação crítica do agente regulador e dos provedores de tecnologia em relação aos elementos de conformidade normativa, aderência tecnológica e balanço de benefícios e riscos dos casos de uso de negócio. (Paixão; Aguiar; Ragazzo, 2021, p. 42)

Além do ambiente colaborativo do LIFT, também foi criado o programa de formação multidisciplinar denominado LIFT Learning, que, além de acelerar projetos de inovação financeira, aproxima a academia e entidades de ensino ao desenvolvimento de soluções voltadas para o mercado, fomentando o empreendedorismo, a criação de *fintechs* por estudantes e a descentralização do ecossistema de inovação financeira no Brasil (Paixão; Aguiar; Ragazzo, 2021, p. 46-47). O programa funciona da seguinte forma:

> O LIFT Learning é centrado em uma universidade tendo um professor como coordenador. Esse coordenador, juntamente com o Banco Central e a Fenasbac, escolhem projetos de *fintechs* e bancos em conformidade com a agenda de desenvolvimento do Banco Central, a agenda BC#. O professor, então, pareia equipes de estudantes universitários com as empresas, que disponibilizam um gerente de projetos dedicado para acompanhar os estudantes.
> Ao final desse tempo espera-se que os estudantes consigam propor ideias de *fintechs* em editais de inovação ou, até mesmo, servir de mão de obra para *startups* financeiras já existentes. É, portanto, além de um programa desenvolvedor de projetos, uma experiência formadora de profissionais para o setor. (Paixão; Aguiar; Ragazzo, 2021, p. 45)

É fundamental que iniciativas regulatórias criativas como o *sandbox* setorial do LIFT e o programa LIFT Learning, além de várias outras medidas tomadas pelo Banco Central para estimular a inovação tecnológica no setor financeiro, sirvam de inspiração para a regulação da IA no país, em que o objetivo de fomento à inovação (responsável) deve ser efetivamente institucionalizado.

Para além desses exemplos, é possível citar também outras abordagens regulatórias experimentais elencadas pela ANPD em seu estudo técnico de 2023 sobre *sandbox* de privacidade. São elas: (i) camas de testagem de inovações (*innovation test beds*); (ii) centros de inovação (*innovation hubs*); (iii) cláusulas de

caducidade (*sunset provision*); (iv) *datathons* e *hackatons*; e (v) prototipagem de políticas (*policy prototyping*).

Mais importante é ter em mente que o número de ferramentas regulatórias à disposição do regulador não é finito. Diante dos desafios diariamente apresentados aos reguladores pelas tecnologias disruptivas como a IA, é preciso manter a visão crítica, a postura pragmática e a imaginação institucional em constante exercício para o desenvolvimento de arranjos regulatórios dinâmicos e aptos a lidar de forma eficiente com as novas tecnologias.

Considerações finais

A relação entre regulação e inovação é complexa e dinâmica, e não há solução ideal que resolva o tão mencionado balanço entre minimizar os riscos da tecnologia e maximizar os seus benefícios. O modelo regulatório ideal de hoje amanhã não o será mais, porque o progresso tecnológico, cada vez mais intensamente, causa a disrupção de paradigmas sociais, revolucionando a economia de dentro para fora.

Entretanto, em meio à torrente de incerteza provocada pelas tecnologias disruptivas, talvez possamos nos abraçar a uma ideia: o direito só conseguirá lidar de forma eficiente e fecunda com as novas tecnologias caso também incorpore esse espírito disruptivo, experimentalista e inovador.

O fato de a regulação ser frequentemente considerada adversária da inovação é consequência da noção, arraigada no fetichismo institucional, de que "a regulação" corresponderia, naturalmente, ao modelo de comando e controle, mais rígido, unilateral e repressivo. É preciso romper com essa visão de mundo segundo a qual instituições seriam "como objetos naturais, forçando-se sobre nossa consciência com força insistente e lembrando-nos de que nascemos num mundo que não é nosso" (Unger, 2020, p. 15). A inovação é bem-vinda não apenas no campo da tecnologia, mas também no das instituições.

O *sandbox* regulatório, instituto brevemente analisado neste capítulo, é exemplo da postura inovadora que o regulador pode e deve adotar. No caso da regulação da IA, dado o modelo regulatório baseado em riscos, o *sandbox* é capaz

de estimular a inovação baseada em IA ética e socialmente responsável, mediante o estabelecimento de uma comunicação colaborativa entre regulador e regulado em torno dos riscos envolvidos na tecnologia. Sua aplicação, adaptada do modelo financeiro, é bem-vinda no âmbito da regulação da IA – mas deve-se sempre ter em mente que a mera instituição de *sandboxes* regulatórios, por si só, não é suficiente para a criação de um ambiente regulatório propício para a inovação tecnológica.

Enfim, independentemente do modelo regulatório para a IA que venha a ser implementado no Brasil, é preciso seguir imaginando e implementando iniciativas regulatórias inovadoras, tais como o LIFT do Banco Central e outras abordagens regulatórias experimentais, visando à construção de um pujante ecossistema empresarial-tecnológico-regulatório para a inovação baseada em IA no país.

Referências

AMATO, Lucas Fucci. **Propriedade desagregada e empreendedorismo democrático:** instituições da economia de mercado e formas jurídicas do capital. Porto Alegre: Fi, 2022. Disponível em: https://www.editorafi.org/436propriedade . Acesso em 3 out. 2024.

AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Ambientes regulatórios experimentais: o sandbox no sistema financeiro brasileiro. **Revista Brasileira de Sociologia do Direito**, v. 10, n. 3, p. 143-171, 2023. Disponível em: https://revista.abrasd.com.br/index.php/rbsd/article/view/747/345 . Acesso em 3 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ***Sandbox* regulatório – estudo técnico ANPD.** 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/sandbox_regulatorio___estudo_tecnico__versao_publica_.pdf/view. Acesso em: 24 ago. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS; BANCO DE DESENVOLVIMENTO DA AMÉRICA LATINA E CARIBE. **Consulta à**

sociedade – *sandbox* regulatório de IA. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-a-sociedade-sobre-sandbox-regulatorio-de-inteligencia-artificial-e-protecao-de-dados-pessoais-no-brasil . Acesso em: 24 ago. 2024.

BACKHOUSE, Roger E. **The Penguin history of Economics.** London: Penguin Books, 2002.

BALDWIN, Robert; CAVE, Martin; LODGE, Martin. **Understanding regulation:** theory, strategy, and practice. 2 ed. Oxford: Oxford University Press, 2012.

BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. **Revista de Direito Administrativo – RDA**, v. 273, p. 123-163, 2016.

FINANCIAL CONDUCT AUTHORITY (United Kingdom). **Regulatory Sandbox.** 2022. Disponível em: https://www.fca.org.uk/firms/innovation/regulatory-sandbox . Acesso em: 24 ago. 2024.

KAUFMAN, Dora. **A inteligência artificial irá suplantar a inteligência humana?** Barueri: Estação das Letras e Cores, 2019.

KAUFMAN, Dora. **Desmistificando a inteligência artificial.** Belo Horizonte: Autêntica, 2022.

KAUFMAN, Dora; JUNQUILHO, Tainá; REIS, Priscila. Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e dos direitos humanos. **Revista de Direitos e Garantias Fundamentais**, v. 24, n. 3, p. 43-71, 2023.

MAZZUCATO, Mariana. **O Estado empreendedor:** desmascarando o mito do setor público *vs.* setor privado. Tradução de Elvira Serapicos. 1 ed. São Paulo: Portfolio-Penguin, 2014.

MORAES, Thiago. Regulatory sandboxes as tools for ethical and responsible innovation of artificial intelligence and their synergies with responsive regulation. *In:* BELLI, Luca; GASPAR, Walter B. (eds.). **The quest for AI sovereignty, transparency and accountability:** official outcome of the UN IGF Data and Artificial Intelligence Governance Coalition. Rio de Janeiro: Internet Governance Forum (IGF): FGV Direito Rio, 2023. p. 303-324.

PAIXÃO, Ricardo Fernandes. Banco Central ganha prêmio de melhor iniciativa de sandbox do mundo. **Jota**, 04 de setembro de 2019. Disponível em: < https://www.jota.info/coberturas-especiais/inova-e-acao/banco-central-ganha-premio-de-melhor-iniciativa-de-sandbox-do-mundo . Acesso em: 24 ago. 2024.

PAIXÃO, Ricardo Fernandes; AGUIAR, João Benício; FREIRE, Thiago Nogueira. Construindo uma comunidade de Fintechs. *In*: PAIXÃO, Ricardo Fernandes; AGUIAR, João Benício; RAGAZZO, Carlos (coords.). **O regulador inovador:** Banco Central e a agenda de incentivo à inovação. São Paulo: Instituto ProPague, 2021. p. 21-48.

SCHUMPETER, Joseph A. **The theory of economic development:** an inquiry into profits, capital, credit, interest, and the business cycle. Tradução de Redvers Opie. New Brunswick: Transaction Publishers, 1983 [1934].

SCHUMPETER, Joseph A. **Capitalismo, socialismo e democracia.** Tradução de Luiz Antônio Oliveira de Araújo. São Paulo: Editora da Unesp, 2017 [1942].

SMUHA, Nathalie A. From a "race to AI" to a "race to AI regulation": regulatory competition for artificial intelligence. **Law, Innovation and Technology**, v. 13, n. 1, p. 57-84, 2021.

UNGER, Roberto Mangabeira. **O direito e o futuro da democracia.** Tradução de Caio Farah Rodriguez e Marcio Soares Grandchamp. São Paulo: Boitempo, 2004 [1996].

UNGER, Roberto Mangabeira. **O homem despertado:** imaginação e esperança. Tradução de Roberto Muggiati. Rio de Janeiro: Civilização Brasileira, 2020.

WIENER, Jonathan B. The regulation of technology, and the technology of regulation. **Technology in Society**, v. 26, p. 483-500, 2004.

WORLD BANK. **Key Data from Regulatory Sandboxes across the Globe.** 2020. Disponível em: https://www.worldbank.org/en/topic/fintech/brief/key-data-from-regulatory-sandboxes-across-the-globe . Acesso em: 24 ago. 2024.

6. Diretrizes para a regulamentação da inteligência artificial: responsabilidade jurídica na era do algoritmo[76]

Carolina Stange Azevedo Moulin[77]

Nota metodológica

A intersecção entre direito e inteligência artificial abrange dois aspectos de maneira mais imediata. A aplicação de ferramentas computacionais para aumentar a eficiência do desempenho de operadores do direito, escritórios de advocacia, tribunais e órgãos legislativos e administrativos é frequentemente designada como "Inteligência Artificial para o Direito" ou "IA e Direito". Esse campo do conhecimento tem como objetivo aplicar tecnologia orientada por inteligência artificial para coletar, extrair e processar informações de textos jurídicos, otimizando a análise de grande número de documentos. Nesse sentido, as *lawtechs* – startups que utilizam tecnologia de IA para prestar serviços jurídicos – geralmente em parceria como universidades e centros de pesquisa, suprem a demanda dos setores público e privado por automação de atividades que exigem processamento massivo de informações na prática jurídica. Por outro lado, a pesquisa focada na criação e interpretação de normas jurídicas para regular o uso da inteligência artificial, "Direito da Inteligência Artificial" ou "Direito da IA", busca entender as implicações éticas, sociais, econômicas, culturais e jurídicas do desenvolvimento de algoritmos autônomos de tomada de decisão.

---

[76] Versão modificada de capítulo originalmente publicado em inglês: MOULIN, C. S. A. Guidelines for the regulation of Artificial Intelligence: reshaping liability in the algorithm era. In: *Norma, linguagem e teoria do direito: reflexões para a compreensão do direito do século XXI* [livro eletrônico] / Organizadores Arnaldo Bastos Santos Neto e Geraldo Henrique Costa Barbosa de Almeida. 1. Ed. Goiânia: Editora Espaço Acadêmico, 2020, pp. 103-118.

[77] Doutora em Direito pela Universidade de São Paulo e em Ciências Sociais pela Universidade de Osnabrück. Graduada em Direito pela Universidade Federal do Espírito Santo.

Intrinsecamente interdisciplinar, o ramo do Direito de IA pode ser dividido em seis tópicos principais:[78] (i) personalidade jurídica de humanos e não humanos; (ii) IA e obrigações contratuais; (iii) IA e propriedade intelectual; (iv) IA e responsabilidade civil; (v) IA e proteção de dados e (vi) direito comparado de IA. Este capítulo se enquadra dentro da abordagem do Direito da IA, uma vez que seu objetivo é avançar reflexões sobre a regulamentação da aplicação da tecnologia de IA. Mais especificamente, o presente texto enfrenta a questão de como apreender a categoria de responsabilidade civil quando se trata de atos ilícitos "cometidos" por algoritmos.

1. Introdução

De carros a armas autônomas, do Chat GPT ao Watson da IBM, do mecanismo de busca do Google às configurações de recomendação do Spotify e da Netflix, a inteligência artificial está cada vez mais presente no cotidiano das pessoas. As ferramentas de aprendizado computacional são usadas para uma vasta gama de atividades cognitivas: diagnóstico médico, marketing personalizado, técnicas de vigilância automatizada, consultoria de investimentos financeiros, busca de informações, direção de veículos, monitoramento do comportamento do consumidor, logística de transporte, entrega de produtos, programação e execução de processos de produção industrial.

Enquanto tais tecnologias indubitavelmente têm o potencial de facilitar e melhorar a vida humana, também apresentam problemas substanciais. Algumas aplicações da IA são eticamente questionáveis, potencialmente perigosas ou colocam desafios sistêmicos. Se a IA tornará a sociedade mais eficiente e mais segura ou se será uma ameaça à civilização depende de como lidaremos com a oportunidade histórica de moldar essas ferramentas. À medida que a aplicabilidade de IA cresce exponencialmente, aumenta também a importância de se pensar em respostas práticas para os dilemas éticos e legais apresentados por sua implementação.

[78] LAWGORITHM. What is Lawgorithm? Disponível em: <https://lawgorithm.com.br/en/about-us/>. Acesso em: 06/03/2020.

Um policial da Califórnia parou um carro autônomo do Google por dirigir muito devagar e atrapalhar o trânsito.[79] Quem o policial deve multar: o passageiro, o proprietário, o programador, o computador do carro ou o Google? Empresas de tecnologia enfrentam alegações de que seu mecanismo de busca descrimina mulheres ao exibir anúncios de empregos bem remunerados com menos frequência do que para homens.[80] Quem deve ser responsabilizado pela discriminação causada por algoritmos tendenciosos? Houve intenção? Situações como as descritas acima levantam questões sobre a responsabilidade civil por atos ilegais resultantes de ações de algoritmos.

O uso maciço da IA também gera desafios econômicos e sociais com relação à transformação do mercado de trabalho. A primeira onda de substituição de mão de obra humana por máquinas ocorreu durante a revolução industrial no final do século XVIII e início do século XIX, quando os motores mecânicos substituíram as pessoas no trabalho manual. A automação do século XXI, no entanto, tem potencial ainda mais profundo do que o anterior, uma vez que os algoritmos agora estão superando pessoas no que sempre foi um diferencial humano: tarefas cognitivas.

Que medidas os governos colocarão em prática para minimizar os efeitos adversos do desemprego em massa resultante da automação? Um software, escrito por alguns programadores, faz o trabalho que antes era realizado por várias centenas de milhares de pessoas. As mudanças no mercado de trabalho estão acontecendo tão rapidamente que oferecer cursos de recolocação profissional pode não ser suficiente: por exemplo, quando um ex-motorista de 50 anos, substituído por veículos autônomos, concluir um curso de marketing digital oferecido pelo governo, os algoritmos já poderão ter substituído também as profissões de publicidade. O software pode se sobrepor até mesmo ao trabalho dos próprios programadores: os novos desenvolvimentos em IA tornam possível

[79] MELVIN, Don. Cop pull over Google self-driving car, finds no driver to ticket. CNN. [2015]. Disponível em: <https://edition.cnn.com/2015/11/13/us/google-self-driving-car-pulled-over/>.Acesso em 09/12/2018.

[80] BROWN, Kristen V. Google showed woman ads for lower paying jobs. SPLINTER. [2015]. Disponível em: <https://splinternews.com/google-showed-women-ads-for-lower-paying-jobs-1793848970>. Acesso em: 09/12/2018.

softwares que programam outros softwares. Dadas essas circunstâncias, como seria uma sociedade sem emprego? Se a desigualdade de renda atingirá níveis nunca antes vistos ou se a humanidade alcançará um padrão de prosperidade sem precedentes, isso dependerá das estruturas jurídicas, sociais e econômicas que os governos e a sociedade civil construirão para lidar com a distribuição da riqueza produzida pela IA.

2. Definição de IA: características, benefícios e riscos

Há muitos mal-entendidos sobre a definição de inteligência artificial. A IA é constantemente retratada em filmes e livros como robôs semelhantes a humanos que subitamente adquirem consciência, tornam-se malévolos e tentam destruir a humanidade. A realidade, entretanto, é totalmente diferente.

A IA pode ser definida como a atividade dedicada a tornar as máquinas inteligentes, considerando inteligência a qualidade que permite uma entidade funcionar adequadamente e em previsão a seu ambiente.[81] A expressão foi cunhada pela primeira vez por John McCarthy em 1956, quando ele descreveu a inteligência artificial como a "ciência e engenharia de fazer máquinas inteligentes".[82] Assim como a inteligência humana, a inteligência das máquinas está ligada à capacidade de pensar de forma autônoma, processando e relacionando informações, em um sistema de entrada e saída que permite acumular aprendizado e prever padrões futuros.

Especialistas dividem a IA em duas categorias: IA restrita (ou IA fraca) e IA geral (ou IA forte). Enquanto a IA restrita é projetada para executar uma tarefa limitada (por exemplo, apenas reconhecimento facial ou apenas pesquisas na

[81] ETZIONI, Amitai; EZTIONI, Oren. Should artificial intelligence be regulated? (June 27, 2017). Issues in Science and Technology. Disponível em:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993506>. Acesso em: 08/12/2018.
[82] PEART, Andy. Homage to John McCarthy, the father of Artificial Intelligence. [2017]. Disponível em: <https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence>. Acesso em: 09/12/2018.

Internet ou apenas dirigir um carro), a IA geral é programada para executar várias funções cognitivas.[83]

Tanto a IA restrita quanto a geral compartilham três características:[84] (i) autonomia considerável; (b) alta opacidade; e (c) capacidade de aprender. A tecnologia orientada por IA é considerada autônoma porque pode fazer várias escolhas por conta própria. Esses instrumentos usam algoritmos complexos para responder às entradas ambientais independentemente da entrada humana em tempo real. A opacidade dos sistemas de IA decorre de três fatores: (i) opacidade intencional (o proprietário do código quer manter os algoritmos em segredo); (ii) incapacidade técnica (a complexidade e a função dos algoritmos estão além da compreensão da maioria das pessoas); ou (iii) escala de aplicação (a tomada de decisão autônoma pela máquina ou o número de programadores envolvidos, ou ambos, gera um algoritmo opaco até mesmo para os programadores). Por fim, capacidade de aprender significa que os instrumentos de IA analisam continuamente as condições ambiente em constante mudança e modificam suas diretrizes internas de acordo com elas.

Os benefícios e as vantagens da aplicação da IA em várias atividades são enormes. No entanto, se deixada em um vácuo normativo, a tecnologia impulsionada pela IA também pode oferecer riscos significativos. Dada a existência de vários tipos e níveis de IA, para estruturar adequadamente uma base sólida para sua regulamentação, é essencial ter em mente as diferenças entre eles. Carros sem motorista e armas autônomas, embora operem sob a mesma lógica de aprendizado de máquina, não oferecem o mesmo risco à sociedade. Portanto, seria insensato proibir estritamente a IA por causa de bots assassinos e, da mesma forma, adiar a necessidade urgente de regulamentar o uso cotidiano da IA alegando que algumas aplicações da tecnologia são inofensivas. Apesar das particularidades de cada aplicação de IA, a construção de diretrizes gerais de

[83] FUTURE OF LIFE INSTITUTE. Benefits and risks of artificial intelligence. Disponível em: <https://futureoflife. org/background/benefits-risks-of-artificial-intelligence/>. Acesso em: 08/12/2018.

[84] ETZIONI, Amitai; EZTIONI, Oren. Keeping AI legal. (February 2, 2016). Vanderbilt Journal of Entertainment & Technology Law Vol. XIX: 1. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2726612>. Acesso em: 08/12/2018.

regulamentação pode preparar o caminho e fornecer uma base comum para um marco regulatório mais amplo sobre IA.

3. Responsabilidade por atos ilícitos resultantes de ações de IA

Em 1942, Isaac Asimov apresentou suas três leis da robótica:[85] (i) um robô não pode ferir um ser humano ou, por inação, permitir que um ser humano seja prejudicado; (ii) um robô deve obedecer às ordens dadas por seres humanos, exceto quando essas ordens entrarem em conflito com a lei anterior; e (iii) um robô deve proteger sua própria existência, desde que essa proteção não entre em conflito com as duas leis anteriores.

As regras de Asimov refletiam a percepção que a humanidade tinha sobre as máquinas inteligentes no início do século XX: robôs semelhantes aos humanos que se tornariam conscientes e se vingariam das pessoas por tê-los criado para a servidão.

Quase 80 anos depois, o desenvolvimento e a disseminação da IA levaram a necessidades regulatórias além daquelas expressas por Asimov. Em 2017, Oren Etzioni sintetizou as preocupações atuais sobre a IA em três regras complementares:[86] (i) um sistema de IA deve estar sujeito ao mesmo conjunto de leis aplicáveis ao seu operador humano; (ii) um sistema de IA deve divulgar claramente que não é humano; e (iii) um sistema de IA não pode reter ou divulgar informações confidenciais sem a aprovação explícita da fonte dessas informações.

As regras de Etzioni foram concebidas para indivíduos, corporações e governos. Pode-se argumentar que sua afirmação é redundante, uma vez que a maioria dos ordenamentos jurídicos modernos já determina que pessoas naturais adultas devem ser responsabilizadas pelos danos causados por seus filhos menores, animais ou bens. Se um objeto cai da janela da casa de uma pessoa e

[85] ASIMOV, Isaac. Histórias de robôs. L&PM Editora, Porto Alegre: 2010.
[86] EZTIONI, Oren. How to regulate artificial intelligence. THE NEW YORK TIMES. [2017]. Disponível em: <https://www.nytimes.com/2017/09/01/opinion/artificial-intelligence-regulations-rules.html>. Acesso em: 08/12/2018.

quebra o carro de outra, o proprietário da casa é obrigado a indenizar o proprietário do veículo na extensão dos danos causados, independentemente da intencionalidade. Se uma criança de dez anos pegar emprestada a bicicleta do vizinho e acidentalmente destruí-la, seus responsáveis legais (geralmente os pais) terão de pagar pelos danos. Se um cachorro morder um pedestre na rua, seu dono terá de indenizar a pessoa ferida. Entretanto, diferentemente de objetos inanimados, a IA é capaz de tomar decisões autônomas; diferentemente de crianças, a IA é altamente opaca, frequentemente não permintindo rastreabilidade de suas ações; e, diferentemente dos animais, a IA tem a capacidade de aprendizado profundo.

Suponha que um banco esteja sendo processado por discriminar pessoas negras na análise de crédito. Em defesa, o banco argumenta que o processamento de informações e a tomada de decisões na análise de crédito são totalmente executados por um algoritmo e que no código de programação original não foi incluída nenhuma variável relacionada à cor da pele do indivíduo. O computador, portanto, deve ter adquirido a tendência tendenciosa de forma autônoma. Rastrear os processos de tomada de decisão feitos pelo algoritmo, entretanto, é uma tarefa extraordinariamente complexa, não raramente impossível. Considerando as evidências de não intenção, o banco deveria ser responsabilizado por negligência? Existem ferramentas disponíveis para monitorar e supervisionar algoritmos de IA, para prevenir ou remediar a tomada de decisões autônomas que levem à violação de regras jurídicas?

Com vistas a garantir a aplicação das regras mencionadas anteriormente, Amitai e Oren Etzioni sugerem que a lei precisa de instrumentos inteligentes para lidar com instrumentos inteligentes.[87] Eles propõem a diferenciação entre duas categorias de IA: (i) IA de primeiro nível, consistente em programas operacionais de IA; e (ii) IA de segundo nível, ou Guardiões de IA, composta por programas de IA de supervisão que revisam a tomada de decisões da primeira categoria e

[87] ETZIONI, Amitai; EZTIONI, Oren. Keeping AI legal. (February 2, 2016). Vanderbilt Journal of Entertainment & Technology Law Vol. XIX: 1. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2726612>. Acesso em: 08/12/2018.

mantêm as decisões em conformidade com a lei. Os Guardiões de IA incluiriam programas de IA para supervisionar, auditar e garantir a conformidade dos programas operacionais de IA.

Assim como empresas são monitoradas por auditores e órgãos governamentais são supervisionados por órgãos de controle, os programas operacionais de IA poderiam ser supervisionados por Guardiões de IA para evitar desvios das instruções incorporadas aos programas de IA pelos programadores humanos. Um Guardião de IA poderia desempenhar uma ampla gama de funções de supervisão. Eles poderiam determinar se os programas operacionais de IA observam as leis de privacidade, se esses sistemas usam informações obtidas ilegalmente ou se o abuso foi um ato deliberado por parte dos programadores ou resultado da operação do sistema de IA. Os Guardiões de IA poderiam investigar se o software de planejamento financeiro direciona seus usuários para investimentos ou planos de seguro nos quais aqueles que desenvolveram o programa têm interesse financeiro. Os instrumentos de monitoramento também poderiam verificar se os resultados dos mecanismos de pesquisa são tendenciosos em favor dos anunciantes do provedor de pesquisa. Os Guardiões de IA poderiam impedir a vigilância contínua de pessoas em espaços públicos e o vazamento de informações confidenciais, rastreando o apagamento automático de informações armazenadas em centros de dados.

O uso de IA para monitorar a IA tem a vantagem da eficiência: os computadores levam muito menos tempo e recursos do que um ser humano para realizar essas análises. Como Amitai e Oren Etzioni apontam,[88] a IA de segundo nível não resolve a questão "quem guarda os guardiões?" Todos os sistemas são falíveis. No entanto, um mínimo de supervisão de máquinas autônomas inteligentes é, sem dúvida, uma maneira de melhorar as interações entre humanos e IA. Os princípios de Etzioni, longe de esgotar as situações envolvendo IA que exigem regulamentação, constituem um ponto de partida para a discussão

[88] ETZIONI, Amitai; EZTIONI, Oren. Keeping AI legal. (February 2, 2016). Vanderbilt Journal of Entertainment & Technology Law Vol. XIX: 1. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2726612>. Acesso em: 08/12/2018.

sobre a responsabilidade por atos ilícitos resultantes de ações de algoritmos. A aplicação de suas três afirmações em conjunto com os institutos jurídicos da negligência e do dever de prevenir danos pode ser desdobrada nas preposições a seguir:

Primeira premissa. Um sistema de IA deve estar sujeito ao mesmo conjunto de leis aplicáveis a seu operador humano, divulgar claramente que não é humano e não pode reter ou divulgar informações confidenciais sem a aprovação explícita da fonte dessas informações.

Segunda premissa. A responsabilidade de garantir a conformidade com a primeira declaração é: (a) dos desenvolvedores de software, se a violação da lei ocorrer devido a um ato cometido na criação e programação do código-fonte; ou (b) dos operadores de software, se a violação da lei ocorrer devido a um ato cometido no uso operacional do software.

Terceira premissa. Os desenvolvedores e operadores de software devem fazer o que estiver razoavelmente ao seu alcance para evitar a violação da lei por um sistema de IA. Se necessário, os desenvolvedores e operadores devem empregar instrumentos de supervisão de IA para monitorar a conformidade dos instrumentos operacionais de IA com a primeira premissa. A ausência de meios adequados de monitoramento é considerada negligência e acarreta a obrigação de indenização pelo desenvolvedor ou operador à vítima, em caso de violação da lei por um sistema de IA.

Quarta premissa. A responsabilidade do desenvolvedor ou do operador pode ser atenuada se for comprovado que os mecanismos de controle adequados foram empregados, embora tenham se mostrado insuficientes para evitar danos.

As quatro premissas gerais acima detalhadas poderiam servir de base para a construção de uma teoria de responsabilidade por atos praticados por IA. Cada vez mais presente em diversas áreas da vida humana, a inteligência artificial desafia os limites jurídicos da figura tradicional da responsabilidade ao acrescentar uma variável complexa na dinâmica: um instrumento capaz de tomar decisões autônomas e de aprendizado profundo, mas quase impossível de ser dissecado pela mente humana por meio de ferramentas manuais. Assim, é

urgente que os operadores do direito, em conjunto com a comunidade científica, aprofundem os estudos sobre as implicações do uso da IA, para adequar as normas jurídicas às novas necessidades surgidas com o intenso desenvolvimento tecnológico neste início de século XXI.

4. Direito de IA em perspectiva comparada

Embora as críticas sejam cada vez mais fortes sobre o vácuo jurídico ainda existente em muitos domínios afetados pelo avanço tecnológico, em especial a IA, poucas iniciativas para regulamentar a inteligência artificial floresceram. Um possível motivo para essa letargia legislativa generalizada é o fato de que os governos nacionais temem que a imposição de restrições ao desenvolvimento e ao uso da IA possa deixá-los para trás na corrida global pela hegemonia tecnológica. Há, contudo, algumas iniciativas de legiferação em curso.

Em outubro de 2016, o Conselho Nacional de Ciência e Tecnologia dos Estados Unidos publicou o relatório "Preparando o Futuro da Inteligência Artificial",[89] que forneceu 23 recomendações para incentivar as instituições públicas e privadas a examinar se e como elas podem aproveitar a IA e o aprendizado de máquina de forma responsável, de modo a beneficiar a sociedade.

O Grupo Europeu de Ética em Ciência e Novas Tecnologias, grupo de pesquisa relacionado à União Europeia, divulgou em março de 2018 uma "Declaração sobre Inteligência Artificial, Robótica e Sistemas 'Autônomos'".[90] O documento listou vários princípios éticos e pré-requisitos democráticos a serem observados na aplicação da IA, como dignidade humana, autonomia,

[89] EXECUTIVE OFFICE OF THE PRESIDENT NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Preparing for the future of artificial intelligence. Washington DC, 2016. Disponível em: <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf>. Acesso em: 08/12/2018

[90] EUROPAN GROUP ON ETHICS AND NEW TECHNOLOGIES. Statement on artificial intelligence, robotics and 'autonomous systems.' doi: 10.2777/531856 Disponível em: <https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf>. Acesso em: 08/12/2018.

responsabilidade, justiça, equidade e solidariedade, democracia, estado de direito e prestação de contas, segurança, integridade física e mental, proteção de dados e privacidade e sustentabilidade. Além disso, dois marcos regulatórios recentes que dizem respeito a alguns aspectos de IA foram aprovados no âmbito da União Europeia: o Regulamento Geral sobre a Proteção de Dados[91] e o Regulamento dos Mercados Digitais.[92] Uma proposta de regulamento específico para inteligência artificial está atualmente sendo discutido no Parlamento Europeu.[93]

O governo britânico, representado pelo Comitê Seleto de Inteligência Artificial, publicou em abril de 2018 o estudo "AI in the UK: ready, willing and able?"[94] O relatório abrangeu várias áreas impactadas pela IA, como saúde, educação e mercado de trabalho, e forneceu recomendações detalhadas para os setores público e privado, em uma tentativa semelhante à americana de promover a inovação sem comprometer os direitos humanos.

O Conselho de Estado da China anunciou em julho de 2017 o seu "Plano de Desenvolvimento de Inteligência Artificial de Próxima Geração".[95] De acordo com o documento, a China pretende ser a líder mundial em IA até 2030. A conquista da liderança global é baseada em três estágios. Em todas elas, destaca-

[91] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 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 (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em 16/03/2024.

[92] UNIÃO EUROPEIA. Regulamento (UE) 2022/1925 de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital (Regulamento dos Mercados Digitais). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R1925>. Acesso em 26/03/2024.

[93] PARLAMENTO EUROPEU. Proposta de Regulamento que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial). Disponível em: <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF>. Acesso em: 26/03/2024.

[94] SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE. AI in the UK: ready, willing and able? Disponível em: <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>. Acesso em: 08/12/2018.

[95] CHINA, State Council of. A new generation artificial intelligence development plan. Disponível em: <https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence
-development-plan/>. Acesso em: 08/12/2018.

se a construção de estruturas abrangentes de leis, regulamentações, éticas e políticas.

Além de ter avançado com a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei federal nº 13.709/2018), o Brasil deu passos importantes em direção à normatização do uso de IA com a edição da Resolução nº 23.732, de 27 de fevereiro de 2024 pelo Tribunal Superior Eleitoral (TSE), que exige transparência quanto à origem de conteúdo gerado por IA e proíbe o deepfake, isto é, "manipulações audiovisuais que confundem o espectador (ou ouvinte) pelo grau de semelhança com a imagem e/ou a voz de pessoas reais,"[96] na propaganda eleitoral. Um marco regulatório específico para inteligência artificial e aplicável de forma geral a outras áreas para além da eleitoral é, atualmente, objeto de discussão a nível federal. Em 07 de março de 2024, na 2ª Reunião Ordinária do Conselho Nacional de Ciência e Tecnologia (CCT), cujo tema foi "Os avanços da Inteligência Artificial (IA) no Brasil", discutiu-se a revisão da Estratégia Brasileira de Inteligência Artificial, publicada em 2021, e a criação de uma Política Nacional de Inteligência Artificial. O tom do debate brasileiro tem se pautado pela necessidade de posicionar o país no tema de forma autônoma, sem ficar "a reboque" da União Europeia, bem como pela consciência de que uma saída verdadeiramente eficaz deverá passar pelo multilateralismo.

Quando se consideram os efeitos da automação no mercado de trabalho e na distribuição de renda, a relevância de internacionalizar o debate se torna maior. Em um mundo altamente globalizado, o desenvolvimento de máquinas superinteligentes no Vale do Silício não expulsará apenas os trabalhadores americanos do mercado de trabalho, mas afetará principalmente a mão de obra desqualificada nos países em desenvolvimento. Se o Uber conseguir mudar sua frota para carros totalmente automatizados, por exemplo, 3 milhões de motoristas em todo o mundo ficarão desempregados da noite para o dia.[97] Os

[96] AMATO, Lucas Fucci. Inovação tecnológica e inovação jurídica: das fake news às deepfakes. *Jota* (15/03/2024). Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/inovacao-tecnologica-e-inovacao-juridica-das-fake-news-as-deepfakes-15032024>. Acesso em 26/03/2024.
[97] MADRIGAL, Alexis C. 3 Million Uber Drivers Are About to Get a New Boss. THE ATLANTIC. [2018]. Disponível em: <https://www.theatlantic.com/technology/archive/2018/04/uber-driver-app-revamp/557117/>. Acesso em: 09/12/2018.

países em desenvolvimento têm pouca estrutura para absorver sozinhos o impacto econômico e social do desemprego em massa resultante da automação de algoritmos.

Dois cenários geralmente vêm à tona com a perspectiva de os robôs se tornarem a principal classe trabalhadora. Em um deles, a renda oriunda do trabalho das máquinas é distribuída e as pessoas terão a chance de passar mais tempo com suas famílias, amigos e vizinhos em atividades comunitárias e culturais. A humanidade, com a ajuda da inteligência artificial, fará progressos surpreendentes na expectativa de vida, na cura de doenças, na erradicação da pobreza e na ciência. O outro cenário leva em conta a possibilidade de se repetirem, em escala ampliada, as consequências da automação que ocorreram na primeira revolução industrial: aumento da concentração dos meios de produção, levando ao crescimento da desigualdade social e econômica, fomentando a violência, a marginalização, a erosão democrática e os movimentos xenófobos.

Seja para seguir o primeiro cenário ou evitar a concretização do segundo, a cooperação entre as nações será essencial. Possíveis soluções para mitigar os efeitos adversos da disseminação da IA, como renda básica universal e redução de dias e semanas de trabalho, só podem ser efetivas se forem colocadas em prática por um número significativo de países. As nações em desenvolvimento, historicamente privadas de autonomia econômica e destinadas à produção de commodities, têm menos estruturas para lidar com o choque disruptivo que a IA logo provocará no mercado de trabalho. Dessa forma, tanto em razão de os países líderes em IA não quererem perder competitividade e os países em desenvolvimento precisarem de ferramentas para evitar o desemprego em massa, é fundamental que o debate sobre a regulamentação da IA seja levado a um fórum multilateral aberto, transparente e participativo.

Conclusão

A tecnologia impulsionada pela IA oferece à humanidade a possibilidade de atingir um nível de prosperidade sem precedentes, mas também de colocar

em risco a sobrevivência da própria civilização. A disseminação de IA nas mais variadas áreas da vida humana - da medicina à guerra, do transporte ao agronegócio, da educação ao mercado de ações - eleva o nível de urgência para regular a atribuição de responsabilidade civil por atos ilícitos cometidos por IA. O campo de conhecimento Direito de IA busca investigar como operacionalizar a responsabilidade jurídica na era do algoritmo. Capazes de tomar decisões autônomas e de aprendizado profundo e, muitas vezes, opacos ao monitoramento humano, os instrumentos de IA exigem uma reformulação dos conceitos de intencionalidade e negligência.

Para cumprir as três regras básicas propostas por Etzioni (a IA está sujeita às mesmas normas legais que os humanos; a IA deve revelar sua condição quando em contato com humanos e a IA só pode reter ou revelar informações confidenciais com consentimento explícito), os desenvolvedores e operadores de software devem empregar todos os meios razoáveis. Isso inclui o uso de Guardiães de IA para monitorar os sistemas operacionais. Embora a ausência de meios adequados de monitoramento deva ser considerada negligência e acarretar a obrigação de indenização, a responsabilidade do desenvolvedor ou do operador pode ser atenuada se forem implantados mecanismos de controle adequados. Com o objetivo de aumentar a efetividade da regulamentação da IA, bem como evitar a ampliação das desigualdades regionais, standards globais poderiam dar o pontapé inicial para uma estrutura regulatória internacional consistente, com o objetivo de proteger direitos humanos sem bloquear a inovação tecnológica.

Referências

AMATO, Lucas Fucci. Inovação tecnológica e inovação jurídica: das fake news às deepfakes. **Jota** (15/03/2024). Disponível em: https://www.jota.info/opiniao-e-analise/artigos/inovacao-tecnologica-e-inovacao-juridica-das-fake-news-as-deepfakes-15032024 . Acesso em 26/03/2024.

ASIMOV, Isaac. **Histórias de robôs.** L&PM Editora, Porto Alegre: 2010.

BROWN, Kristen V. Google showed woman ads for lower paying jobs. **SPLINTER.** [2015]. Disponível em: https://splinternews.com/google-showed-women-ads-for-lower-paying-jobs-1793848970 . Acesso em: 09/12/2018.

CHINA, State Council of. **A new generation artificial intelligence development plan.** Disponível em: https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/ . Acesso em: 08/12/2018.

ETZIONI, Amitai; EZTIONI, Oren. Keeping AI legal. (February 2, 2016). **Vanderbilt Journal of Entertainment & Technology Law** Vol. XIX: 1. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2726612 . Acesso em: 08/12/2018.

ETZIONI, Amitai; EZTIONI, Oren. Should artificial intelligence be regulated? (June 27, 2017). **Issues in Science and Technology**. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993506 . Acesso em: 08/12/2018.

EUROPAN GROUP ON ETHICS AND NEW TECHNOLOGIES. **Statement on artificial intelligence, robotics and 'autonomous systems.'** doi: 10.2777/531856. Disponível em: https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf . Acesso em: 08/12/2018.

EXECUTIVE OFFICE OF THE PRESIDENT NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. **Preparing for the future of artificial intelligence.** Washington, 2016. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf . Acesso em: 08/12/2018

EZTIONI, Oren. How to regulate artificial intelligence. **THE NEW YORK TIMES**. [2017]. Disponível em: https://www.nytimes.com/2017/09/01/opinion/artificial-intelligence-regulations-rules.html . Acesso em: 08/12/2018.

FUTURE OF LIFE INSTITUTE. **Benefits and risks of artificial intelligence.** Disponível em: https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/ . Acesso em: 08/12/2018.

LAWGORITHM. **What is Lawgorithm?** Disponível em: https://lawgorithm.com.br/en/about-us/ . Acesso em: 06/03/2020.

MADRIGAL, Alexis. 3 Million Uber Drivers Are About to Get a New Boss. **The Atlantic.** [2018]. Disponível em: https://www.theatlantic.com/technology/archive/2018/04/uber-driver-app-revamp/557117/ . Acesso em: 09/12/2018.

MELVIN, Don. Cop pull over Google self-driving car, finds no driver to ticket. **CNN.** [2015]. Disponível em: https://edition.cnn.com/2015/11/13/us/google-self-driving-car-pulled-over/ .Acesso em 09/12/2018.

PARLAMENTO EUROPEU. Prop**osta de Regulamento que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial).** Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0004.02/DOC_1&format=PDF . Acesso em: 26/03/2024.

PEART, Andy. **Homage to John McCarthy, the father of Artificial Intelligence.** [2017]. Disponível em: https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence . Acesso em: 09/12/2018.

SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE. **AI in the UK:** ready, willing and able? Disponível em: https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf . Acesso em: 08/12/2018.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais (Regulamento Geral sobre a Proteção de Dados).** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679 . Acesso em 16/03/2024.

UNIÃO EUROPEIA. **Regulamento (UE) 2022/1925 de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital**

(Regulamento dos Mercados Digitais). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R1925 . Acesso em 26/03/2024.

7. A Proteção de Direitos Fundamentais no Regulamento Europeu da Inteligência Artificial[98]

Clara Martins Pereira[99]

I. Introdução: a inteligência artificial e os direitos fundamentais

A regulação da Inteligência Artificial tem vindo a emergir como um dos maiores desafios atualmente enfrentados pelo chamado Direito Digital.[100] Começando com o aparecimento dos primeiros algoritmos computorizados nos anos 30-40 (CHABERT *et al*, 1999, pp. 455 ss.) e das primeiras formas de "Inteligência Artificial"[101] nos anos 50 (HAENLEIN e KAPLAN, 2019, p. 7)—e culminando na recente popularização de modelos de finalidade geral como o Chat GPT (HACKER *et al*, 2023, p. 1112)—as aplicações de Inteligência Artificial permeiam cada vez mais o dia-a-dia das sociedades contemporâneas (HM UK

[98] Uma versão inicial deste capítulo serviu de inspiração às participações feitas pela autora no 33.º Digital Business Congress organizado pela APDC – Associação Portuguesa para o Desenvolvimento das Comunicações (ocorrido entre 14 e 15 de maio de 2024), no Morais Leitão Summer Retreat (ocorrido entre 27 e 28 de junho 2024), na Palestra "Regulação da Inteligência Artificial no Brasil - Ética, Inteligência Artificial e Regulação" organizada pelo Programa de Pós-Graduação em Direito Político e Económico da Universidade Presbiteriana Mackenzie (ocorrida a 27 de junho de 2024), e na 5.ª Edição da Abreu Sustainability School sobre "Direitos Fundamentais na Era da Inteligência Artificial" (ocorrida a 4 de Setembro de 2024). A autora agradece todas as discussões, comentários e questões que tiveram lugar durante cada uma dessas sessões. Todos os erros permanecem da responsabilidade da autora.

[99] Assistant Professor in Law, University of Durham.

[100] Por "Direito Digital" entende-se a área do direito que se ocupa da regulação da chamada "Economia Digital" (INOZEMTSEV, 2021, p. 8)—sendo "Economia Digital" a área da economia que engloba as possibilidades geradas pelas tecnologias que resultam da combinação da digitalização da informação com o advento e popularização da Internet (CARLSSON, 2024, p. 245).

[101] A definição de "Inteligência Artificial" levanta, também ela, uma série de dúvidas sobre que tipos de tecnologias algorítmicas podem ser consideradas verdadeiramente "inteligentes" e sobre que tipo de tecnologias algorítmicas caem fora do conceito de Inteligência Artificial tal como este é entendido atualmente. Para uma discussão mais aprofundada destas questões, *ver*, por exemplo, WANG, 2019, p. 1.

GOVERNMENT, 2021, p. 5),[102] criando novos problemas para o Direito e inspirando novas soluções para esses problemas.[103]

O presente capítulo debruça-se sobre uma das principais problemáticas criadas pelas tecnologias de Inteligência Artificial para o Direito—a ameaça que estas tecnologias podem representar para os chamados direitos fundamentais e humanos (FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2021, p. 1)—e, correspondentemente, sobre uma das mais ambiciosas soluções jurídicas avançadas em resposta a esse problema—o Regulamento Europeu da Inteligência Artificial,[104] recentemente aprovado pela União Europeia e em vigor desde 2 de agosto de 2024 ("Regulamento Europeu", "Regulamento" ou "*AI Act*").[105] Mais especificamente, o presente capítulo propõe-se a avaliar a eficácia deste Regulamento no cumprimento do seu objetivo de proteção dos direitos fundamentais,[106] utilizando como referência os instrumentos tradicionalmente subjacentes à proteção de direitos fundamentais no espaço Europeu—em

[102] Parafraseando o Governo Inglês, entrámos firmemente na "era da Inteligência Artificial", onde as interações com aplicações de Inteligência Artificial acontecem diariamente "quer o reconheçamos quer não" (HM UK GOVERNMENT, 2021, p. 5).

[103] O número (e diversidade) de soluções jurídicas desenvolvidas em resposta aos problemas criados pela Inteligência Artificial é ilustrado de forma expressiva pelo repositório de iniciativas legislativas e regulamentares gerido pelo *AI Policy Observatory* da Organização para a Cooperação e Desenvolvimento Económico ou Económico ("OCDE"), o qual pode ser consultado em <https://oecd.ai/en/dashboards/policy-instruments/Emerging_technology_regulation> acedido em 30 de Setembro de 2024.

[104] Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 ("Regulamento Europeu da Inteligência Artificial", "Regulamento Europeu", "Regulamento", ou "AI Act"), aprovado em 13 de junho de 2024, e disponível para consulta na sua versão portuguesa em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689> acedido a 30 de setembro de 2024.

[105] *Ver* o Artigo 113.º do Regulamento Europeu da Inteligência Artificial. Cumpre notar: que os Capítulos I e II do Regulamento apenas são aplicáveis a partir de 2 de fevereiro de 2025; que o Capítulo III, Secção 4, o Capítulo V, o Capítulo VII, o Capítulo XII e o Artigo 78.º do Regulamento são aplicáveis a partir de 2 de agosto de 2025 (com exceção do Artigo 101.º); e que o Artigo 6.º, n.º 1, e as obrigações correspondentes previstas no Regulamento Europeu são aplicáveis a partir de 2 de agosto de 2027.

[106] Como veremos, um dos objetivos do Regulamento Europeu é precisamente "assegura[r] (...) um elevado nível de proteção (...) dos direitos fundamentais" (*ver* o Artigo 1.º, n.º1 do Regulamento Europeu da Inteligência Artificial).

particular a Carta dos Direitos Fundamentais da União Europeia ("Carta")[107] e a Convenção Europeia dos Direitos Humanos ("Convenção Europeia").[108]

Começando pela análise do problema jurídico a que se dedica este capítulo, cumpre notar que os riscos advenientes das tecnologias de Inteligência Artificial para os direitos fundamentais e humanos têm sido amplamente documentados tanto pela doutrina dedicada a estes temas,[109] como pelos *watchdogs*[110] que monitorizam a atividade dos protagonistas da revolução da Inteligência Artificial.[111] Assim, são hoje conhecidos vários exemplos de aplicações de Inteligência Artificial que podem entrar em conflito com o núcleo de direitos a que habitualmente nos referimos como direitos fundamentais ou humanos.[112] Neste âmbito, são particularmente ilustrativos os casos que chegam à discussão pública vindos das áreas da *(i)* segurança pública e vigilância, da *(ii)* tomada de decisões sobre o acesso a serviços essenciais, do *(iii)* policiamento preditivo, do *(iv)* desenvolvimento de armas e outros sistemas de defesa, e da *(v)* classificação de indivíduos no âmbito de sistemas de crédito social, ou "*social scoring*" (EDRi – EUROPEAN DIGITAL RIGHTS, 2020, p. 1).

[107] A versão portuguesa do texto completo da Carta encontra-se disponível para consulta em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT> acedido a 30 de setembro de 2024.

[108] A versão portuguesa do texto completo da Convenção Europeia encontra-se disponível para consulta em <https://www.echr.coe.int/documents/d/echr/Convention_POR> acedido a 30 de setembro de 2024.

[109] A título de exemplo, *veja-se*, *inter alia,* ALMADA e PETIT, 2023; BRKAN *et al*, 2021; BROWNSWORD, 2023; GORDON, 2021; UFERT, 2020; e WENDEHORST, 2022.

[110] Os chamados "*watchdogs*" são organizações tipicamente não governamentais que monitorizam e avaliam criticamente a atuação de entidades públicas e privadas e alertam o público para atividades que aparentem ir contra o interesse público (DAGGETT, 2002, pp. 105-108)

[111] *Veja-se*, a título exemplo, a atividade desenvolvida por organizações como a *Algorithm Watch* – relativamente ao impacto da Inteligência Artificial nas sociedades modernas – e a rede European Digital Rights ("EDRi")—especificamente em relação ao impacto da Inteligência Artificial e outras tecnologias da Economia Digital nos direitos fundamentais.

[112] Uma discussão mais detalhada sobre o conceito de "direitos fundamentais" (e sobre a sua relação com o conceito vizinho de "direitos humanos") pode ser encontrada na Secção II.1 *infra.*

1. Casos de utilização de Inteligência Artificial: a tecnologia em rota de colisão com os direitos fundamentais

Uma análise breve de alguns dos "casos de utilização" (ou "*use cases*") das tecnologias de Inteligência Artificial ajuda a concretizar as preocupações levantadas pela tensa relação que se tem vindo a estabelecer entre estas tecnologias e os direitos fundamentais. Na área da *(i)* segurança pública e vigilância, as aplicações de Inteligência Artificial são crescentemente utilizadas na captura de dados biométricos em público, criando riscos potencialmente significativos para, entre outros, os direitos fundamentais ao respeito pela vida privada e familiar[113] e à proteção de dados pessoais[114] (FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2018, p. 20). A título de exemplo, a empresa concessionária da Linha Amarela do metro de São Paulo (a Via Quatro) foi notícia, em 2018, devido ao tratamento e captura não consentidos de imagens gravadas por aparelhos de reconhecimento facial com o objetivo de registar reações a anúncios publicitários (SILVEIRA BORGES *et al*, pp. 187 ss.); o episódio levantou, então, questões relativas à admissibilidade de restrições a direitos fundamentais com finalidades meramente comerciais (e eventualmente desproporcionais face aos fins de segurança pública que terão inicialmente justificado a sua utilização).[115] Já no âmbito da defesa de fronteiras, vale a pena atentar no controverso *iBorderCtrl* — um projeto piloto atualmente em fase de teste

[113] *Ver*, por exemplo, o Artigo 7.º da Carta e o Artigo 8.º da Convenção Europeia. Atendendo o objeto do presente capítulo — que se foca na proteção dos direitos fundamentais no âmbito do Regulamento Europeu da Inteligência Artificial e no espaço Europeu — menções a direitos fundamentais específicos são normalmente feitas por referência a exemplos retirados da Carta ou da Convenção Europeia (ainda que as disposições de uma e de outra encontrem frequentemente paralelos em instrumentos de carácter universal, como a Declaração Universal dos Direitos Humanos das Nações Unidas, ou noutros instrumentos de carácter regional, como a Convenção Americana sobre Direitos Humanos).

[114] *Ver*, por exemplo, o Artigo 8.º da Carta.

[115] De facto, o Instituto Brasileiro de Defesa ao Consumidor acabou por intentar uma ação contra a Via Quatro que levou à proibição do uso das imagens recolhidas pela empresa sem autorização e à sua condenação no pagamento de uma indemnização por danos não patrimoniais no valor de R$ 100,000; o sentido da decisão de primeira instância veio a ser confirmado em segunda instância pela 8ª Câmara de Direito Público do Tribunal de Justiça de São Paulo, levando a um aumento da indemnização devida pela Via Quatro para R$ 500,000: *ver* Apelação da 8ª Câmara de Direito Público do Tribunal de Justiça de São Paulo de 10 de maio de 2023 (processo nº 1090663-42.2018.8.26.0100), disponível para consulta em < https://esaj.tjsp.jus.br/cposg/show.do?processo.codigo=RI006J6T80000&processo.foro=990&processo.numero=10906634220188260100> acedido a 30 de setembro de 2024.

na Hungria, na Grécia e na Látvia (EUROPEAN COMMISSION, 2018), e que utiliza a Inteligência Artificial na análise das "micro-expressões" feitas por indivíduos à entrada destes países (EDRI – EUROPEAN DIGITAL RIGHTS, 2020, p. 19)—e, bem assim, na decisão do Tribunal de Justiça Europeu que veio reconhecer os riscos criados por este projeto para os direitos fundamentais.[116]

Já na área da *(ii)* tomada de decisões sobre o acesso a serviços essenciais, merece atenção a utilização de tecnologias de Inteligência Artificial na análise de emoções, comportamentos e características protegidas[117]—e merece atenção também o impacto que este tipo de análise pode ter no acesso a produtos de interesse económico geral,[118] com risco para os direitos fundamentais à dignidade,[119] à proteção de dados pessoais,[120] e à não discriminação[121] (EDRI – EUROPEAN DIGITAL RIGHTS, 2020, pp. 4 ss.). Neste âmbito, a ferramenta "*Redditometro*", inaugurada pelas autoridades tributárias do governo Italiano em 2010, ilustra bem os riscos inerentes à utilização de tecnologias de Inteligência Artificial na tomada de decisões sobre a capacidade contributiva de indivíduos, com impacto decisivo nos seus direitos fundamentais (EUROPEAN PLATFORM UNDECLARED WORK, 2018, pp. 1-2). De facto, uma primeira versão deste *Redditometro* apresentava-se como uma ferramenta de "*profiling*" alimentada por Inteligência Artificial e que fazia inferências sobre os contribuintes italianos com base na média das despesas associadas a determinadas categorias familiares e geográficas (EDRI – EUROPEAN DIGITAL RIGHTS, 2020, p. 10). No seguimento de uma investigação da autoridade para a proteção de dados Italiana (a "Garante

---

[116] *Ver* o Acórdão do Tribunal Geral (Décima Secção) de 15 de dezembro de 2021 (processo n.º T-158/19), disponível para consulta em <https://curia.europa.eu/juris/document/document.jsf?text=&docid=251282&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=810186> acedido a 30 de setembro de 2024.

[117] Por "características protegidas" entende-se o conjunto de características que não podem estar na base de decisões discriminatórias e que incluem, designadamente, sexo, raça, cor, origem étnica ou social, características genéticas, língua, religião ou convicções, opiniões políticas ou outras, pertença a uma minoria nacional, riqueza, nascimento, deficiência, idade ou orientação sexual (*ver* EUROPEAN COMMISSION, 2024).

[118] *Ver*, por exemplo, o Artigo 36.º da Carta.

[119] *Ver*, por exemplo, o Artigo 1.º da Carta e o Artigo 1.º da Convenção Europeia.

[120] *Ver*, por exemplo, o Artigo 8.º da Carta.

[121] *Ver*, por exemplo, o Artigo 21.º da Carta e o Artigo 14.º da Convenção Europeia.

per la Protezione dei Dati Personali" ou "GPDP"), a nova versão do *Redditometro* está hoje sujeita a limites significativos na utilização de dados obtidos por inferência (GPDP - GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 2013, p.1).

No âmbito da *(iii)* atividade policial, a utilização de tecnologias de Inteligência Artificial em programas de vigilância com finalidades preditivas tem também vindo a surgir em confronto com uma série de direitos fundamentais — designadamente os direitos fundamentais à integridade física e mental,[122] à liberdade e à segurança,[123] ao respeito pela vida privada e familiar,[124] à liberdade de reunião e de associação,[125] à igualdade perante a lei,[126] à não discriminação[127] e à presunção de inocência[128] (CASTETS-RENARD, 2021, pp. 100-101). De facto, a utilização da Inteligência Artificial na criação de perfis de suspeitos em momento prévio ao do cometimento de qualquer crime tem vindo a ser amplamente criticada por organizações de defesa dos direitos dos cidadãos na era digital (EDRI – EUROPEAN DIGITAL RIGHTS, 2020, pp. 10-15) — e vale a pena atentar na decisão do Tribunal Constitucional Federal Alemão de 2023 que veio a declarar como inconstitucional a utilização do software de vigilância *Palantir* em Hesse, tendo em conta as suas finalidades (predominantemente) preditivas e os riscos criados para direitos fundamentais previstos na Constituição Alemã.[129] Para além da Alemanha, também a Bélgica, a Dinamarca, a Holanda, a Itália, o Reino Unido e a Suíça têm vindo a abraçar a utilização da Inteligência Artificial no desenvolvimento de programas de policiamento preditivo (EDRI – EUROPEAN DIGITAL RIGHTS, 2020, pp. 10-15), ainda que a eficácia destes programas continue por demonstrar (KRASMANN e EGBERT, 2019, pp. 3-4) — e ainda que o seu impacto

[122] *Ver*, por exemplo, o Artigo 3.º da Carta.
[123] *Ver*, por exemplo, o Artigo 6.º da Carta e o Artigo 5.º da Convenção Europeia.
[124] *Ver*, por exemplo, o Artigo 7.º da Carta e o Artigo 8.º da Convenção Europeia.
[125] *Ver*, por exemplo, o Artigo 12.º da Carta e o Artigo 11.º da Convenção Europeia.
[126] *Ver*, por exemplo, o Artigo 20.º da Carta e o Protocolo n.º 12 da Convenção Europeia.
[127] *Ver*, por exemplo, o Artigo 21.º da Carta e o Artigo 14.º da Convenção Europeia.
[128] *Ver*, por exemplo, o Artigo 22.º da Carta e o Artigo 6.º da Convenção Europeia.
[129] Designadamente, o direito fundamental à "autodeterminação informacional" (um direito fundamental sem correspondência clara na Carta); para uma discussão *ver* BVerfG, Judgment of the First Senate of 16 February 2023 - 1 BvR 1547/19 -, paras. 1-178, disponível para consulta em <https://www.bverfg.de/e/rs20230216_1bvr154719en.html> acedido em 30 de setembro de 2024.

nos direitos fundamentais continue a preocupar numerosas organizações internacionais (CHIUSI, 2020; EDRI – EUROPEAN DIGITAL RIGHTS, 2020, pp. 10-15).

Também o sector do *(iv)* desenvolvimento de armas e outros sistemas de defesa (os chamados "*Lethal Autonomous Weapon Systems*" ou "LAWS") tem vindo a ser palco de conflitos e tensões entre as tecnologias de Inteligência Artificial incorporadas nessas armas e os direitos fundamentais e humanos (ICRC - INTERNATIONAL COMMITTEE OF THE RED CROSS, 2019, p. 6), em particular (ainda que não exclusivamente), o direito fundamental ao respeito pela vida privada e familiar.[130] Neste âmbito, as tecnologias de Inteligência Artificial têm vindo a revelar-se particularmente promissoras no desenvolvimento de *drones* capazes de proceder à identificação e abate automáticos de alvos estratégicos sem necessidade de decisão humana prévia (LONGPRE *et al*, 2022, pp. 47-56). De facto, relatos provenientes de conflitos armados recentes—designadamente da guerra na Ucrânia e do conflito entre Israel e o Hamas (THE GUARDIAN, 2024)—têm vindo a denunciar a utilização deste tipo de sistemas, com consequências importantes para os indivíduos e comunidades mais diretamente afetados por estes conflitos (UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS, 2023, pp. 2-8).

Finalmente, vale a pena atentar na utilização da Inteligência Artificial no âmbito da *(v)* classificação de indivíduos ao abrigo de sistemas de crédito social (ou "*social scoring*"), designadamente no que toca ao tratamento de dados relacionados com o seu comportamento social—e que podem levar a que estes indivíduos sejam tratados desfavoravelmente em contextos não relacionados com aqueles em que tais dados são originalmente recolhidos (GESLEVICH PACKIN e LEV-ARETZ, 2020, p. 632). O exemplo mais conhecido destas práticas é o sistema de crédito social atualmente em desenvolvimento pelo Governo chinês—e que inclui uma camada adicional de avaliação de comportamentos sociais que acresce às práticas de classificação de crédito ("*credit scoring*") já há muito implementadas no sistema financeiro (GESLEVICH PACKIN e LEV-ARETZ, 2020, p. 641). Os riscos

[130] *Ver*, por exemplo, o Artigo 7.º da Carta e o Artigo 8.º da Convenção Europeia.

que estes sistemas encerram para direitos fundamentais como o direito à dignidade,[131] ou o direito ao respeito pela vida privada e familiar[132] estão relativamente bem documentados (EDRi – EUROPEAN DIGITAL RIGHTS, 2020, p. 2), dando lugar a acesas discussões sobre a melhor forma de proceder à regulamentação do *social scoring* (*ver, inter alia,* GELLER, 2022).

2. O Regulamento Europeu da Inteligência Artificial enquanto veículo para a proteção dos direitos fundamentais

Atendendo aos vários casos de utilização de Inteligência Artificial que atualmente ilustram o potencial de conflito entre estas tecnologias e os direitos fundamentais, é pouco surpreendente que, um pouco por todo o mundo, legisladores e reguladores tenham vindo a notar a necessidade de regular a Inteligência Artificial—destacando, em particular, a importância do papel desempenhado por iniciativas legislativas e regulamentares na mitigação da ameaça que estas tecnologias podem representar para tais direitos.

Na Europa, especificamente, dois quadros regulamentares especiais foram já aprovados em resposta direta a esta ameaça: de um lado, o Regulamento Europeu da Inteligência Artificial—que se propõe a "assegurar um elevado nível de proteção...dos direitos fundamentais consagrados na Carta [dos Direitos Fundamentais da União Europeia]"[133]—e, de outro lado, a Convenção-Quadro do Conselho da Europa[134] sobre Inteligência Artificial e Direitos Humanos, Democracia e Estado de Direito[135]—que foi aprovada em 17 de maio de 2024 e

[131] *Ver*, por exemplo, o Artigo 1.º da Carta e o Artigo 1.º da Convenção Europeia.
[132] *Ver*, por exemplo, o Artigo 7.º da Carta e o Artigo 8.º da Convenção Europeia.
[133] *Ver* o Artigo 1.º, n.º1 do Regulamento Europeu da Inteligência Artificial.
[134] Cumpre notar que o Conselho da Europa é diferente do Conselho Europeu e do Conselho da União Europeia: enquanto o Conselho Europeu é o órgão que reúne os chefes de Estado ou Governo dos 27 Estados-Membros da União Europeia—e o Conselho da União Europeia é constituído por ministros nacionais de todos os países da União Europeia—o Conselho da Europa situa-se inteiramente fora do quadro institucional da União Europeia. Trata-se, antes, de uma organização internacional sediada em Estrasburgo (França) que defende os direitos humanos, a democracia e o Estado de Direito—e embora todos os Estados Membros da União Europeia sejam também membros do Conselho da Europa, o contrário não é verdade, sendo que o Conselho da Europa tem 46 Estados Membros (por oposição aos 27 Estados Membros da União Europeia).
[135] A versão portuguesa do texto completo da Convenção encontra-se disponível para consulta em <https://www.echr.coe.int/documents/d/echr/Convention_POR> acedido a 30 de setembro de 2024.

que se tornou, dessa forma, no primeiro tratado internacional juridicamente vinculativo para a garantia do respeito pelos direitos humanos no âmbito da utilização de sistemas de Inteligência Artificial (COUNCIL OF EUROPE, 2024, p. 2).

Ainda que não ignore o quadro mais completo de proteção de direitos fundamentais face aos riscos criados pela Inteligência Artificial que se tem vindo a formar ao nível Europeu (LEVANTINO e PAOLUCCI, 2024, pp. 4-7), o presente capítulo foca-se apenas no Regulamento Europeu da Inteligência Artificial—e propõe-se a discutir a sua efetividade na proteção destes direitos. Em última instância, conclui-se, em primeiro lugar, que o Regulamento Europeu da Inteligência Artificial se assume, pelo menos à primeira vista, como um instrumento de proteção de "direitos fundamentais", utilizando este conceito, designadamente: *(1)* na determinação dos seus objetivos, *(2)* na determinação dos termos da sua aplicação, *(3)* no desenho do sistema de classificação de risco que aí se impõe às aplicações de Inteligência Artificial, *(4)* na desenvolvimento do conteúdo dos deveres impostos aos destinatários do Regulamento, *(5)* na determinação dos direitos conferidos a quem se vê afetado (ou potencialmente) afetado por aplicações de Inteligência Artificial abrangidas pelo Regulamento, *(6)* no desenho do sistema de governação subjacente ao Regulamento, e, finalmente *(7)* na determinação das regras e limites que governam as alterações que podem ser feitas ao Regulamento Europeu.

Ao mesmo tempo, as referências frequentes ao conceito de "direito fundamentais" no *AI Act* dizem pouco sobre a eficácia deste instrumento na proteção deste tipo de direitos. De facto, do confronto entre o Regulamento e os instrumentos tradicionalmente utilizados na proteção de direitos fundamentais no espaço Europeu resulta claro que a eficácia do Regulamento na proteção dos direitos fundamentais fica muito aquém do compromisso com um "elevado nível de proteção" assumido no Artigo 1.º do *AI Act*. Como veremos, tal deve-se sobretudo à natureza do *AI Act* enquanto regulamento de segurança de produtos assente numa abordagem baseada no risco—natureza essa dificilmente

compatível com a lógica tradicionalmente subjacente à proteção dos direitos fundamentais.[136]

Nesse sentido, os argumentos tecidos neste capítulo acompanham a doutrina que tem vindo a assinalar a natureza híbrida do *AI Act* (*inter alia,* ALMADA e PETIT, 2023). Ao mesmo tempo, fazem uma contribuição original para a discussão em curso através da análise sistemática das várias manifestações do conceito de "direitos fundamentais" constantes do *AI Act*, e da sua confrontação explícita com as características que presidem aos principais instrumentos de defesa dos direitos fundamentais vigentes na Europa. Acresce, no entanto, que as conclusões deste exercício não são apenas relevantes para o estudo do Regulamento Europeu da Inteligência Artificial (ou no âmbito da proteção de direitos fundamentais na Europa): primeiro, porque muitas são as jurisdições que neste momento se vêm a braços com a tarefa de regular a Inteligência Artificial; segundo, porque os problemas criados pela Inteligência Artificial para os direitos fundamentais não conhecem fronteiras; e, terceiro, porque muitas das características subjacentes aos instrumentos de defesa dos direitos fundamentais que vigoram na Europa encontram paralelo nos instrumentos de defesa dos direitos fundamentais utilizados noutras partes do Mundo.[137] Deste modo, espera-se que a análise do Regulamento Europeu da Inteligência Artificial constante deste capítulo possa influenciar outros exercícios de regulamentação da Inteligência Artificial—tanto na Europa como fora dela.

Este capítulo está organizado da seguinte forma: depois da presente Introdução, em que foi feita uma breve apresentação sobre a importância e papel desempenhado pelos direitos fundamentais na regulação da Inteligência Artificial—em particular, no Regulamento Europeu da Inteligência Artificial (*Parte I*)—, discute-se o conceito de direitos fundamentais, bem como a evolução

[136] Em sentido semelhante, veja-se, em particular, ALMADA e PETIT, 2023; e WENDEHORST, 2022.
[137] A título de exemplo, veja-se que a discussão *infra* sobre o campo de aplicação subjetivo, as regras de interpretação especial e os limites à modificação dos direitos fundamentais aplicáveis ao nível da Carta e da Convenção Europeia encontram paralelos significativos tanto em convenções de carácter universal como a Convenção Universal dos Direitos Humanos (*ver,* em particular, os Artigos 29.º - 30.º da Declaração), como noutras convenções regionais, como a Convenção Americana sobre os Direitos Humanos (*ver,* nomeadamente, os Artigos 1.º - 2.º e 27.º - 31.º dessa Convenção).

da sua proteção no espaço Europeu (*Parte II*). De seguida, é feita uma análise detalhada das várias manifestações desta figura dos "direitos fundamentais" no Regulamento Europeu (*Parte III*). A *Parte IV* encerra o capítulo, refletindo sobre o papel efetivamente desempenhado pelo *AI Act* na proteção de direitos fundamentais por referência aos instrumentos de defesa dos direitos fundamentais atualmente vigentes na Europa e enunciando as conclusões que podem ser retiradas dessa reflexão.

II. A proteção dos direitos fundamentais no contexto europeu

O presente capítulo propõe-se a analisar o papel desempenhado pelo Regulamento Europeu da Inteligência Artificial na defesa dos direitos fundamentais face aos riscos criados por tecnologias e aplicações de Inteligência Artificial. Naturalmente, essa análise requer uma discussão prévia sobre *(1)* o conceito de direitos fundamentais, e sobre *(2)* os termos em que a proteção destes direitos face aos desenvolvimentos tecnológicos trazidos pela Inteligência Artificial tem vindo a evoluir no espaço Europeu—levando, primeiro, à aprovação do Regulamento Europeu da Inteligência Artificial e, mais recentemente, à celebração da Convenção-Quadro do Conselho da Europa sobre Inteligência Artificial e Direitos Humanos, Democracia e Estado de Direito.

1. Direitos fundamentais e direitos humanos

A proteção dos chamados "direitos fundamentais" é pedra angular da vasta generalidade dos sistemas jurídicos modernos,[138] mas a definição do que se entende por "direitos fundamentais", a concretização dos direitos que podem ser reconduzidos a esse núcleo e os termos em que estes (ou alguns destes) direitos podem ser restringidos e limitados continua a ser objeto de discussão acesa na

[138] Por esse motivo também, a proteção dos direitos humanos tem vindo a ser objeto de proteção por parte do direito internacional—tanto a nível regional (veja-se, a título de exemplo, e para além da Carta e da Convenção Europeia, a Convenção Americana sobre Direitos Humanos), como a nível mundial (em particular, através de Declaração Universal dos Direitos Humanos das Nações Unidas). Para uma discussão sobre o carácter universal dos direitos humanos (e das controvérsias associadas a essa discussão), veja-se, por exemplo BROWN, 2007, pp. 41ss..

doutrina (*ver, inter alia,* DEMBOUR, 2010, pp. 2-4).[139] Uma análise detalhada do que se entende por "direitos fundamentais" excede largamente o âmbito deste capítulo, mas vale a pena atentar sobre o significado que essa expressão tem vindo a assumir no espaço Europeu—distinguindo, em particular, entre os conceitos de "direitos fundamentais" e "direitos humanos".

No contexto Europeu, os direitos fundamentais são os direitos e as liberdades básicas inerentes a todos os seres humanos, independentemente da sua nacionalidade, local de residência, sexo, etnia, cor de pele, sexualidade, religião, língua ou outras características protegidas. Nesse sentido, a Carta dos Direitos Fundamentais da União Europeia encontra-se assente "nos valores indivisíveis e universais da dignidade do ser humano, da liberdade, da igualdade e da solidariedade", colocando "o ser humano do cerne [de ação da União Europeia]."[140] A ideia subjacente aos chamados "direitos fundamentais" é, assim, a ideia de que cada indivíduo humano tem o direito a ver respeitados os seus direitos e liberdades—incluindo desde os seus direitos civis e políticos, até aos seus direitos económicos e sociais (*ver, inter alia,* NICKEL, 2007, p. 9)—pelo simples facto de ser humano (*ver, inter alia,* GARDNER, 2007). Entre estes direitos fundamentais, encontram-se, então, o direito à vida, o direito à proteção de dados pessoais e o direito à não discriminação, para dar apenas alguns exemplos.

Qual é, então, a diferença entre direitos fundamentais e direitos humanos? Ao passo que os direitos fundamentais são tradicionalmente associados a proteções constitucionais de caráter nacional, os direitos humanos são universais e estão tipicamente ligados ao direito internacional. Assim, a proteção dos direitos inerentes à condição humana a nível nacional é geralmente feita no âmbito das constituições nacionais (e sob a bandeira de "direitos fundamentais"), ao mesmo tempo que a proteção desses mesmos direitos a nível internacional é feita através de instrumentos do direito internacional (e tipicamente por referência ao conceito de "direitos humanos"). No contexto Europeu, a proteção

[139] Fontes importantes para a discussão do conceito e regime de proteção aplicável aos direitos fundamentais e humanos incluem, *ia*, BANTEKAS e OETTE, 2024; BEITZ, 2009; BUCHANNA, 2013; GRIFFIN, 2008; MOECKLI *et al*, 2022; e NICKEL, 2007.

[140] *Ver* o Preâmbulo da Carta.

dada a estes direitos é feita tanto por referência à expressão "direitos humanos" — designadamente em sede da Convenção Europeia de Direitos Humanos — como por referência à expressão "direitos fundamentais" — nomeadamente na Carta (presumivelmente refletindo as ambições constitucionais da União Europeia).[141]

Em última instância, a própria União Europeia — através da sua Agência dos Direitos Fundamentais ("European Union Agency for Fundamental Rights" ou "FRA") — reconhece que tanto a expressão "direitos fundamentais" como a expressão "direitos humanos" têm "em larga medida a mesma substância" (FRA, 2024). Assim, mais importante do que as questões de terminologia subjacentes à preferência pela expressão "direitos fundamentais" em detrimento da expressão "direitos humanos" é a análise do nível de proteção oferecido a uns e a outros no espaço Europeu — tanto ao nível da União Europeia, como no contexto mais alargado da Europa-continente.

2. A proteção dos direitos fundamentais no espaço Europeu

A proteção dos direitos fundamentais no espaço Europeu, e, em particular, ao nível da União Europeia, assenta numa arquitetura institucional "singularmente complexa" (MUIR, 2014, p. 219). Os dois instrumentos de direito internacional mais relevantes[142] neste contexto são, ao nível da União Europeia, a Carta e, no contexto espacial mais abrangente da Europa continente, a Convenção Europeia[143] — da qual a União Europeia é parte desde 2020, em conformidade com os requerimentos do Tratado de Lisboa.[144] Também

[141] Para uma discussão mais aprofundada das ambições constitucionais da União Europeia, veja-se, a título de exemplo, WALKER, 2024. Particularmente no contexto do chamado "Direito Digital" veja-se, em particular, CELESTE, 2024.

[142] A estes dois instrumentos juntam-se, ao nível da União Europeia, os princípios gerais da União Europeia com relevância para os direitos fundamentais e os vários instrumentos legislativos da União Europeia com implicações ao nível da proteção dos direitos fundamentais (ver MUIR, 2014, pp. 219-220) — e, de alguma forma, o próprio Regulamento Europeu da Inteligência Artificial (*ver infra*).

[143] Em complemento à Convenção Europeia, o Conselho da Europa aprovou também 7 protocolos (Protocolo Adicional e Protocolos n.º 4, 6, 7 , 12, 13 e 16) — aos quais se juntam um número de acordos, convenções, cartas e protocolos adicionais especializados.

[144] Na sua origem, a Convenção Europeia dos Direitos Humanos era mera fonte de inspiração para a União Europeia — que apenas se torna signatária da Convenção (e a ela efetivamente vinculada) no seguimento da entrada em vigor do Tratado de Lisboa. Para uma discussão, ver, entre outros, MUIR, 2014, p. 219).

relevantes no contexto Europeu são, de um lado, os instrumentos de carácter mais universal, como a Declaração Universal dos Direitos Humanos das Nações Unidas[145] (a que se juntam, por exemplo, a Declaração dos Direitos das Crianças[146] e a Convenção sobre os Direitos das Pessoas com Deficiência[147])—e, de outro lado, os instrumentos de direitos humanos e fundamentais em vigor nos vários países Europeus.[148]

E como funciona a proteção destes direitos fundamentais ou humanos? No contexto Europeu, a proteção dos direitos fundamentais é feita através de instrumentos jurídicos que—à semelhança de instrumentos jurídicos de proteção de direitos fundamentais e humanos vigentes noutras geografias—apresentam três características distintivas principais, referentes, nomeadamente: *(i)* aos destinatários das obrigações que deles resultam; *(ii)* à sua interpretação; e *(iii)* às limitações às interferências com direitos fundamentais deles constantes.[149] No que toca *(i)* ao campo de aplicação subjetivo dos direitos fundamentais e humanos, cumpre notar que tais direitos são tipicamente oponíveis a Estados, às autoridades públicas (tais como governos, tribunais, e autoridades locais) através das quais atuam estes Estados—e, em determinadas circunstâncias, a entidades

[145] *Ver* a Declaração Universal dos Direitos Humanos adotada pela Assembleia Geral das Nações Unidas em 10 de dezembro 1948, e disponível para consulta na sua versão portuguesa em <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos> acedido a 30 de setembro de 2024.

[146] *Ver* a Declaração dos Direitos das Crianças adotada pela Assembleia Geral das Nações Unidas em 20 de novembro de 1989, e disponível para consulta na sua versão portuguesa em < https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca> acedido a 30 de setembro de 2024.

[147] *Ver* a Convenção sobre os Direitos das Pessoas com Deficiência adotada pela Assembleia Geral das Nações Unidas em 13 de dezembro de 2006, e disponível para consulta na sua versão portuguesa em < https://www.unicef.org/brazil/convencao-sobre-os-direitos-das-pessoas-com-deficiencia> acedido a 30 de setembro de 2024.

[148] Veja-se, a título de exemplo, o *Human Rights Act* 1998 do Reino Unido—embora a maioria dos países europeus consagre estes direitos humanos nas suas constituições escritas, nesses casos sob a figura dos tais "direitos fundamentais").

[149] Estas três características encontram-se refletidas nos artigos 51.º a 54.º da Carta, mas encontram paralelo noutros instrumentos de proteção dos direitos fundamentais e humanos. Vejam-se, designadamente, o campo de aplicação subjetivo, as regras de interpretação especial e os limites à modificação dos direitos fundamentais aplicáveis ao nível de convenções de carácter universal como a Declaração Universal dos Direitos Humanos das Nações Unidas (*ver,* nomeadamente, os artigos 29.º - 30.º da Declaração), e de outras convenções regionais, como a Convenção Americana sobre os Direitos Humanos (*ver,* em particular, os artigos 1.º - 2.º e 27.º - 31.º da Convenção).

privadas que prestem serviços públicos.[150] No que respeita *(ii)* à interpretação dos direitos fundamentais constantes destes instrumentos, esta é frequentemente sujeita a regras especiais e que têm em atenção, designadamente, as disposições de outros instrumentos jurídicos (de carácter internacional ou nacional) que versem sobre os mesmos direitos. Finalmente, no que concerne *(iii)* às limitações às interferências com direitos fundamentais, os instrumentos de defesa dos direitos humanos vigentes no espaço Europeu apenas permitem tais interferências em circunstâncias muito específicas—nomeadamente quando essas interferências: *(a)* se encontrem previstas na lei; *(b)* sirvam um interesse geral reconhecido concorrente; e *(c)* sejam proporcionais, designadamente no contexto de uma sociedade democrática.[151]

Um exemplo ajuda a ilustrar como é que estas limitações às interferências com direitos fundamentais funcionam na prática. No contexto da União Europeia, uma medida—tal como a obrigação de apresentar um documento de identificação com fotografia na travessia de fronteiras—que interfira, designadamente, com os direitos fundamentais ao respeito pela vida privada e familiar,[152] à proteção de dados pessoais,[153] ou à livre circulação de pessoas[154] deve *(a)* constar de instrumento legal. Neste caso, são relevantes, designadamente, a Diretiva 2004/38/CE[155] (que estabelece, no seu artigo 5.º, que a entrada de cidadãos da União Europeia nos seus vários Estados Membros pode

[150] Por exemplo, a Carta dos Direitos Fundamentais da União Europeia tem por destinatários "as instituições, órgãos e organismos da União, na observância do princípio da subsidiariedade, bem como os Estados-Membros...quando apliquem o direito da União" (*ver* o Artigo 51.º da Carta).

[151] Para além disso, alguns instrumentos—como é o caso, por exemplo, da Convenção Europeia dos Direitos Humanos – contêm direitos humanos que são absolutos e que, nesses termos, não podem ser de nenhuma forma restringidos. Veja-se, em particular, o caso da proibição da tortura constante do Artigo 3.º da Convenção Europeia e da proibição da escravatura e do trabalho forçado constante do Artigo 4.º da Convenção Europeia

[152] *Ver*, por exemplo, o Artigo 7.º da Carta e o Artigo 8.º da Convenção Europeia.

[153] *Ver*, por exemplo, o Artigo 8.º da Carta.

[154] *Ver*, por exemplo, o Artigo 45.º da Carta e o Artigo 2.º do Protocolo n.º 4 da Convenção Europeia.

[155] Diretiva 2004/38/CE do Parlamento Europeu e do Conselho de 29 de abril de 2004 relativa ao direito de livre circulação e residência dos cidadãos da União e dos membros das suas famílias no território dos Estados-Membros, que altera o Regulamento (CEE) n.º 1612/68 e que revoga as Diretivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE e 93/96/CEE ("Diretiva 2004/38/CE")—designadamente o seu Considerando (22).

ser feita depender da apresentação de documento de identificação válido), e o Regulamento (UE) 2019/1157[156] (que reforça a segurança dos cartões de identificação dos cidadãos da União Europeia). Tal interferência deve, igualmente, *(b)* servir um interesse geral concorrente com o interesse na proteção da privacidade e dos dados pessoais—neste caso, o interesse de "garantir a segurança dos...povos [da União Europeia]."[157] Finalmente, uma interferência desta natureza deve *(c)* ser necessária no contexto de uma sociedade democrática—ou, mais precisamente, deve ser capaz de passar um teste de proporcionalidade que demonstre que a restrição em causa é indispensável e não vai para além do que é estritamente necessário para a prossecução da finalidade que lhe subjaz. Neste caso, veja-se, a título de exemplo, que a recolha de dados constantes de cartões de identificação é necessariamente feita em segurança,[158] e apenas pode servir para fins de verificação da autenticidade dos documentos em causa e da identidade do titular[159]—e para nenhuns outros.[160]

No espaço Europeu, a proteção dos direitos fundamentais e as medidas que limitam a interferência com direitos fundamentais—no exemplo *supra*, com os direitos fundamentais ao respeito pela vida privada e familiar e à proteção de dados pessoais[161]—não são apenas asseguradas pelos instrumentos legais que

---

[156] *Ver* o Regulamento (UE) 2019/1157 do Parlamento Europeu e do Conselho de 20 de junho de 2019 que visa reforçar a segurança dos bilhetes de identidade dos cidadãos da União e dos títulos de residência emitidos aos cidadãos da União e seus familiares que exercem o direito à livre circulação ("Regulamento (UE) 2019/1157")—em particular o seu Considerando (1).

[157] *Ver* o Considerando (1) do Regulamento (UE) 2019/1157.

[158] *Ver* o Artigo 10.º do Regulamento (UE) 2019/1157.

[159] *Ver* o Artigo 11.º do Regulamento (UE) 2019/1157.

[160] Outros instrumentos jurídicos comunitários relevantes em matéria de proteção de dados, incluem—para além 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" ou "RGPD")—a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados.

[161] Como vimos *supra*, outro direito fundamental relevante neste contexto—e especificamente relevante no contexto da União Europeia—é o direito à livre circulação de pessoas, consagrado no Artigo 45.º da Carta.

enunciam esses direitos (tais como a Carta, ou a Convenção Europeia). Cada vez mais, a defesa dos direitos fundamentais aparece como preocupação central de instrumentos comunitários sectoriais (MUIR, 2014, p. 220). A título de exemplo—e atentando novamente na exigência da partilha de dados de identificação pessoal na travessia de fronteiras—cumpre notar que também o Regulamento Geral Europeu sobre a Proteção de Dados ("RGPD") se propõe a "defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais",[162] sujeitando o tratamento de determinadas categorias de dados pessoais a regras particularmente exigentes[163] (UFERT, 2020, pp. 1092 ss.). Do mesmo modo, e sendo a captura e utilização de dados pessoais na travessia de fronteiras um dos "casos de utilização" mais importantes da Inteligência Artificial—e, designadamente, um dos "casos de utilização" que melhor ilustra os riscos para os direitos fundamentais criados por estas tecnologias[164]—também o Regulamento Europeu da Inteligência Artificial versa sobre práticas de Inteligência Artificial que "classifiquem individualmente pessoas singulares com base nos seus dados biométricos"[165] e procedam à "identificação biométrica à distância em «tempo real» em espaços acessíveis ao público".[166]

Estas (e outras) regras no Regulamento Europeu da Inteligência Artificial que versam sobre aplicações de Inteligência Artificial que criam risco para os direitos fundamentais têm por objetivo explícito assegurar a proteção desses direitos[167]—mas quão eficaz é o Regulamento no cumprimento deste seu objetivo? A próxima seção examina em detalhe as várias manifestações do conceito de "direitos fundamentais" no Regulamento Europeu. Desta forma, a Secção III do presente capítulo representa o último passo necessário antes do exercício conduzido na Secção IV—a qual confronta as características do Regulamento Europeu da Inteligência Artificial que se prendem com a proteção

[162] *Ver* o Artigo 1.º, n.º 2 do RGPD.
[163] *Ver* o Artigo 9.º do RGPD.
[164] Para uma discussão mais aprofundada, *ver* Secção I.1 *supra*.
[165] *Ver* o Artigo 5.º, n.º1(g) do Regulamento Europeu da Inteligência Artificial.
[166] *Ver* o Artigo 5.º, n.º1(h) do Regulamento Europeu da Inteligência Artificial.
[167] *Ver* o Artigo 1.º, n.º1 do Regulamento Europeu da Inteligência Artificial.

de direitos fundamentais com as características típicas dos instrumentos tradicionalmente utilizados no espaço Europeu para proteção desses direitos, criando assim condições para avaliar a efetividade da contribuição feita pelo Regulamento para essa proteção.

III. Os direitos fundamentais no Regulamento Europeu da Inteligência Artificial

As secções anteriores demonstram que muitas das aplicações de Inteligência Artificial postas já em prática na nova Economia Digital encerram um risco significativo para os direitos fundamentais inerentes à condição humana e amplamente reconhecidos como tal, designadamente no espaço Europeu. Foi também notado que esse risco serve de inspiração explícita a vários instrumentos regulatórios aplicáveis à Inteligência Artificial que têm vindo a aparecer no contexto Europeu—nomeadamente, ao Regulamento Europeu da Inteligência Artificial. Cabe agora analisar de que forma é que o Regulamento trata a questão dos direitos fundamentais, antes de avaliar a relevância que este poderá vir a assumir na proteção destes direitos, à medida a que as aplicações de Inteligência Artificial se tornam cada vez mais presentes no espaço Europeu.

À primeira vista, o Regulamento Europeu da Inteligência Artificial apresenta-se como um regulamento de segurança de produtos, assente numa lógica que, como veremos, é fundamentalmente distinta da lógica que habitualmente preside à proteção dos direitos humanos, designadamente ao nível da Europa (em sentido semelhante, ALMADA e PETIT, 2023; SOUSA E SILVA, 2024; e WENDEHORST, 2022).[168] De facto, os princípios e regras que constam do *AI Act* são desenhados por referência a aplicações e casos de utilização de Inteligência Artificial, em vez de se referirem às tecnologias de Inteligência Artificial em si. Por outras palavras, o objeto de regulação do Regulamento não é a Inteligência Artificial enquanto tecnologia, mas os vários produtos de

[168] Esta lógica foi já descrita na Secção II.2 *supra*.

Inteligência Artificial que preocupam o legislador comunitário[169]—e que, nos termos do Regulamento, ficam assim sujeitos a determinadas regras de segurança.[170]

Ao mesmo tempo, o Regulamento Europeu da Inteligência Artificial também se posiciona explicitamente como um instrumento de proteção de direitos humanos—utilizando o conceito de "direitos fundamentais" de sete formas distintas: *(1)* na determinação dos seus objetivos, *(2)* na determinação dos termos da sua aplicação, *(3)* no desenho do sistema de classificação de risco que aí se impõe às aplicações de Inteligência Artificial, *(4)* na desenvolvimento do conteúdo dos deveres impostos aos destinatários do Regulamento, *(5)* na determinação dos direitos conferidos a quem se vê afetado (ou potencialmente) afetado por aplicações de Inteligência Artificial abrangidas pelo Regulamento, *(6)* no desenho do sistema de governação subjacente ao Regulamento, e, finalmente *(7)* na determinação das regras e limites que governam as alterações que podem ser feitas ao Regulamento Europeu.

A presente secção examina sucessivamente cada uma das manifestações do conceito de "direitos fundamentais" no Regulamento Europeu da Inteligência Artificial (*Secção III*)—deixando para a secção seguinte a avaliação global do papel que pode vir a ser efetivamente desempenhado pelo *AI Act* na proteção desses direitos (*Secção IV*).

1. Direitos fundamentais e os objetivos do Regulamento

A manifestação mais óbvia do conceito de "direitos fundamentais" no Regulamento Europeu da Inteligência Artificial prende-se com a definição dos objetivos principais deste Regulamento. De facto, a proteção dos direitos

[169] Este enfoque específico colocado nas aplicações de Inteligência Artificial—por oposição à tecnologia da Inteligência Artificial—permite ao *AI Act* apresentar-se, assim, como um regulamento "tecnologicamente neutro", ainda que esta neutralidade seja de alguma forma posta em causa pelas regras do Regulamento que se aplicam aos modelos de Inteligência Artificial de finalidade geral (*ver* os Artigos 1.º, n.º2, alínea f) e 2.º. n.º1, alínea a) do Regulamento Europeu da Inteligência Artificial). Tal como o nome indica, tais modelos têm a "capacidade de servir para diversas finalidades, tanto para utilização direta como para integração noutros sistemas de IA" (*ver* o Artigo 3.º, 66) do Regulamento Europeu da Inteligência Artificial).

[170] Para uma discussão, *ver* a Secção III.3 *infra*.

fundamentais surge como um dos dois objetivos essenciais do *AI Act*, os quais incluem, por um lado (*i*) a promoção do mercado interno—em particular, o desenvolvimento, a utilização, e a adoção da Inteligência Artificial no mercado interno—e, simultaneamente, *(ii)* a proteção dos direitos fundamentais, em linha com os instrumentos de direitos humanos aplicáveis no espaço Europeu.[171]

Esta procura concomitante pela promoção do mercado interno e pela proteção dos direitos fundamentais de quem entra em contacto com aplicações de Inteligência Artificial abrangidas pelo Regulamento é subsumível ao binómio inovação/segurança que tantas vezes preside às discussões sobre desenvolvimento tecnológico e regulamentação (*ver, inter alia,* BRAUN, 1994, pp. 95 ss.). Notavelmente, este binómio atravessa todo o Regulamento, fazendo várias aparições nos seus Considerandos (*inter alia*, Considerandos (1)-(10), (20), (65), (75), (92), (96) e (176)),[172] e aparecendo de forma particularmente expressiva na definição dos objetivos do *AI Act*, que o seu Artigo 1.º define nos seguintes termos:

> A finalidade do presente regulamento é melhorar o funcionamento do mercado interno e promover a adoção de uma inteligência artificial (IA) centrada no ser humano e de confiança, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança e dos direitos fundamentais consagrados na Carta, incluindo a democracia, o Estado de direito e a proteção do ambiente, contra os efeitos nocivos dos sistemas de IA na União, bem como apoiar a inovação.[173]

A aparente simplicidade com que o Regulamento descreve este objetivo duplo de promoção do mercado interno e da inovação, por um lado, e de proteção dos direitos fundamentais e da segurança, por outro lado, esconde uma série de desafios, subsumíveis a duas categorias principais: primeiro, a problemas de "*naming*"—ou identificação—e, em segundo lugar, a problemas de "*claiming*"—ou responsabilização[174] (HARKENS, 2024).

---

[171] *Ver* o Artigo 1.º, n.º1 do Regulamento Europeu da Inteligência Artificial.
[172] Destes (e doutros) Considerandos constam ainda várias referências à Carta dos Direitos Fundamentais da União Europeia (*ver,* em particular, Considerandos (1), (2), (6), (7), (27), (28), (48), (59), (62), (63), (134) e (176)).
[173] *Ver* o Artigo 1.º, n.º1 do Regulamento Europeu da Inteligência Artificial.
[174] A importância dos sistemas de responsabilização na proteção dos direitos fundamentais, designadamente no contexto da regulação da Inteligência Artificial é discutida em maior detalhe em WENDEHORST, 2022, pp. 192 ss..

Os desafios subsumíveis ao problema de "*naming*" prendem-se com: *(i)* as dificuldades de identificação dos riscos de interferência com direitos fundamentais criados pelas aplicações de Inteligência Artificial, em particular na presença das assimetrias informativas típicas de sistemas do tipo "*black box*";[175] *(ii)* as dificuldades de determinação dos termos em que esses riscos se podem materializar (e em que podem ser mitigados); e, finalmente, com *(iii)* as dificuldades de identificação e governação das entidades responsáveis por gerir estes riscos. Já os desafios que podem ser englobados na categoria de "*claiming*" incluem: *(i)* as dificuldades na implementação de deveres de transparência que possam assegurar efetiva responsabilização pela violação de direitos fundamentais no âmbito do Regulamento; e *(ii)* as questões levantadas pela implementação de vias legais de reação às interferências com direitos fundamentais—incluindo a respetiva publicitação junto do público e de instituições de defesa destes direitos.

2. Direitos fundamentais e a aplicação do Regulamento

O conceito de "direitos fundamentais" também é utilizado pelo Regulamento para clarificar os termos em que se dá a aplicação deste instrumento—incluindo questões relativas à sua relação com outros instrumentos jurídicos, à sua interpretação, e ao seu campo de aplicação subjetivo.

No que toca à relação entre o *AI Act* e outros instrumentos jurídicos, o Regulamento é perentório em utilizar o conceito de "direitos fundamentais" para esclarecer que o *AI Act* não prejudica a aplicação de outros instrumentos criadores de direitos fundamentais reconhecidos pelos Estados membros e ao nível da União Europeia.[176] No campo da interpretação, esclarece-se ainda que o *AI Act* "deverá ser aplicado em conformidade com os valores da União

[175] Para uma discussão do problema "black box" associado com as tecnologias de Inteligência Artificial, *ver* BATHEE, 2018, pp. 889 ss.).

[176] *Ver* o Considerando (9) do Regulamento Europeu da Inteligência Artificial, o qual esclarece que o AI Act "não prejudica a aplicação de instrumentos criadores de direitos fundamentais reconhecidos pelos Estados membros e a nível da União."

consagrados na Carta"[177] e "desenvolvido em conformidade com (...) os direitos e liberdades fundamentais consagrados nos Tratados e (...) com a Carta"[178]—devendo as regras aplicáveis aos sistemas de Inteligência Artificial classificados pelo Regulamento como sendo de risco elevado ser, também elas, "coerentes com a Carta."[179]

Finalmente, e no que toca ao campo de aplicação subjetivo do Regulamento, cumpre notar que o conceito de "direitos fundamentais" é utilizado para excluir explicitamente do seu âmbito "autoridades públicas de países terceiros [e] organizações internacionais abrangidas pelo âmbito do [Regulamento] (...) quando essas autoridades ou organizações usem sistemas de IA no âmbito da cooperação internacional ou de acordos internacionais para efeitos de cooperação policial e judiciária com a União ou com um ou vários Estados-Membros" na medida em que—e *apenas* na medida em que—esses países ou organizações apresentem "salvaguardas adequadas em matéria de proteção de direitos e liberdades fundamentais das pessoas."[180] Apesar desta exceção, cumpre aqui notar que os destinatários do *AI Act* não incluem apenas autoridades e organizações de caráter público; conforme esclarece a Comissão Europeia, o enquadramento jurídico constante do Regulamento aplica-se "tanto a intervenientes públicos como privados estabelecidos dentro ou fora da UE"—contando, naturalmente, que "o sistema de IA em causa seja colocado no mercado da União ou que a sua utilização tenha impacto em pessoas localizadas na UE" (COMISSÃO EUROPEIA, 2024). Assim, o objetivo de proteção dos direitos fundamentais não parece ter tido um impacto decisivo na determinação do âmbito de aplicação subjetivo do Regulamento, pelo menos no sentido de o converter num instrumento puro de proteção de direitos fundamentais subsumível a uma lógica de vinculação de autoridades públicas (ou, em

[177] *Ver* o Considerando (2) do Regulamento Europeu da Inteligência Artificial.
[178] *Ver* o Considerando (6) do Regulamento Europeu da Inteligência Artificial.
[179] *Ver* o Considerando (7) do Regulamento Europeu da Inteligência Artificial.
[180] *Ver* o Considerando (22) do Regulamento Europeu da Inteligência Artificial.

circunstâncias limitadas, de entidades privadas que prestem serviços públicos).[181]

3. Direitos fundamentais e o sistema de classificação de risco aplicável às aplicações de Inteligência Artificial no âmbito do Regulamento

À primeira vista, o conceito de "direitos fundamentais" parece assumir particular importância para o funcionamento do sistema de classificação de risco de aplicações de Inteligência Artificial que se encontra no centro do Regulamento Europeu da Inteligência Artificial—afirmando mesmo o Regulamento que: "A dimensão das repercussões negativas causadas pelo sistema de IA nos direitos fundamentais protegidos pela Carta é particularmente importante quando se classifica um sistema de IA como sendo de risco elevado."[182]

Mas em que termos é que o objetivo da proteção de direitos fundamentais molda este sistema de classificação? Antes de mais, cumpre reconhecer que o sistema de classificação de risco proposto pelo Regulamento Europeu da Inteligência Artificial é, atualmente, a grande carta de apresentação do Regulamento Europeu—e o produto mais visível da abordagem à regulação da Inteligência Artificial "baseada no risco" subjacente ao *AI Act* (UNESCO, 2024, p. 35). A ideia de uma abordagem "baseada no risco" surge, assim, nos Considerandos do Ato como "a base para um conjunto proporcionado e eficaz de regras vinculativas"[183]—cujo conteúdo é adaptado "à intensidade e ao âmbito dos riscos que podem ser criados pelos sistemas de IA."[184]

Esta abordagem baseada no risco tem vindo a ser adotada noutras áreas da regulação do mundo digital—incluindo o Regulamento Europeu dos Serviços Digitais[185] e o Regulamento Europeu dos Mercados Digitais[186]—sendo justificada

[181] *Ver* a discussão na Secção II.2 *supra*.
[182] *Ver* Considerando (48) do Regulamento Europeu da Inteligência Artificial.
[183] *Ver* Considerando (27) do Regulamento Europeu da Inteligência Artificial.
[184] *Ver* Considerando (26) do Regulamento Europeu da Inteligência Artificial.
[185] 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 Europeu dos Serviços Digitais").
[186] 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 Europeu dos Mercados Digitais").

principalmente em razão das assimetrias informativas e dos ciclos de inovação rápidos que marcam a economia digital (HUSOVEC, 2024, pp. 274-276). No caso específico do Regulamento Europeu da Inteligência Artificial, esta abordagem leva: *(i)* à proibição de determinadas aplicações ou casos de utilização de Inteligência Artificial de risco inaceitável; *(ii)* à imposição de requisitos especialmente exigentes a sistemas de Inteligência Artificial de risco elevado;[187] e *(iii)* à imposição de obrigações mínimas de transparência (designadamente) a aplicações de Inteligência Artificial de risco limitado.[188] Numa lógica de proporcionalidade, os restantes sistemas de Inteligência Artificial com presença no espaço Europeu ficam essencialmente cobertos por outros instrumentos regulatórios aplicáveis a nível comunitário e nacional (como a legislação genericamente aplicável à segurança de produtos).

O grande desafio subjacente a esta abordagem baseada no risco reside, por um lado, nas dificuldades inerentes à definição do conceito de "risco"—a que o Regulamento se refere como "a combinação da probabilidade de ocorrência de danos com a gravidade desses danos"[189]—e, em particular, nas especiais dificuldades que presidem à identificação e medição do risco criado por aplicações de Inteligência Artificial.[190]

Ora, é precisamente aqui que o conceito de "direitos fundamentais" volta a ser utilizado pelo Regulamento—o qual parece fazer o seu sistema de

[187] Na prática, a Comissão Europeia estima que a classificação de alto risco—que atrai a maior parte das regras constantes do *AI Act*—apenas se venha a aplicar um número muito limitado dos sistemas de Inteligência Artificial em uso na União Europeia (EUROPEAN COMMISSION, 2024), mas isso não impediu o rol de críticas que têm sido tecidas às regras aplicáveis aos sistemas de risco elevado e ao próprio sistema de classificação de risco (*ver, inter alia,* VEALE e ZUIDERVEEN BORGESIUS, 2021).

[188] Notavelmente, e apesar de o sistema de classificação de risco subjacente ao Regulamento Europeu da Inteligência Artificial ser invariavelmente representado sob a forma de pirâmide (*ver, inter alia,* EUROPEAN COMMISSION, 2024), nada parece impedir que um sistema de Inteligência Artificial esteja simultaneamente sujeito às obrigações que resultam da sua classificação como sistema de risco elevado e às obrigações mínimas de transparência aplicáveis, em particular, às aplicações de Inteligência Artificial de risco limitado.

[189] *Ver* o Artigo 3.º n.º 2 do Regulamento Europeu da Inteligência Artificial.

[190] Além de amplamente documentadas na doutrina, estas dificuldades têm sido também reconhecidas pelas próprias agências da União Europeia, tendo a FRA assumido recentemente a tarefa de levar a cabo uma análise empírica dos melhores métodos para medir o risco criado pelas aplicações de Inteligência Artificial para direitos fundamentais (*ver* FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2024)

classificação de risco depender do grau de ameaça que as várias aplicações de Inteligência Artificial representam para os direitos fundamentais. Dentro dessa lógica, as práticas absolutamente inaceitáveis serão aquelas que criam um risco também ele inaceitável para os direitos fundamentais—e que, seja devido à probabilidade da sua ocorrência, devido à gravidade dos danos advenientes da sua materialização (ou a uma combinação das duas coisas), ameaçam de tal forma os direitos fundamentais que mesmo a sua mitigação se torna insuficiente. Já os sistemas de risco elevado serão aqueles que criam uma ameaça significativa—mas não inteiramente inaceitável—para os direitos fundamentais. Nesse sentido, vejam-se os Considerandos (28), (32), (43), (46), (48), (52), (53) e (57)-(59) do *AI Act*—e, em particular, o seu Artigo 6.º[191] quando refere, nomeadamente, que "um sistema de IA (…) não pode ser considerado de risco elevado se não representar um risco significativo de danos para (…) os direitos fundamentais das pessoas singulares".[192]

Ao mesmo tempo, há motivos para argumentar que a centralidade do conceito de "direitos fundamentais" para o sistema de classificação de risco que serve de base ao Regulamento Europeu é mais aparente que real. Em primeiro lugar, cumpre notar que—ao contrário do que acontece com outros instrumentos de Direito Comunitário—as referências aos "direitos fundamentais" feitas pelo *AI Act* são tipicamente referências muito genéricas e que não especificam os direitos fundamentais concretos por elas abrangidos. Em contraste, o RGPD, por exemplo, encerra medidas de proteção específicas do direito fundamental à proteção de dados pessoais,[193] e o Regulamento dos Serviços Digitais propõe-se

[191] Correspondentemente, e como se verá melhor na Secção III.7 *infra*, também a alteração da lista de sistemas de risco elevado constantes do Anexo III do Regulamento Europeu depende, em particular, do risco que estes representam para os direitos fundamentais (*ver* o Artigo 7.º, n.º1 alínea b) e n.º2, alínea e) do Regulamento Europeu da Inteligência Artificial.).

[192] Os n.ºs 3 e 4.º do Artigo 6.º do Regulamento têm vindo a ser objeto de crítica por criarem *loopholes* que permitem aos destinatários do *AI Act* escapar mais facilmente às obrigações que este impõe (para uma discussão *ver, inter alia,* ALMADA e PETIT, 2023, p. 9). Ao mesmo tempo, *cfr* o Artigo 6.º n.º8 do Regulamento, o qual dá resposta pelo menos parcial a essas preocupações.

[193] *Ver* o Considerando (1) e, em particular, o Artigo 1.º, n.º2 e os vários Artigos pertencentes ao Capítulo II do RGPD.

a proteger concretamente o direito fundamental à liberdade de expressão (no mesmo sentido, *ver* ALMADA e PETIT, p. 11).[194]

Em segundo lugar, vale a pena assinalar que as referências feitas pelo Regulamento Europeu da Inteligência Artificial aos "direitos fundamentais" raras vezes emprestam relevância autónoma a esse conceito, o qual aparece quase sempre acompanhado de referências à necessidade de proteção da saúde e da segurança—valores tradicionalmente associados à regulamentação de produtos (NOTTAGE, 2018, pp. 231 ss.). Assim, alguma doutrina tem vindo a apontar ao *AI Act* um viés significativo no sentido de favorecer o objetivo de promoção do mercado interno (designadamente através do desenvolvimento, da utilização, e da adoção da Inteligência Artificial nesse mercado), em detrimento do objetivo de proteção dos direitos fundamentais—em claro contraste com o que acontece tanto com outros regulamentos comunitários que se propõem a defender direitos fundamentais específicos, como, naturalmente, com instrumentos tradicionais de proteção dos direitos fundamentais como a Carta ou a Convenção Europeia.

4. Direitos fundamentais e os deveres resultantes do Regulamento

A relevância do conceito de "direitos fundamentais" para o Regulamento Europeu de Inteligência Artificial manifesta-se também no conteúdo das várias obrigações que dele resultam, em particular no que toca aos sistemas de Inteligência Artificial classificados como sendo de "risco elevado".[195] Tais

[194] *Ver* os Artigos 14.º, 34.º, 48.º e 91.º do Regulamento dos Serviços Digitais.

[195] Neste contexto, são destinatários (das obrigações) do Regulamento Europeu da Inteligência Artificial (a) os prestadores que coloquem no mercado ou coloquem em serviço sistemas de IA ou que coloquem no mercado modelos de IA de finalidade geral no território da União, independentemente de estarem estabelecidos ou localizados na União ou num país terceiro; (b) os responsáveis pela implantação de sistemas de IA que tenham o seu local de estabelecimento ou que estejam localizados na União; (c) os prestadores e responsáveis pela implantação de sistemas de IA que tenham o seu local de estabelecimento ou estejam localizados num país terceiro, se o resultado produzido pelo sistema de IA for utilizado na União; (d) os importadores e distribuidores de sistemas de IA; (e) os fabricantes de produtos que coloquem no mercado ou coloquem em serviço um sistema de IA juntamente com o seu produto e sob o seu próprio nome ou a sua própria marca; e (f) os mandatários dos prestadores que não estejam estabelecidos na União (*ver* Artigo 2.º n.º1 do Regulamento Europeu da Inteligência Artificial). Atendendo ao sistema de governação que subjaz ao Regulamento, aparecem ainda como destinatários de determinadas obrigações constantes do Regulamento as autoridades nacionais e comunitárias responsáveis pela sua aplicação (*ver*, por exemplo, os Artigos 57.º - 58.º, 77.º ss. e 112.º do Regulamento Europeu da Inteligência Artificial).

obrigações podem ser funcionalmente agrupadas em três categorias: *(i)* deveres aplicáveis em sede de desenvolvimento das aplicações de Inteligência Artificial de risco elevado; *(ii)* deveres aplicáveis em sede de implantação das aplicações de Inteligência Artificial de risco elevado; *e (iii)* deveres aplicáveis em sede de teste das regras aplicáveis às aplicações de Inteligência Artificial de risco elevado ao abrigo do Regulamento.

No momento do (*i*) desenvolvimento das aplicações de Inteligência Artificial cobertas pelo Regulamento, este impõe a criação e implantação de um sistema de gestão de riscos—o qual, para o que interessa à presente análise, deve abranger, designadamente, "a identificação e análise dos riscos conhecidos e razoavelmente previsíveis que o sistema de IA de risco elevado pode representar para (...) os direitos fundamentais quando é utilizado em conformidade com a sua finalidade prevista."[196] Também durante a fase de desenvolvimento de aplicações de Inteligência Artificial de risco elevado, o Regulamento impõe que quaisquer sistemas que "envolvam o treino de modelos com dados" se baseiem em "conjuntos de dados de treino, validação e teste que cumpram" determinados critérios de qualidade—exigindo, em particular, que tais dados fiquem "sujeitos a práticas de governação e gestão de dados adequadas à finalidade prevista do sistema de IA" e que devem incluir exames "para detetar eventuais enviesamentos suscetíveis de (...) ter repercussões negativas nos direitos fundamentais (...)."[197] Finalmente, o Regulamento manda que os sistemas de IA de alto risco sejam desenvolvidos "de maneira a assegurar que o seu funcionamento seja suficientemente transparente para permitir aos responsáveis pela implantação interpretar os resultados do sistema e utilizá-los de forma adequada"— sendo que as instruções de utilização devem conter, pelo menos, "as características, capacidades e limitações de desempenho do sistema de IA de risco elevado, incluindo: (...) (iii) qualquer circunstância conhecida ou previsível (...) que possa causar [riscos] para os direitos fundamentais."[198]

[196] *Ver* o Artigo 9.º, n.º1 e n.º2 do Regulamento Europeu da Inteligência Artificial.
[197] *Ver* o Artigo 10.º, n.º1 e n.º2, alínea f) do Regulamento Europeu da Inteligência Artificial.
[198] *Ver* o Artigo 13.º, n.º1 e n.º3, alínea b), do Regulamento Europeu da Inteligência Artificial.

Seguidamente, e agora durante a fase de *(ii)* implantação de aplicações de Inteligência Artificial de risco elevado, o Artigo 27.º do *AI Act* obriga à execução de uma avaliação do impacto que a utilização desse sistema possa ter nos direitos fundamentais.[199] Finalmente, e já em sede de *(iii)* teste das regras aplicáveis às aplicações de Inteligência Artificial de risco elevado ao abrigo do Regulamento, os Artigos 57.º e 58.º do *AI Act* obrigam a que os ambientes de testagem da regulamentação da IA a nível nacional permitam identificar e atenuar riscos criados para os direitos fundamentais e para a sociedade em geral.

Em última análise, cumpre notar que, muito embora o Regulamento Europeu remeta efetivamente para o conceito de "direitos fundamentais" em sede de densificação de algumas das obrigações dele constantes, a configuração destes deveres revela, ainda assim, um viés significativo em favor da promoção do mercado interno (e em desfavorecimento da proteção dos direitos fundamentais). Em particular, acompanhamos a doutrina que nota que os deveres aplicáveis no contexto do Regulamento Europeu são sobretudo procedimentais, resultando na aplicação de testes e *standards* que—uma vez cumpridos—são condição suficiente para que a aplicação de Inteligência Artificial continue a circular no mercado. Em contraste claro, os deveres aplicáveis no contexto de outros instrumentos comunitários moldados, também eles, por referência ao conceito de direitos fundamentais—como é o caso do RGPD e do DSA—preveem requisitos que obrigam os destinatários desses instrumentos a proteger muito mais ativamente os direitos fundamentais que os motivam (no mesmo sentido, *ver* ALMADA e PETIT, 2023 pp. 20 ss.). A título de exemplo, veja-se o artigo 25.º do RGPD, o qual obriga especificamente os

[199] A avaliação prevista no Artigo 27.º do Ato deve incluir "(a) uma descrição dos processos do responsável pela implantação em que o sistema de IA de risco elevado seja utilizado de acordo com a sua finalidade prevista; (b) uma descrição do período em que o sistema de IA de risco elevado se destina a ser utilizado e com que frequência; (c) as categorias de pessoas singulares e grupos suscetíveis de serem afetados no contexto específico de utilização do sistema; (d) os riscos específicos de danos suscetíveis de terem impacto nas categorias de pessoas singulares ou grupos de pessoas [previamente] identificadas (...), tendo em conta as informações facultadas (...) nos termos do artigo 13.º [do Regulamento]; (e) uma descrição da aplicação das medidas de supervisão humana de acordo com as instruções de utilização; e (f) as medidas a tomar caso esses riscos se materializem, incluindo as disposições relativas à governação interna e aos mecanismos de apresentação de queixas" (*ver* o Artigo 27.º do Regulamento).

responsáveis pelo tratamento de dados a adotar medidas técnicas e organizativas adequadas para "aplicar com eficácia os princípios da proteção de dados" for forma a "prote[ger] os direitos dos titulares dos dados".[200]

5. Direitos fundamentais e os direitos resultantes do Regulamento

Conforme assinalado *supra*, o *AI Act* é sobretudo um regulamento de segurança de produtos. Nesses termos, a sua arquitetura assenta mais na imposição de obrigações e requerimentos de segurança do que na concessão de direitos aos indivíduos que o Regulamento visa proteger.

Assim, a relevância do conceito de "direitos fundamentais" no contexto do Regulamento Europeu é inevitavelmente limitada pelo facto de este atribuir apenas dois direitos subjetivos a quem veja os seus direitos fundamentais ameaçados por aplicações de Inteligência Artificial: por um lado, *(i)* o direito de apresentar queixa a uma autoridade de fiscalização do mercado nos termos do seu artigo 85.º—o qual assiste a "qualquer pessoa singular ou coletiva que tenha motivos para considerar que houve uma infração às disposições do presente regulamento"—e, por outro lado, *(ii)* o direito a obter explicações sobre decisões individuais—o qual assiste aos indivíduos sujeitos a decisões tomadas por sistemas de Inteligência Artificial de risco elevado e que produzam efeitos jurídicos ou análogos que afetem significativamente essa pessoa (com repercussões negativas nos seus direitos fundamentais).[201]

6. Direitos fundamentais e o sistema de governação subjacente ao Regulamento

Uma das manifestações menos discutidas no conceito de "direitos fundamentais" no Regulamento Europeu da Inteligência Artificial é o impacto que a arquitetura existente de proteção dos direitos fundamentais tem no sistema de governação subjacente ao *AI Act*—designadamente nas relações que se

[200] *Ver* o Artigo 25.º, n.º1 do RGPD.
[201] *Ver* o Artigo 86.º n.º1 do Regulamento Europeu da Inteligência Artificial.

estabelecem entre as entidades comunitárias e de âmbito nacional responsáveis pela aplicação do *AI Act* ou de outros instrumentos jurídicos a ele adjacentes.

Especificamente, o Regulamento Europeu regulamenta a relação entre, de um lado, as autoridades nacionais competentes por supervisionar a aplicação de (partes) do *AI Act*—e, de outro lado, as autoridades e organismos públicos que procedem à defesa dos direitos fundamentais no espaço Europeu. Nos termos dos Considerandos do Regulamento, tais entidades devem atuar em regime de estrita colaboração[202]—sendo que o disposto no Regulamento não pode prejudicar as competências, atribuições, poderes e independência destas últimas.[203] Esta obrigação de colaboração tem a sua manifestação mais clara nos Artigos 77.º e seguintes do Regulamento. Assim, entidades que procedam à defesa dos direitos fundamentais têm poderes para "solicitar e aceder a toda a documentação elaborada ou mantida nos termos do [Regulamento] (...) nos casos em que o acesso a essa documentação for necessário para o exercício dos seus mandatos dentro dos limites das respetivas jurisdições." [204] Para além disso, tais entidades têm ainda o direito a serem informadas de quaisquer riscos para os direitos fundamentais que venham a ser identificados pelas autoridades que vigiam o cumprimento do Regulamento.[205]

7. Direitos fundamentais e os limites à modificação do Regulamento

Finalmente—e em termos particularmente interessantes para uma análise comparativa face ao disposto nos instrumentos de defesa dos direitos humanos tradicionalmente vigentes no espaço Europeu—o *AI Act* utiliza o conceito de "direitos fundamentais" para regulamentar e, crucialmente, estabelecer limites à sua própria revisão.

Desde logo, o Regulamento estabelece que nenhuma revisão sua que leve à alteração das condições que permitem a exclusão de aplicações de Inteligência Artificial da lista de aplicações de risco elevado constantes do seu Anexo III pode

[202] *Ver* o Considerando (139) do Regulamento Europeu da Inteligência Artificial.
[203] *Ver* o Considerando (157) do Regulamento Europeu da Inteligência Artificial.
[204] *Ver* o Artigo 77.º n.º1 do Regulamento Europeu da Inteligência Artificial.
[205] *Ver* o Artigo 79.º n.º2 do Regulamento Europeu da Inteligência Artificial.

conduzir a uma diminuição do nível geral de proteção dos direitos fundamentais previstos no Regulamento. Concretizando, o Artigo 7.º sujeita qualquer alteração do Anexo III a requerimentos adicionais conforme a modificação em causa conduza a um: *(i)* aditamento (ou mero ajuste) de uma aplicação de Inteligência Artificial; ou, em vez disso, a uma *(ii)* remoção de uma das práticas de Inteligência Artificial listadas pelo Regulamento. O (*i*) aditamento (ou mero ajuste) de casos de utilização constantes do Anexo III fica dependente de uma avaliação nos termos da qual o nível de risco que essas aplicações representam para os direitos fundamentais seja tido como equivalente ou superior ao risco já associado aos casos de utilização incluídos no Anexo III.[206] Já a *(ii)* remoção de casos de utilização do Anexo III fica sujeita a condições mais exigentes: por um lado, à condição de que o sistema de Inteligência Artificial em causa tenha deixado de representar um risco significativo para os direitos fundamentais;[207] e, por outro lado, à condição de que a supressão em causa não leve a uma diminuição do "nível geral de proteção da saúde, da segurança e dos direitos fundamentais ao abrigo do direito da União."[208]

Finalmente, o Artigo 112.º do Regulamento Europeu da Inteligência Artificial—que obriga a Comissão Europeia a avaliar anualmente a necessidade de alterar a lista das aplicações de Inteligência Artificial proibidas nos termos do Artigo 5.º e a lista das aplicações de Inteligência Artificial de risco elevado constantes do Anexo III do Regulamento—estabelece que tais exercícios de avaliação devem atender, em especial, ao impacto que essas aplicações possam ter, designadamente, nos direitos fundamentais.

***

[206] *Ver* o Artigo 7.º n.º1, alínea a) do Regulamento Europeu da Inteligência Artificial. Para além disso, apenas podem ser aditados novos casos de utilização ao Anexo III se os sistemas de Inteligência Artificial em causa se destinarem a ser utilizados em qualquer um dos domínios enunciados nesse Anexo (*ver* o n.º 1.º, alínea b) do mesmo Artigo).

[207] *Ver* o Artigo 7.º n.º3, alínea a) do Regulamento Europeu da Inteligência Artificial. Esta avaliação é feita atendendo aos critérios enumerados no n.º2 do mesmo Artigo, e que incluem, em particular, "a medida em que a utilização de um sistema de IA já (...) tenha tido repercussões negativas nos direitos fundamentais ou tenha suscitado preocupações significativas quanto à probabilidade de (...) essas repercussões negativas ocorrerem."

[208] *Ver* o Artigo 7.º n.º3, alínea b) do Regulamento Europeu da Inteligência Artificial.

Em última análise, a presente reflexão demonstra que várias são as manifestações do conceito de "direitos fundamentais" no Regulamento Europeu da Inteligência Artificial—influenciando desde os principais objetivos do Regulamento aos termos em que este pode ser alterado. Ao mesmo tempo, não é claro que as várias remissões feitas pelo Regulamento para os "direitos fundamentais" tenham o condão de o transformar num instrumento de defesa efetiva destes direitos capaz de "assegurar um elevado nível de proteção"[209] desses direitos—pelo menos quando tais remissões são confrontadas com as principais características dos instrumentos de defesa dos direitos fundamentais tradicionalmente vigentes no espaço Europeu. A tarefa de proceder a essa avaliação é deixada para a última Secção deste capítulo.

IV. Conclusão: o nível de proteção assegurado aos direitos fundamentais pelo Regulamento Europeu da Inteligência Artificial

Nenhuma dúvida há de que as tecnologias de Inteligência Artificial podem representar uma ameaça significativa para os direitos fundamentais de quem interage com estas tecnologias. Desde a segurança pública, ao policiamento preditivo, passando pelo *social scoring*, várias (e cada vez mais) são as áreas em que as aplicações de Inteligência Artificial e os direitos humanos entram em rota de colisão. Deste modo, várias são também as propostas legislativas e regulamentares que têm vindo a surgir em resposta a este conflito—e também o Regulamento Europeu da Inteligência Artificial assume para si esta tarefa de proteção dos direitos fundamentais.

Questão distinta é a de saber se o Regulamento Europeu cumpre com as condições necessárias para levar a bom termo a tarefa a que se propõe no seu Artigo 1.º—a de "assegurar um elevado nível de proteção"[210] dos direitos fundamentais ameaçados pelas tecnologias de Inteligência Artificial. De facto, muitas são as manifestações do conceito de "direitos fundamentais" ao longo do

[209] *Ver* o Artigo 1.º n.º1 do Regulamento Europeu da Inteligência Artificial.
[210] *Ver* o Artigo 1.º n.º1 do Regulamento Europeu da Inteligência Artificial.

Regulamento,[211] mas uma análise comparativa entre o Regulamento e os instrumentos jurídicos que tradicionalmente presidem à proteção dos direitos fundamentais no espaço Europeu revela diferenças importantes na forma como uns e outros instrumentos se propõem a defender estes direitos.

Nesta sua última Secção, o presente capítulo contrasta: de um lado, *(i)* as características do Regulamento Europeu que resultam das várias remissões por ele feitas para o conceito de "direitos fundamentais"; e, de outro lado, *(ii)* as principais características dos instrumentos jurídicos que presidem à proteção dos direitos fundamentais no espaço Europeu—designadamente a Carta e a Convenção Europeia. O objetivo deste confronto é a avaliação da capacidade do Regulamento Europeu para assegurar uma proteção efetiva dos direitos fundamentais face ao risco criado por aplicações de Inteligência Artificial—assentando tal avaliação em dois pressupostos. Primeiro, pressupõe-se que o grau de proteção dos direitos fundamentais assegurado pela Convenção Europeia (e, correspondentemente, pela Carta)[212] é a bitola pela qual a eficácia de outros instrumentos na proteção de direitos fundamentais deve ser medida; e, de facto, a Convenção Europeia é largamente considerada o "instrumento internacional mais eficiente do mundo na proteção dos direitos individuais" (HELFER, 1993). Segundo, pressupõe-se, então, que o grau de semelhança entre os trâmites que presidem à proteção de direitos fundamentais no âmbito da Convenção Europeia (e da Carta) e os trâmites que presidem à proteção de direitos fundamentais em sede do Regulamento é um bom critério para avaliar a capacidade do Regulamento para cumprir este seu objetivo. Noutras palavras: quanto mais o Regulamento comungar das características da Convenção Europeia (e da Carta), maior será o seu potencial para atingir o objetivo de

[211] *Ver* a discussão na Secção III.1 *supra*.

[212] A Carta é necessariamente tão (ou mais) mais protetora que a Convenção Europeia, dispondo o seu Artigo 53.º, n.º3 que "na medida em que a (...) Carta contenha direitos correspondentes aos direitos garantidos pela Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, o sentido e o âmbito desses direitos são iguais aos conferidos por essa Convenção" sendo que Esta disposição não obsta a que o direito da União confira uma proteção mais ampla".

proteção de direitos fundamentais a que estes (outros) instrumentos há muito se dedicam (e com assinalável sucesso).[213]

Comparar as características do Regulamento Europeu que resultam das várias referências nele feitas ao conceito de "direitos fundamentais" (elencadas na Secção III *supra*) e as principais características dos instrumentos gerais de proteção de direitos humanos vigentes na Europa (discutidas na Secção II *supra*)—em particular, ainda que não exclusivamente, as restrições às interferências com direitos fundamentais que deles resultam—é um exercício que revela mais diferenças do que semelhanças.

No campo das semelhanças, temos de facto o objetivo de proteção dos direitos fundamentais que é comum a todos estes instrumentos—mas cumpre notar que, no Regulamento Europeu, esse objetivo aparece lado a lado com um objetivo de promoção do mercado interno e inovação, ficando por esclarecer a relação entre os dois objetivos, e, em particular, o que é que acontece em casos em que estes objetivos entrem em conflito (na medida em que isso não resulte já evidente dos termos do Regulamento). Outro ponto comum entre o Regulamento Europeu da Inteligência Artificial, a Carta e a Convenção Europeia é o facto de todos estes instrumentos conferirem direitos subjetivos aos indivíduos por eles abrangidos—mas também aqui cumpre notar que o Regulamento Europeu concede apenas dois tipos de direitos subjetivos, privilegiando antes a criação de obrigações para a generalidade dos destinatários do Ato (os quais, contrariamente ao que acontece em sede da Convenção Europeia e da Carta não têm de ser, por norma, Estados e outras entidades públicas).

É também interessante notar que, embora todos estes instrumentos incluam limites às interferências com direitos fundamentais, as restrições constantes do Regulamento Europeu—aplicáveis apenas no contexto de modificações da lista de aplicações de risco elevado constantes do seu Anexo III e das aplicações de risco inaceitável constantes do Artigo 5.º—apresentam um

[213] Naturalmente, e uma vez que a proteção dos direitos fundamentais não é o único objetivo do Regulamento Europeu da Inteligência Artificial (*ver* Artigo 1.º do Regulamento), o seu (maior ou menor) cumprimento não pode ser base única para a avaliação do seu mérito—mas é uma parte importante desse *puzzle*.

escopo restrito (nos termos descritos), e incluem uma margem de apreciação significativa. De facto—e ao mesmo tempo que o Artigo 18.º da Convenção Europeia e o Artigo 53.º da Carta representam proibições estritas às interferências com direitos fundamentais que não lhes sejam conformes—o *AI Act* exige apenas que aditamentos ao seu Anexo III sejam precedidos por uma avaliação de direitos fundamentais, e que remoções do Anexo III se refiram a aplicações que tenham deixado de apresentar risco "significativo" para os direitos fundamentais (sem que tal leve a uma diminuição do "nível geral de proteção" destes direitos). Já as revisões anuais da lista de aplicações constantes do Artigo 5.º e do Anexo III que a Comissão está obrigada a levar a cabo nos termos do Artigo 112.º do Regulamento deve "atender, em especial" ao impacto que as aplicações em causa possam ter nos direitos fundamentais.

Em última instância, a maior diferença entre o Regulamento Europeu e os instrumentos jurídicos tradicionalmente utilizados no espaço Europeu para a proteção de direitos fundamentais—e, na verdade, outros instrumentos avulsos que têm vindo a ser aprovados com o intuito de reforçar a defesa de terminados direitos fundamentais, tais como o direito à privacidade (no caso do RGPD), ou o direito à liberdade de expressão (no caso do Regulamento dos Serviços Digitais)—relaciona-se com o sistema de classificação de risco subjacente ao *AI Act*, e que opera numa lógica de segurança de produtos que é fundamentalmente diferente da lógica de proteção de direitos fundamentais da Convenção Europeia ou da Carta.

Para começar, o sistema de classificação de risco subjacente ao *AI Act* parece pressupor que as aplicações de Inteligência Artificial são produtos como quaisquer outros,[214] deixando sem resposta satisfatória os problemas de "*naming*" e "*claiming*" inerentes aos sistemas de Inteligência Artificial (HARKENS, 2024). Em primeiro lugar, não é claro que o Regulamento reconheça as especiais

[214] Em sentido contrário—distinguindo a Inteligência Artificial de outros produtos mais tradicionais, como torradeiras ou máquinas de lavar a loiça—*veja-se, inter alia*, CAROLI, 2024 e SOUSA e SILVA, 2024, p. 7). Para além disso, há ainda quem defenda que as aplicações de Inteligência Artificial não devem ser vistas como produtos—objetos, ou ferramentas—mas sim como agentes (*veja-se, inter alia*, HARARI, 2024)

dificuldades de identificação dos riscos criados pela Inteligência Artificial para os direitos fundamentais—advenientes, designadamente, do facto de nem todas estas aplicações terem propósitos ou objetivos pré definidos (que permitam uma identificação fácil de riscos subjacentes),[215] e do facto de a ameaça criada (para os direitos fundamentais) pela Inteligência Artificial ser qualitativamente diferente da ameaça criada (para a saúde e para a segurança) pela generalidade dos produtos; conforme tem sido amplamente assinalado, as aplicações de Inteligência Artificial podem atentar mais profundamente contra o núcleo do que significa ser humano (e contra direitos como o direito fundamental à dignidade ou à vida privada) que a generalidade dos produtos (ALMADA e PETIT, 2023, pp. 19-20). Em segundo lugar, não resulta do Regulamento um sistema de direitos que permita aos indivíduos cujos direitos fundamentais sejam afetados por aplicações de Inteligência Artificial reagir efetivamente contra os destinatários das obrigações impostas pelo *AI Act*.[216]

Na prática, a lógica de segurança de produtos subjacente ao *AI Act* acaba por redundar num instrumento que permite a circulação de aplicações de Inteligência Artificial que—criando embora risco para os direitos fundamentais—cumpram os requisitos mínimos impostos aos destinatários das obrigações constantes do Regulamento. Feita a medição das vantagens (para a inovação e promoção do mercado interno) e das desvantagens (para a segurança e para os direitos fundamentais) de determinada aplicação de Inteligência Artificial—e chegando-se à conclusão de que as vantagens da sua circulação são maiores que as desvantagens da sua proibição—essa circulação é permitida; qualquer dano que dela resulte é, nesses termos, tido como admissível (ainda que eventualmente compensável). Em contraste, a lógica subjacente aos instrumentos tradicionais de defesa dos direitos fundamentais reconhece as dificuldades de medir interferências com esses direitos, reconhece a sua superior importância—

[215] O exemplo mais claro de aplicações de Inteligência Artificial sem propósitos e objetivos pré-definidos é o dos modelos de finalidade geral—os quais apenas vieram a ser abrangidos pelo Regulamento Europeu de Inteligência Artificial em momento posterior ao da sua conceção inicial enquanto regulamento de segurança de produtos; para uma discussão, *ver, inter alia,* ALMADA e PETIT, 2023, pp. 14 ss.

[216] *Ver* nota de rodapé n.º 96 *supra.*

e sugere, enfim, que qualquer interferência seja limitada ao mínimo necessário para a prossecução de interesses concorrentes reconhecidos (e fundamentados na lei). Simplificando, enquanto a lógica do Regulamento Europeu da Inteligência Artificial é uma lógica de cumprimento de *standards* mínimos para lá dos quais qualquer dano é tolerável (ainda que eventualmente compensável)—a lógica subjacente à Carta e à Convenção Europeia é uma lógica de limitação das interferências com direitos fundamentais ao mínimo necessário (para uma discussão, *ver, inter alia,* CHRISTOFFERSEN, 2011; HARRIS, O'BOYLE e WARBRICK, 2023; JACOBS, WHITE, e OVEY, 2021; e NUSSBERGER, 2010).

Em última análise, não é que não existam bons motivos para a aprovação de um Regulamento sobre Inteligência Artificial assente numa lógica de segurança de produtos: a regulação da Inteligência Artificial a nível Europeu é uma regulação que se pretendia abrangente e de carácter horizontal e que, por esse motivo, teve de procurar legitimidade na competência geral de harmonização do mercado único e de facilitação do acesso ao mercado que é comum à lógica de regulação de produtos. Para além disso, a experiência e sucessos acumulados pela União Europeia no campo da regulação e segurança de produtos é bem conhecida—e não surpreende que a União tenha procurado replicar esses sucessos no campo da Inteligência Artificial. E é claro que a tarefa de conciliar duas lógicas—tanto uma lógica de segurança de produtos como uma lógica de proteção de direitos fundamentais—num mesmo Regulamento seria sempre difícil, sendo natural que uma delas—neste caso a lógica de proteção dos direitos fundamentais—viesse a sofrer, particularmente no final de um processo político e regulatório tão difícil e delicado como o que antecedeu a aprovação do *AI Act* (no mesmo sentido, *veja-se*, ALMADA e PETIT, 2023).

Também a questão de saber se a falta de eficiência do Regulamento Europeu na tarefa de proteção dos direitos fundamentais é particularmente problemática fica por discutir—dependendo a resposta, designadamente, de uma avaliação do quadro jurídico aplicável às interferências das aplicações de Inteligência Artificial com os direitos fundamentais para lá do *AI Act*. Em qualquer caso, cumpre reconhecer que—à semelhança do que acontece também

com a regulação de (outro tipo de) produtos—a ausência de direitos no *AI Act* poderá vir a ser de alguma forma compensada em sede de regimes de responsabilidade decorrente de produtos, particularmente com a recente aprovação de uma nova diretiva relativa a produtos defeituosos[217] e a planeada aprovação de uma nova Diretiva da responsabilidade da Inteligência Artificial[218] (WENDEHORST, 2022, 197). Para além disso, o certo é que as aplicações de Inteligência Artificial não existiam num vácuo jurídico antes da aprovação do Regulamento—e a tarefa de defesa de direitos fundamentais ameaçados por estas aplicações é levada a cabo por um quadro jurídico que vai bem para além do *AI Act*.[219]

Ao mesmo tempo, não há como evitar a conclusão que resulta da análise conduzida pelo presente capítulo: a de que o Regulamento Europeu da Inteligência Artificial não alcança, por si só, a tarefa de "assegurar um elevado nível de proteção"[220] dos direitos fundamentais a que se propôs. Pelo contrário, a eficácia do Regulamento Europeu na proteção desses direitos fica muito aquém da eficácia que resulta do quadro tradicional de proteção de direitos fundamentais no espaço Europeu—e, suspeita-se, da eficácia com que cumprem esta tarefa outros instrumentos comunitários avulsos que também se propõem a defender direitos fundamentais face às ameaças para eles criadas pela nova

---

[217] *Ver* a nova Diretiva do Parlamento Europeu e do Conselho em matéria de responsabilidade decorrente dos produtos defeituosos e que revoga a 85/374/CEE disponível para consulta em https://data.consilium.europa.eu/doc/document/PE-7-2024-INIT/en/pdf acedido a 10 de outubro de 2024.

[218] *Ver* a Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à adaptação das regras de responsabilidade civil extracontratual à inteligência artificial ("Diretiva Responsabilidade da IA") disponível para consulta na sua versão portuguesa em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52022PC0496> acedido a 30 de setembro de 2024.

[219] Este enquadramento jurídico mais abrangente é, de resto, reconhecido pelo próprio Regulamento Europeu da Inteligência Artificial, notando o seu Considerando (63) que "a classificação de um sistema de IA como sendo de risco elevado por força do [*AI Act*] não deverá ser interpretada como uma indicação de que a utilização do sistema é lícita ao abrigo de outros atos do direito da União ou ao abrigo do direito nacional compatível com o direito da União, por exemplo, em matéria de proteção de dados pessoais ou de utilização de polígrafos e de instrumentos semelhantes ou de outros sistemas para detetar o estado emocional de pessoas singulares. Essa utilização deverá continuar sujeita ao cumprimento dos requisitos aplicáveis resultantes da Carta".

[220] *Ver* o Artigo 1.º, n.º1 do Regulamento Europeu da Inteligência Artificial.

economia digital.[221] Apesar das numerosas manifestações do conceito de "direitos fundamentais" no Regulamento—e apesar de este se assumir como um instrumento de defesa destes direitos—as aparências iludem, e os indivíduos que vejam os seus direitos fundamentais ameaçados pela Inteligência Artificial terão de procurar conforto fora do *AI Act*.

Referências

ALMADA, Marco, e PETIT, Nicolas. The EU AI Act: A Medley of Product Safety and Fundamental Rights? **Working Paper, RSC** 2023/59, EUI Robert Schuman Centre for Advanced Studies, 2023, https://cadmus.eui.eu/handle/1814/75982. Acesso em 30 de setembro de 2024.

ALMADA, Marco, e RADU, Anca. "The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy". **German Law Journal**, p. 1–18, 2024.

BANTEKAS, Ilias, e OETTE, Lutz. **International Human Rights Law and Practice**. 3.ª edição, Cambridge University Press, 2020.

BATHAEE, Yavar. "The Artificial Intelligence Black Box and the Failure of Intent and Causation". **Harvard Journal of Law & Technology**, v. 31, n. 2, p. 889–938, 2018.

BEITZ, Charles R. **The Idea of Human Rights.** Oxford University Press, 2011.

BRAUN, Ernest. "Promote or Regulate: The Dilemma of Innovation Policy". In: AICHHOLZER, Georg; SCHIENSTOCK, Gerd (eds.). **Technology Policy:** Towards an Integration of Social and Ecological Concerns. Berlin: De Gruyter, 2010. p. 95–124.

BRKAN, Maja, et al. "European fundamental rights and digitalization". **Maastricht Journal of European and Comparative Law**, v. 27, n. 6, p. 697–704, 2020.

BROWN, Chris. "Universal human rights: A critique". **The International Journal of Human Rights**, v. 1, n. 2, p. 41–65, 1997.

[221] A análise de tais instrumentos (e da sua eficácia na proteção de direitos fundamentais) excede largamente o âmbito do presente capítulo.

BROWNSWORD, Roger. "AI and Fundamental Rights: The People, the Conversations, and the Governance Challenges". In: VICENTE, Dário Moura *et alli* (orgs.). **The Legal Challenges of the Fourth Industrial Revolution**. Springer International Publishing, 2023. p. 335–55.

BUCHANAN, Allen. **The Heart of Human Rights.** Oxford University Press, 2014.

CARLSSON, Bo. "The Digital Economy: what is new and what is not?" **Structural Change and Economic Dynamics**, v. 15, n. 3, p. 245–64, 2004.

CAROLI, Laura. **Will the EU AI Act work? Lessons learned from past legislative initiatives, future challenges.** 31 de agosto de 2024, https://iapp.org/news/a/will-the-eu-ai-act-work-lessons-learned-from-past-legislative-initiatives-future-challenges . Acesso em 30 de setembro de 2024.

CASTETS-RENARD, Céline. "Human Rights and Algorithmic Impact Assessment for Predictive Policing". In: REICHMAN, Amnon (ed.). **Constitutional Challenges in the Algorithmic Society**. Cambridge University Press, 2021, p. 93–110, https://doi.org/10.1017/9781108914857.007. Acesso em 30 de setembro de 2024.

CELESTE, Edoardo. "Digital Constitutionalism: A Socio-Legal Approach". **European Data Protection Law Review**, v. 10, n. 2, p. 146–49, 2024.

CHABERT, Jean-Luc. **A History of Algorithms:** From the Pebble to the Microchip. Springer Science & Business Media, 2012.

CHIUSI, Fabio. **Automating Society Report 2020.** Algorithm Watch, 2020, https://automatingsociety.algorithmwatch.org/ . Acesso em 30 de setembro de 2024.

CHRISTOFFERSEN, Jonas, e RASK MADSEN, Mikael. "Introduction: The European Court of Human Rights between Law and Politics". *In:* CHRISTOFFERSEN, Jonas, e RASK MADSEN, Mikael (eds.). **The European Court of Human Rights between Law and Politics**, Oxford University Press, 2011.

COUNCIL OF EUROPE. **Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.** 2024, https://rm.coe.int/ai-convention-brochure/1680afaeba . Acesso em 30 de setembro de 2024.

DAGGETT, Susan D. "NGOs as Lawmakers, Watchdogs, Whistle-Blowers, and Private Attorneys General A Cartography of Governance Exploring the Province of Environmental NGOs". **Colorado Journal of International Environmental Law and Policy**, v. 13, n. 1, p. 99–114, 2002.

DEMBOUR, Marie-Bénédicte. "What Are Human Rights? Four Schools of Thought". **Human Rights Quarterly**, v. 32, n. 1, p. 1–20., 2010.

EDRI - EUROPEAN DIGITAL RIGHTS. **Use cases: Impermissible AI and fundamental rights breaches.** https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf . Acesso em 30 de setembro de 2024.

EUROPEAN COMMISSION. **AI Act.** 2024, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai . Acesso em 30 de setembro de 2024.

EUROPEAN COMMISSION. *Artificial Intelligence – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683. Acesso em 30 de setembro de 2024.

EUROPEAN COMMISSION. *Non-discrimination*. 2024, https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/equality/non-discrimination_en?prefLang=pt . Acesso em 30 de setembro de 2024.

EUROPEAN COMMISSION. **Smart lie-detection system to tighten EU's busy borders.** Research and Innovation, 24 de outubro de 2018, https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders . Acesso em 30 de setembro de 2024.

EUROPEAN PLATFORM UNDECLARED WORK. **Good practice fiche - Italy: Redditometro online tool.** Factsheets on Existing Tools to Address Undeclared

Work, 2018, https://www.ela.europa.eu/sites/default/files/2021-10/Redditometro%20online%20tool.pdf . Acesso em 30 de setembro de 2024.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Assessing high-risk artificial intelligence.** 2024, https://fra.europa.eu/pt/project/2023/assessing-high-risk-artificial-intelligence . Acesso em 30 de setembro de 2024.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Under watchful eyes: biometrics, EU IT systems and fundamental rights.** 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf . Acesso em 30 de setembro de 2024.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **What are fundamental rights?** 2024, https://fra.europa.eu/en/content/what-are-fundamental-rights#:~:text='Fundamental%20rights'%20expresses%20the%20concept,is%20used%20in%20international%20law . Acesso em 30 de setembro de 2024.

GARDNER, John. "'Simply In Virtue of Being Human': The Whos and Whys of Human Rights". **Journal of Ethics and Social Philosophy**, v. 2, n. 2, p. 1–23, 2007.

GELLER, Anja. **Social Scoring by States:** Legitimacy under European Law - with References to China. 28 de novembro de 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4478415 . Acesso em 30 de setembro de 2024.

GORDON, John-Stewart (ed.). **Smart Technologies and Fundamental Rights**. Brill, 2020.

GPDP - GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Redditometro: concluso l'esame del Garante.** 21 de novembro de 2013, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2765125 . Acesso em 30 de setembro de 2024.

GRIFFIN, James. **On Human Rights.** Oxford University Press, 2008.

HACKER, Philipp, et al. "Regulating ChatGPT and other Large Generative AI Models". *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, Association for Computing Machinery, 2023, p. 1112–23. **ACM Digital Library**, https://arxiv.org/abs/2302.02337. Acesso em 30 de setembro de 2024.

HAENLEIN, Michael, e KAPLAN, Andreas. "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence". **California Management Review**, v. 61, n. 4, p. 5–14, 2019.

HARARI, Yuval Noah. "'Never summon a power you can't control': Yuval Noah Harari on how AI could threaten democracy and divide the world". **The Guardian**, 24 de agosto de 2024. *The Guardian*, https://www.theguardian.com/technology/article/2024/aug/24/yuval-noah-harari-ai-book-extract-nexus . Acesso em 30 de setembro de 2024.

HARKENS, Adam. "How algorithmic policing challenges fundamental rights protection in the EU : lessons from the United Kingdom". **The Challenges of Artificial Intelligence for Law in Europe. Data Science, Machine Intelligence, and Law**, Springer, 2024.

HARRIS, David, *et alli*. **Harris, O'Boyle, and Warbrick:** Law of the European Convention on Human Rights, Oxford University Press, 2018.

HELFER, Laurence R. "Consensus, Coherence and the European Convention on Human Rights". **Cornell International Law Journal**, v. 26, n. 1, 1993.

HM UK Government. **National AI Strategy.** Command Paper, 525, setembro de 2021, https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf . Acesso em 30 de setembro de 2024.

HUSOVEC, Martin. "Risk-Based Approach to Digital Services". **Principles of the Digital Services Act**, Oxford University Press, 2024.

ICRC - INTERNATIONAL COMMITTEE OF THE RED CROSS. **Artificial intelligence and machine learning in armed conflict:** A human-centred approach. 6 de junho de 2019, https://www.icrc.org/sites/default/files/document_new/file_list/ai_and_machine_learning_in_armed_conflict-icrc.pdf . Acesso em 30 de setembro de 2024.

INOZEMTSEV, Maxim I. "Digital Law: The Pursuit of Certainty Editorial". **Digital Law Journal**, v. 2, n. 1, p. 8–28, 2021.

KRASMANN, Susanne, e EGBERT, Simon. **Predictive Policing.** Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis. Universität Hamburg - Fachbereich Sozialwissenschaften, 30 de abril de 2019, https://www.wiso.uni-hamburg.de/fachbereich-sowi/ueber-den-fachbereich/fachgebiete/fachgebiet-kriminologische-sozialforschung/predictive-policing/egbert-krasmann-2019-predictive-policing-projektabschlussbericht.pdf . Acesso em 30 de setembro de 2024.

LEVANTINO, Francesco Paolo, e PAOLUCCI, Federica. "Advancing the Protection of Fundamental Rights through AI Regulation: How the EU and the Council of Europe are Shaping the Future". **European Yearbook on Human Rights 2024**, Philip Czech, Lisa Heschl, Karin Lukas, Manfred Nowak e Gerd Oberleitner, Brill, 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4881656 . Acesso em 30 de setembro de 2024.

LONGPRE, Shayne, et al. "Lethal Autonomous Weapons Systems & Artificial Intelligence: Trends, Challenges, and Policies". **MIT Science Policy Review**, v. 3, p. 47–56, 2022.

MOECKLI, Daniel, *et alli* (eds.). **International Human Rights Law.** 4.ª edição Oxford University Press, 2022.

MUIR, Elise. "The Fundamental Rights Implications of EU Legislation: Some Constitutional Challenges". **Common Market Law Review**, v. 51, n. 1, 2014.

NICKEL, James. **Making Sense of Human Rights.** 2.ª edição, Wiley-Blackwell, 2006.

NOTTAGE, Luke. "Product Safety Regulation". **Handbook of Research on International Consumer Law**, Second Edition, Edward Elgar Publishing, 2018.

NUSSBERGER, Angelika. **The European Court of Human Rights.** Oxford University Press, 2020.

PACKIN, Nizan Geslevich, e LEV-ARETZ, Yafit. "Algorithmic Analysis of Social Behavior for Profiling, Ranking, and Assessment". *In:* BARFIELD, Woodrow (ed.). **The Cambridge Handbook of the Law of Algorithms**. Cambridge University Press, p. 632–53, 2020.

RAINEY, Bernadette, et al. **Jacobs, White, and Ovey:** The European Convention on Human Rights. Eighth Edition, Oxford University Press, 2020.

ROBINS-EARLY, Nick. "AI's 'Oppenheimer moment': autonomous weapons enter the battlefield". **The Guardian**, 14 de julho de 2024. *The Guardian*, https://www.theguardian.com/technology/article/2024/jul/14/ais-oppenheimer-moment-autonomous-weapons-enter-the-battlefield . Acesso em 30 de setembro de 2024.

SILVEIRA BORGES, Gustavo, et al. "Inteligência Artificial, Consumo e Responsabilidade Jurídica: Análise do Caso da Via Quatro do Metro de São Paulo". **Revista Paradigma**, v. 33, n. 1, p. 173–99, 2024.

SOUSA E SILVA, Nuno. **The Artificial Intelligence Act:** critical overview. 2024, https://arxiv.org/abs/2409.00264 . Acesso em 30 de setembro de 2024.

UFERT, Fabienne. "AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?" **European Papers - A Journal on Law and Integration**, v. 5, n. 2, p. 1087–97, 2020.

UNESCO. **Consultation Paper on AI Regulation:** Emerging Approaches Across the World. Digital Transformation, CI/DIT/2024/CP/01, 16 de agosto de 2024, https://unesdoc.unesco.org/ark:/48223/pf0000390979 . Acesso em 30 de setembro de 2024.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS. **Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects:** Non-exhaustive compilation of definitions and characterizations. CCW/GGE.1/2023/CRP.1, 10 de março de 2023, https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf . Acesso em 30 de setembro de 2024.

VEALE, Michael, e ZUIDERVEEN BORGESIUS, Frederik. "Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach". **Computer Law Review International**, v. 22, n. 4, p. 97–112, 2021.

WALKER, Neil. "The Burden of the European Constitution". **The Future of EU Constitutionalism**, Matej Avbelj, Bloomsbury, 2024.

WANG, Pei. "On Defining Artificial Intelligence". **Journal of Artificial General Intelligence**, v. 10, n. 2, p. 1–37, 2019.

WENDEHORST, Christiane. "Liability for Artificial Intelligence: The Need to Address Both Safety Risks and Fundamental Rights Risks". *In:* VOENEKY, Silja (ed.). **The Cambridge Handbook of Responsible Artificial Intelligence**. Cambridge University Press, 2022. p. 187–209.

8. Transparência *versus* explicação: o papel da ambiguidade na IA jurídica[222]

Elena Esposito[223]

Tradução de Isabela Gomes Ribeiro[224]*, revisão técnica de Izabela Zonato Villas Boas*[225]

1 Introdução: da inteligência artificial à comunicação artificial

Lidando com técnicas opacas de aprendizagem de máquinas, a questão crucial tornou-se a interpretabilidade do trabalho dos algoritmos e dos seus resultados. O artigo argumenta que a mudança para a interpretação requer um movimento da inteligência artificial para uma forma inovadora de comunicação artificial. Em muitos casos, o objetivo da explicação não é revelar os procedimentos das máquinas, e sim comunicar-se com elas e obter informação relevante e controlada. Como as explicações humanas não exigem transparência das ligações neurais ou processos de pensamento, as explicações algorítmicas não têm de revelar as operações da máquina, mas têm de produzir reformulações que façam sentido para os seus interlocutores. Esse movimento tem consequências importantes para a comunicação jurídica, em que a ambiguidade desempenha um papel fundamental. O problema da interpretação nos argumentos jurídicos, discute o artigo, não é que os algoritmos não explicam o suficiente, mas que devem explicar muito e com muita precisão, restringindo a liberdade de interpretação e a contestabilidade das decisões jurídicas. A consequência pode

[222] Artigo originalmente publicado em **Journal of Cross-Disciplinary Research in Computational Law**, v.1, n.1, 2021. Tradução originalmente publicada na **Revista Direito Mackenzie**, v. 16, n. 3, 2022. Agradeço à autora e ao editor da Revista, professor Marco Antonio Loschiavo Leme de Barros, pela autorização para republicar o texto.

[223] Professora de sociologia na Universidade de Bielefeld, Alemanha, e na Universidade de Modena-Reggio Emilia, Itália.

[224] Mestranda em Direito Político e Econômico na Universidade Presbiteriana Mackenzie.

[225] Mestra em Direito Político e Econômico na Universidade Presbiteriana Mackenzie, Mestra pelo Instituto Internacional de Sociologia Jurídica em Oñati (Espanha), membro do Research Committee on Sociology of Law da International Sociological Association

ser uma possível limitação da autonomia da comunicação jurídica que está na base do Estado de Direito moderno.

Depois de repetidos "invernos" (RUSSELL; NORVIG, 2003, p. 29. CARDON; COINTET; MAZIERES, 2018, p. 173), a investigação IA parece estar agora numa nova "primavera" – na qual, no entanto, as máquinas, a forma de trabalhar e mesmo os problemas mudaram. Hoje falamos mais de algoritmos do que de computadores. Tomamos como certa a referência à web (incluindo a participação ativa dos usuários) e o fato de que os dados a serem processados não são escassos, e sim excessivamente abundantes. Estamos no mundo dos algoritmos de autoaprendizagem e de *big data*. Nessa nova fase, o problema central não é a capacidade ou o poder processante dos computadores[226]. Atualmente, a questão crucial é a interpretação, ou melhor, a interpretabilidade dos algoritmos[227] (DEANGELIS, 2014) e dos resultados do seu trabalho.

O artigo argumenta que a mudança para a interpretação exige que a investigação sobre o processamento de informação digital passe da referência à inteligência (artificial) para a referência a uma forma inovadora de comunicação, que pode ser definida como artificial (ESPOSITO, 2017, p. 249; ESPOSITO, 2021). O objetivo não é construir máquinas inteligentes, mas ser capaz de se comunicar com algoritmos para obter informação relevante e controlada. O que deve ser compreendido é a informação gerada nessa comunicação e não os processos das máquinas, que são e muitas vezes devem permanecer obscuros. Faço minhas observações nas próximas duas seções do artigo que tratam da questão da transparência e do objetivo das explicações.

A mudança da inteligência para a comunicação traz problemas e oportunidades em muitos campos diferentes, incluindo a complexa área de interpretação jurídica, abordada na seção 'Razão artificial e jurisprudência mecânica'. Lá, discuto o papel da interpretação para a autonomia do sistema

[226] O que as pessoas tentaram prever com a Lei de Moore e suas variantes.

[227] Em discurso recente sobre a IA e suas transformações, o uso do termo 'algoritmo' é frequentemente impreciso. Naturalmente, a programação de computadores tem usado algoritmos desde o início e o termo já existia antes da cibernética. Neste texto, sigo o uso atual, por mais imperfeito que seja, e uso 'algoritmos' para me referir a técnicas avançadas de programação que utilizam aprendizagem de máquinas e grandes dados.

jurídico, e, na seção seguinte, exploro a necessidade de ambiguidade na argumentação jurídica e os desafios resultantes para a utilização de algoritmos. A 'jurisprudência mecânica' pode afetar a prática jurídica e os princípios em que esta se baseia, notadamente o Estado de Direito.

2 A interpretação de máquinas incompreensíveis

A recente ênfase no problema da interpretação é uma consequência da inovação nas técnicas de programação e gestão de dados. Com métodos de aprendizagem profunda, e utilizando *big data*, os algoritmos aprendem de forma autônoma a executar as suas tarefas de formas não necessariamente previstas por seus programadores e que, em alguns casos, são incompreensíveis para os humanos, incluindo aqueles que os projetaram. Mesmo os programadores podem não compreender como a máquina procede e como ela alcança os seus resultados (GOODFELLOW; BENGIO; COURVILLE, 2016; BURRELL, 2016; WEINBERGER, 2017; GILPIN; BAU; YUAN; BAJWA; SPECTER; KAGAL, 2018. BUSUIOC, 2020). Quando se precisa entender os resultados e procedimentos dos algoritmos, é necessário interpretá-los, e não está claro como isso deve ser alcançado.

Algoritmos que trabalham com a aprendizagem de máquinas e *big data* estão ficando cada vez melhores em fazer cada vez mais coisas: eles produzem informação de forma rápida e precisa; eles estão aprendendo a dirigir carros com mais segurança e confiabilidade do que os humanos; eles podem responder às nossas perguntas, conversar, compor música e ler livros; e eles podem até mesmo escrever textos interessantes, apropriados, e – se necessário – engraçados. Eles alcançaram esses resultados, que parecem sugerir que as máquinas finalmente se tornaram inteligentes, já que seus programadores desistiram mais ou menos explicitamente de tentar reproduzir artificialmente os processos da inteligência humana. Os algoritmos funcionam de uma forma radicalmente diferente, que pode ser incompreensível para a nossa inteligência. A transparência, ou a falta dela, é, portanto, um problema.

Os algoritmos de aprendizagem de máquinas são de difícil entendimento, antes de tudo porque funcionam sem compreender seus materiais – eles fazem algo diferente. Programas recentes de tradução, por exemplo, não tentam entender os documentos que traduzem e os seus designers não confiam em nenhuma teoria de linguagem (BOELLSTORFF, 2013). Os algoritmos traduzem textos em mandarim sem conhecer mandarim; seus programadores também não conhecem. Os exemplos se multiplicam em todas as áreas nas quais os algoritmos têm mais sucesso, por exemplo, competindo com jogadores humanos no xadrez, pôquer e go (SILVER; HASSABIS, 2016), produzindo textos, programas de recomendação (PREY, 2018), reconhecimento de imagem e muitos outros. Os algoritmos não compreendem nada dos materiais com os quais estão lidando; eles "não raciocinam como as pessoas para escrever [ou, pode-se acrescentar, para trabalhar em geral] como as pessoas" (HAMMOND, 2015). Portanto, as operações das máquinas e seus resultados são muitas vezes obscuros para os observadores humanos.

Mesmo que sejam muito eficazes, porém, a confiança nas caixas pretas não é tranquilizadora, especialmente quando sabemos que as suas operações não são imunes a vieses e erros de vários tipos (PASQUALE, 2015). Em muitos casos, queremos verificar a correção dos resultados produzidos pelas máquinas, que podem ser errados ou inadequados de muitas maneiras diferentes, e com consequências diferentes. No campo médico, por exemplo, existe a preocupação de que os algoritmos possam não levar adequadamente em conta informações que, embora relevantes, podem não ser explícitas (HOLZINGER; LANGS; DENK; ZATLOUKAL; MÜLLER, 2019). Por exemplo, Caruana et al discutem um algoritmo que previu que os pacientes asmáticos estavam com menor risco de morte por pneumonia, ignorando o fato de que os pacientes já vinham recebendo assistência médica intensa (CARUANA; LOU; GEHRKE; KOCH; STURM; ELHADAD, 2015). Em outros campos, como o policiamento (LUM; ISAAC, 2016), a concessão de crédito ao consumidor (O'NEIL, 2016), ou processos de admissão universitária (HAO, 2020), existe a preocupação de que, por meio de vieses sistémicos ou de confirmação, eles possam reproduzir ou intensificar os

desequilíbrios nos dados. Consequentemente, deseja-se poder verificar seus resultados e controlar a forma como são obtidos. No campo jurídico, discutido detalhadamente mais adiante, a obscuridade dos procedimentos algorítmicos pode comprometer a contestabilidade das decisões.

O recente ramo de pesquisa sobre '*explainable AI*' (XAI) tenta responder a essa preocupação desenvolvendo procedimentos para explicar as operações de algoritmos de autoaprendizagem (WACHTER; MITTELSTADT; FLORIDI, 2017; DOSHI-VELEZ; KORTZ; BUDISH; BAVITZ; GERSHMAN; O´BRIEN; SCOTT; SCHIEBER; WALDO; WEINBERGER; WELLER; WOOD, 2017; MILLER, 2019). Os resultados esclarecem vários aspectos dos processos de interação com máquinas e são muitas vezes bastante úteis no gerenciamento de tais processos em situações específicas. No entanto, no caso de algoritmos de aprendizagem profunda, existe um obstáculo básico: se por explicação se entende um procedimento que permite aos observadores humanos compreender o que a máquina faz e por quê, a empresa não tem esperança. Os processos de algoritmos recentes que parecem inteligentes são intrinsecamente incompreensíveis para a inteligência humana. Como Weinberger afirma, exigir uma explicação nesse sentido equivaleria a "forçar a IA ser artificialmente estúpida o suficiente para que possamos compreender como ela chega à sua conclusão" (WEINBERGER, 2017; DOSHI-VELEZ; KIM, 2017; MONTAVON; SAMEK; MÜLLER, 2018; MONROE, 2018; RUDIN, 2019; BUSUIOC, 2020).

A estratégia deve ser diferente e, de fato, muitos projetos sobre XAI adotaram recentemente outra abordagem, compatível com a obscuridade radical dos processos algorítmicos (ROHLFING; CIMIANO; SCHARLAU; MATZNER; BUHL; BUSCHMEIER; ESPOSITO; GRIMMINGER; HAMMER; KERN; KOPP; THOMMES; NGOMO; SCHULTE; WACHSMUTH; WAGNER; WREDE, 2020). A noção chave é a transparência, frequentemente tomada como o primeiro elemento de projetos de IA explicáveis (ROSCHER; BOHN; DUARTE; GARCKE, 2020). Contudo, o debate envolve muitas outras noções relacionadas, cujas relações nem sempre são claras (MONROE, 2018; ANANNY; CRAWFORD, 2018; LIPTON, 2018; O'HARA, 2020), bem como as interações entre humano-

computador muito além das questões de aprendizagem profunda que a desencadearam. Quando e por que se torna necessário explicar as operações dos algoritmos? O objetivo da explicação deve ser a transparência? Qual é a relação entre transparência e opacidade, e entre explicação e interpretação? O que deve ser explicado, a quem e para qual finalidade? E quando se pode dizer que uma explicação foi realmente produzida? A resposta a estas perguntas diz respeito à própria interpretação da IA e à sua relevância social.

3 Será que a explicação requer transparência?

No estudo sociológico da tecnologia, a falta de transparência tem sido um problema antigo (WEYER; SCHULZ-SCHAEFFER, 2009; LUHMANN, 2017). O problema se torna ainda mais agudo no caso dos algoritmos. Aqui quero distinguir um tipo específico de não-transparência, que pode ser chamado de opacidade, em relação a métodos recentes de aprendizagem de máquinas, tais como redes neurais, que usam algoritmos de "caixa preta" (BUHRMESTER; MÜNCH; ARENS, 2019). Os modelos correspondentes podem ser radicalmente incompreensíveis para os observadores humanos, por mais experientes que sejam. Outros modelos que são em princípio compreensíveis (não opacos), como algoritmos de "caixa branca" baseados em árvores de decisão (QUINLAN, 1986) ou programação de lógica indutiva (MUGGLETON; DE RAEDT, 1994), podem, no entanto, também se revelar não transparentes, devido ao seu tamanho ou complexidade, bem como pelo acesso restrito à informação relevante (como a obtenção e utilização de dados de formação ou o desenvolvimento e implementação do modelo), ou em geral, porque o observador não tem as competências necessárias.

Na utilização de algoritmos, a não-transparência é muito mais ampla do que a opacidade, e mesmo que fosse obrigatório que todas as fontes de dados e todos os procedimentos fossem acessíveis aos utilizadores, a maioria dos sistemas continuaria a ser incompreensível para seus usuários. Contudo, por si só, isso não é novo nem problemático: o funcionamento interno da tecnologia sempre foi incompreensível para a maioria dos usuários (LATOUR, 1999). A

questão é que hoje os algoritmos fazem algo sem precedentes, diferente de outros sistemas tecnológicos: eles tomam decisões – sobre diagnósticos médicos, a seleção dos estudantes a serem admitidos nas universidades, as mudanças a serem feitas no go, as pessoas a receberem crédito ou liberdade condicional. São essas decisões que devem ser explicadas, e não os processos internos das máquinas. O objetivo da XAI é, na verdade, a explicação, não a transparência, e desse ponto de vista a opacidade dos sistemas de aprendizagem profunda não faz diferença; de qualquer forma, compreender a IA não é o problema.

O objetivo não é revelar os procedimentos das máquinas, mas sim fazer com que as próprias máquinas forneçam explicações que sejam informativas para o usuário. Não se pede que as máquinas sejam transparentes para os observadores humanos, mas que expliquem as suas decisões de uma forma que faça sentido para os seus interlocutores. E como seus interlocutores são sempre diferentes e localizados em situações e contextos diferentes, com interesses e necessidades diferentes, as explicações terão que ser diversas e específicas. A questão é fornecer explicações apropriadas aos diferentes usuários.

Isso é o que acontece quando os seres humanos tomam decisões, para as quais também podemos ser obrigados a oferecer explicações, dando pistas que permitam ao destinatário dar sentido à decisão. Quando se obtém uma explicação, se obtém informação sobre a decisão sem ser informado sobre os processos neurofisiológicos ou psíquicos do explicador, os quais (felizmente) podem permanecer obscuros ou privados. Explicar as nossas decisões não requer a divulgação do nosso processo de pensamento, muito menos as conexões dos nossos neurônios. As explicações, afirma Luhmann (1990), são "reformulações com o benefício adicional de uma melhor conectividade". O emissor produz uma nova comunicação que fornece elementos adicionais relacionados ao pedido específico do interlocutor e suas necessidades. Em todo caso, esse é um processo inteiramente comunicativo: não precisamos acessar o cérebro ou a mente dos nossos interlocutores, nem precisamos acessar o mundo externo. Precisamos apenas obter pistas que permitam que a comunicação prossiga de uma forma controlada e não arbitrária.

A mesma abordagem pode ser prevista para lidar com os dilemas de explicação na interação com as máquinas de autoaprendizagem. Muitos têm sugerido que somente modelos inerentemente compreensíveis devem ser usados nos casos em que a explicação possa ser necessária (ROBBINS, 2019). Contudo, isso não resolve o problema geral do qual surge a necessidade de explicação[228]. Em vez disso, as máquinas, opacas ou não, deveriam ser capazes de produzir "reformulações" dos seus processos que correspondam às solicitações dos seus interlocutores e lhes permitam exercer a forma de controle adequada ao contexto. O desafio técnico nas interações com um parceiro digital é reproduzir a situação comunicativa em que as explicações são solicitadas e fornecidas entre seres humanos.

De fato, muitos projetos XAI recentes não tentam imitar os cálculos feitos pelo algoritmo, e sim produzir "explicações *post-hoc*" que reproduzem o que os seres humanos fazem na comunicação. A transparência não pode ser a solução, porque, como Lipton afirma, por mais que a transparência seja entendida (no nível de todo o modelo, no nível dos componentes individuais ou no nível dos algoritmos de treinamento), as explicações humanas não exibem transparência (LIPTON, 2018, p. 15). Os processos pelos quais as pessoas explicam suas decisões são distintos daqueles pelos quais as tomam e geralmente são produzidos após o fato, o que afeta a tomada de decisões. Do mesmo modo, no campo da XAI, os designers são programas de treinamento para produzir explicações que ilustram (poderíamos dizer "reformular") o fato após o funcionamento dos algoritmos, sem impactar sua performance. Assim como os processos linguísticos que geram explicações humanas diferem dos processos neurais que produzem as decisões a serem explicadas, os processos que produzem explicações de modelos de IA também serão diferentes dos processos do modelo[229]. Eles podem, por exemplo, utilizar explicações verbais produzidas

[228] 'Se o ML está sendo usado para uma decisão que requer uma explicação, então ele deve ser explicável IA e um humano deve ser capaz de verificar se as considerações usadas são aceitáveis, mas se já sabemos quais considerações devem ser usadas para uma decisão, então não precisamos do ML.' (ROBBINS, 2019)

[229] Como as explicações bem-sucedidas por algoritmos não requerem acesso ao funcionamento dos algoritmos, a natureza de caixa preta dos algoritmos de aprendizado profundo não faz

pela máquina, visualizações e explicações locais, como mapas de saliência (LIPTON, 2018, p. 15 et seq). A compreensão do usuário das explicações produzidas pela máquina não tem que se relacionar com os processos da máquina.

Essa perspectiva promissora implica uma mudança profunda em relação à abordagem que tem guiado os projetos de IA desde seu início nos anos de 1950 – como o próprio nome Inteligência Artificial indica. De forma contraditória, os recentes projetos de XAI não estão focados na inteligência da máquina. Antes, o objetivo é o de produzir uma condição de 'diálogo' entre o algoritmo e o usuário no qual a máquina fornece respostas, tomando como *input* os sempre diferentes pedidos de esclarecimento dos seus interlocutores (CIMIANO; RUDOLPH; HARTFIEL, 2010), e é capaz de participar numa metacomunicação (BATESON, 1972; LUHMANN, 1997, p. 250-251) que pode ter como objeto os processos da máquina ou os dados utilizados. O objetivo não é e não pode ser que os interlocutores compreendam esses processos, mas que interpretem o que a máquina comunica sobre esses processos de tal modo que possam exercer uma forma de controle. O debate sobre a explicação implica uma mudança da inteligência para a própria característica que permite que os algoritmos contribuam efetivamente para a produção de novas informações na nossa sociedade: a sua capacidade de participar na comunicação. As máquinas devem ser capazes de produzir explicações adequadas em resposta a diferentes pedidos dos seus interlocutores.

4 Razão artificial e jurisprudência mecânica

Se XAI implica um movimento do foco na inteligência para o foco na comunicação, a tarefa de observação sociológica seria mostrar como as interações com algoritmos afetam a comunicação na sociedade em geral (LUHMANN, 1993, p. 304; ESPOSITO, 2017), e especificamente como as explicações algorítmicas

diferença para sua explicabilidade. Pelo contrário, algoritmos complexos como as redes neurais profundas podem ser mais eficientes no aprendizado, sendo as representações mais eficazes na comunicação com os usuários (LIPTON, 2018).

funcionam como processos de comunicação que dependem da opacidade. Isso pode acontecer de diferentes maneiras em diferentes domínios da sociedade. Na pesquisa científica, por exemplo na medicina, a atenção será direcionada para a possibilidade de descobrir estruturas causais nos dados[230]; no policiamento, será direcionada para a confiança nas decisões dos algoritmos; quando os algoritmos decidirem sobre a seleção de candidatos ou devedores, a questão será se as decisões algorítmicas estão em conformidade com os princípios éticos. Esta seção explora o campo jurídico: como a falta de transparência e sua gestão no funcionamento dos algoritmos pode afetar a prática jurídica e seus pressupostos, notadamente o Estado de Direito.

No campo jurídico, hoje os algoritmos são capazes de cumprir muitas tarefas de forma barata, eficaz e rápida: eles podem automatizar o preenchimento de documentos, realizar a *due diligence*, reunir e analisar dados antigos, classificar por meio de informações jurídicas e realizar outras atividades que anteriormente exigiam trabalho humano. As oportunidades resultantes e os riscos associados ao trabalho provocaram um amplo debate tanto no campo jurídico quanto em outros setores (SUSSKIND, 2008). A questão que queremos abordar aqui é mais abstrata e complexa, envolvendo o papel da interpretação nos argumentos jurídicos. Aqui, também, os computadores podem ser utilizados de forma útil para realizar muitas tarefas. As pessoas falam de "jurisprudência mecânica" (WALTON; MACAGNO; SARTOR, 2021) ou "ciência jurídica computacional" (LETTIERI; ALTAMURA; GIUGNO; GUARINO; MALANDRINO; PULVIRENTI; VICIDOMINI; ZACCAGNINO, 2018), sistemas computacionais de raciocínio jurídico capazes de explorar bases de dados jurídicos (ALETRAS; TSARAPATSANIS; PREOȚIUC-PIETRO; LAMPOS, 2016), identificar regras relevantes, tomar decisões (BINNS, 2020), gerar argumentos e, também, explicar sua cadeia de raciocínio aos usuários (ASHLEY, 2017). As máquinas participam

[230] O animado debate sobre a diferença entre correlação e causalidade na ciência é um caso influente, desencadeando um profundo repensar de questões epistemológicas básicas, como a relação entre explicações e previsões. (PEARL, 2000; PEARL; MACKENZIE, 2018; BREIMAN, 2001; SHMUELI, 2020; SOBER, 2016).

de forma autônoma da comunicação jurídica: elas podem gerar informações juridicamente relevantes, elaborar um argumento e até mesmo explicá-lo.

O problema é mais profundo e não diz respeito apenas à possível ameaça às habilidades dos trabalhadores humanos e seus empregos. Diz respeito aos fundamentos do direito positivo moderno, que envolvem a autonomia do direito e a questão da interpretação. Como Hildebrandt argumentou, nossa forma de sistema jurídico se desenvolveu como resultado da disseminação da máquina de impressão e das mudanças resultantes na forma como produzimos, escrevemos e lemos textos (HILDEBRANDT, 2020; LUHMANN, 1993, p. 349). A máquina de impressão produz textos padronizados, idênticos e imutáveis, que são retirados da "*mouvance*" da comunicação oral e dos manuscritos (ZUMTHOR, 1972; EISENSTEIN, 1979) – livros que escapam à prática do comentário. Em textos anteriores, numa cultura que se manteve preponderantemente oral, foram adicionados glosas e comentários em cada leitura e se tornaram parte do texto, que mudava ("*moved*") continuamente, produzindo cada vez uma comunicação diferente (ASSMANN; GLADIGOW, 1995). O texto "móvel" incorporou a interpretação.

Quando, com a máquina de impressão, o texto se tornou fixo e permaneceu o mesmo em todas as leituras, as interpretações se multiplicaram e se tornaram variáveis. A escrita, argumenta Luhmann, dá origem à diferença entre texto e interpretação, que a máquina de impressão generaliza (LUHMANN, 1993, p. 362). O texto fixo deve ser interpretado para fazer sentido no contexto específico. Entretanto, as situações em que um texto é lido são todas únicas, diferentes de qualquer outra; se o texto permanecer o mesmo, a forma de considerá-lo deve mudar. A pluralidade de interpretações é inevitável e legítima: como os contextos e as circunstâncias são sempre diferentes, as interpretações devem variar para levá-los em conta (ESPOSITO, 2002, p. 226-227). As interpretações de um mesmo texto, portanto, podem ser sempre diferentes, e qualquer interpretação pode ser contestada.

Isso acontece em todos os campos que têm a ver com textos, mas na prática jurídica assume uma forma mais complicada[231]. Se as leis são textos escritos e as decisões judiciais também assumem essa forma, é necessário muito trabalho de interpretação para levar em conta a variedade de circunstâncias e casos jurídicos. Os juízes interpretam as leis e casos anteriores, e os seus observadores (advogados, litigantes, público) interpretam as suas decisões. De acordo com Hildebrandt (2020), a liberdade de interpretação é a base do Estado de Direito moderno. Essa liberdade é a base da autonomia do judiciário. Ela permite ao judiciário seguir a sua própria lógica e critérios. Estes não são ditados pela soberania e podem entrar em conflito com os princípios e preferências do poder político. Nos termos de Fried, "a racionalidade da lei é uma racionalidade à parte", que não segue os princípios da racionalidade geral, mas apenas a "razão artificial da lei" (FRIED, 1981, p. 35, 39 e 58)[232].

A autonomia de interpretação é um requisito básico para a independência da lei, mas não significa arbitrariedade ou obscuridade. As decisões dos juízes devem ser explicadas, ou seja, motivadas (em termos jurídicos) de acordo com a racionalidade específica da lei, explicitando as razões em que se baseiam. De acordo com esta racionalidade, então, as explicações são interpretadas e as decisões podem ser contestadas. "O propósito da interpretação não é assegurar que todos os leitores compreendam o texto da mesma forma, mas que diferentes pessoas que enfrentam o mesmo texto participem de uma comunicação unitária" (LUHMANN, 1993, p. 362). Esse é o tipo de transparência exigida pelo funcionamento controlado do sistema jurídico e aquele segundo o qual a possível transparência dos algoritmos deve ser avaliada. A explicação dada pela inteligência artificial na jurisprudência mecânica atende os requisitos da "razão artificial da lei"? Uma decisão tomada com base em procedimentos automatizados pode ser justificada de modo a permitir o funcionamento da

[231] Sobre a performatividade da linguagem, ver AUSTIN, 1962. No campo jurídico, essa é uma condição básica: as palavras pronunciadas por um juiz ou um legislador são fatos imediatos e têm consequências concretas.

[232] A Teoria sociológica dos Sistemas descreve essas condições como *out-differentiation (Ausdifferenzierung)* do sistema jurídico na sociedade moderna. Ver Luhmann (n. 33), p. 743 *et seq.*

comunicação legal e possivelmente a contestação pelas pessoas envolvidas? A falta de transparência dos algoritmos, que, como vimos, é inevitável em seu uso comunicativo, é compatível com as exigências de transparência das decisões legais?

5 O papel da ambiguidade nos argumentos jurídicos

Em um primeiro nível, esse parece ser o caso. Que os processos digitais que conduzem à decisão são diferentes daqueles de nossa inteligência e possivelmente não são acessíveis ou compreensíveis para os observadores humanos, mas no que diz respeito à comunicação legal, isso não marca necessariamente uma cesura com as decisões tomadas pelos agentes humanos. Como afirmam Canale e Tuzet, "motivação jurisdicional não consiste no relato psicológico do processo que conduziu à decisão, mas na indicação das razões legais que a justificam" (CANALE; TUZET, 2020) ou, como assevera Luhmann, "o argumento não reflete o que o leitor tem em mente" (LUHMANN, 1993, p. 362). Uma motivação correta não implica que os pensamentos e passos que levaram à decisão sejam descritos e, portanto, pode ser argumentado, nem deve ser necessário descrever os processos seguidos pelo algoritmo para chegar ao seu resultado. Não é necessariamente um problema que os processos digitais sejam incompreensíveis para os seres humanos, se o algoritmo for capaz de explicar sua decisão num sentido comunicativo, ou seja, de indicar de forma compreensível as razões legais que a levaram ou, no sentido de Fried (1981), a razão artificial em que se baseia.

Em um segundo nível, no entanto, as coisas são mais complicadas. De uma perspectiva sociológica, o desempenho do direito para a sociedade como um todo é a "absorção da incerteza" na gestão do litígio (LUHMANN, 1966, p. 56-57)[233]. Deve ser possível confiar no fato de que as regras legais são aplicadas a casos concretos e de uma forma válida (LETTIERI, 2020, p. 72). Para absorver a

[233] Na clássica definição de March e Simon: "A absorção da incerteza ocorre quando as inferências são retiradas de um conjunto de evidências e as inferências, ao invés das próprias evidências, são, então, comunicadas" (MARCH; SIMON, 1958, p. 165).

incerteza, a validade deve ser argumentada (motivada), ou seja, a decisão legal deve ser justificada, fornecendo fundamentos para ela. Como os casos a serem tratados são sempre diferentes, os fundamentos devem ser apropriados ao contexto (WALTON; MACAGNO; SARTOR, 2021), mas a própria decisão sobre o que conta como contexto pode ser controversa e levar a dúvidas e discordâncias (EASTERBROOK, 2017, p. 81, 83-84). Na maioria dos casos, além disso, muitas das provas apresentadas por ambas as partes para apoiar seus argumentos são baseadas em regras e precedentes conflitantes (BERMAN; HAFNER, 1988). Embora todas as decisões jurídicas se refiram ao mesmo conjunto de regras, os argumentos (explicações) devem ser diferentes, caso a caso, e coordenados de forma flexível entre si.

Para que a coordenação seja possível, a ambiguidade desempenha um papel fundamental na comunicação jurídica (LETTIERI, 2020. HILDEBRANDT, 2020. HOFFMANN-RIEM, 2020). Os argumentos "são tipicamente vagos e ambíguos" (WALTON; MACAGNO; SARTOR, 2021, p. 4), ou seja, "suscetíveis de mais de uma interpretação razoável" (SOLAN, 2004). As normas legais são caracterizadas por múltiplas camadas de ambiguidade, que dificultam sua organização em um todo formal e totalmente consistente. Em casos típicos de argumentos jurídicos "a inconsistência é a norma" (WALTON; MACAGNO; SARTOR, 2021, p. 5; MATTARELLA, 2011), e, na verdade, o objetivo do argumento só pode ser "evitar inconsistências visíveis" (LUHMANN, 1993, p. 356). O objetivo real do argumento não é conseguir coerência lógica abstrata, mas fazer com que os fundamentos da decisão pareçam convincentes – e uma justificativa jurídica é convincente não porque todos os seus passos foram verificados: "A racionalidade da gestão de problemas jurídicos reside... não na exatidão lógica de suas conclusões... Deve bastar que convença a todos de que convenceu seu autor" (LUHMANN, 1966, p. 55, 59). A motivação (explicação) parece convincente quando todos estão convencidos de que outros a acham convincente. A eficácia retórica conta mais do que a consequência lógica das etapas do argumento, que não é examinada em detalhes.

Advogados e juízes, que são "os mestres da razão artificial da lei", são por experiência e expertise profissional muito competentes para lidar com a ambiguidade e usá-la para fins retóricos, por exemplo, aplicando "uma intuição treinada e disciplinada em que a multiplicidade de detalhes é muito extensa para permitir que nossas mentes trabalhem sobre ela dedutivamente" (FRIED, 1981, p. 57). A tarefa dos advogados, afirma Garfinkel, é tornar ambíguas as interpretações de fatos e leis (GARFINKEL, 1967, p. 111). Funciona bem quando se interage com seres humanos, pois para uma comunicação eficaz é suficiente regular "a apresentação, não a produção da decisão" (LUHMANN, 1966, p. 106). Advogados e juízes devem apresentar um relato convincente das decisões que tomam, mas a sua interpretação pode e muitas vezes deve permanecer vaga, pois "não se preocupa com a forma como compreendemos ou produzimos textos, mas sim com a forma como estabelecemos a aceitabilidade de uma leitura específica dos mesmos" (WALTON; MACAGNO; SARTOR, 2021, p. 9). O que os observadores interpretam é a interpretação geralmente ambígua por parte do juiz ou do advogado.

Para os algoritmos, contudo, a ambiguidade é um desafio. A gestão competente da vagueza é notoriamente um problema para as máquinas, que vem sendo discutido há décadas nos discursos sobre os limites da inteligência artificial (DREYFUS, 1972). Ainda hoje é difícil, para os algoritmos, lidar com os vários níveis de ambiguidade sempre presentes na comunicação humana ou, no campo jurídico, gerenciar a multiplicidade de possíveis interpretações de regras e normas (LETTIERI, 2020). Além disso, se o foco passa da inteligência das máquinas (o que elas podem compreender e como) para sua participação na comunicação, surgem outros problemas relacionados à ambiguidade: não só a dificuldade das máquinas em lidar com a ambiguidade da comunicação humana, mas também a dificuldade de elas mesmas gerarem uma comunicação ambígua, ou seja, de administrarem de forma competente a ambiguidade exigida pelos argumentos jurídicos.

As explicações jurídicas produzidas pelos algoritmos devem ser elas mesmas ambíguas, assim como são aquelas que resultam da interpretação de

normas jurídicas por humanos. A ambiguidade não é, como tendemos a pensar, oposta à transparência (ANANNY; CRAWFORD, 2018; OLSEN, 2014; HEIMSTÄDT; DOBUSCH, 2020), mas, ao contrário, é necessária para fornecer a multiplicidade de interpretações jurídicas indispensável para a contestabilidade. Como Hildebrandt afirma, "devido à ambiguidade inerente à linguagem humana, os ICIs[234] orientados por texto geram um tipo específico de multi-interpretabilidade que, por sua vez, gera um tipo específico de contestabilidade" (HILDEBRANDT, 2020, p. 7-8). Para contestar uma decisão, é preciso ser capaz de desenvolver uma perspectiva sobre a decisão que seja independente daquela fornecida pelo tomador da decisão (O'HARA, 2020), ou seja, questionar a sua interpretação. Contudo, para fazer isso, a motivação deve parecer juridicamente ambígua – isto é, deve ser, como vimos, suscetível a mais de uma interpretação razoável. A máquina que não tem sua própria perspectiva não interpreta, portanto, suas explicações carecem de ambiguidade. As explicações que ela oferece são reformulações das decisões que são tomadas seguindo outras regras, portanto não faz sentido perguntar o que o algoritmo significou – os algoritmos não significam nada.

A falta de uma gestão competente da ambiguidade é um problema que também é percebido em experiências que tentam realizar uma forma de XAI no campo jurídico. Mesmo para os modelos computacionais mais recentes que produzem argumentação jurídica, a falta de ambiguidade é uma restrição (WALTON; MACAGNO; SARTOR, 2021, p. 11) muito além do que é exigido na comunicação legal entre seres humanos guiados pelo imperativo de parecer convincente e absorver a incerteza. Paradoxalmente, então, pode-se dizer que o problema da interpretação na argumentação jurídica – mesmo e precisamente quando se trata de algoritmos que são obscuros para a inteligência humana – não é que a máquina não explique o suficiente, mas que deve explicar demais, e com muita precisão. Como reconhecem os estudiosos nesse campo, esse nível de detalhe pode obscurecer, em vez de iluminar, a prática da comunicação jurídica:

[234] "Information and communication infrastructures". Tradução: Infraestruturas de informação e comunicação.

> Estamos bem cientes de que, ao utilizar a abordagem de argumentação estruturada e formalista, existe o perigo de confundir os leitores mais do que explicar-lhes como os tribunais podem fazer um melhor trabalho de luta com os difíceis (chamados de perversos) problemas de interpretação estatutária (WALTON; MACAGNO; SARTOR, 2021, p. 12)[235].

Por um lado, portanto, há o risco de que a explicação não seja convincente. Por outro lado, se for convincente, talvez possa surgir um problema ainda mais grave: podem ser impostos limites à liberdade de interpretação que sustenta a autonomia da comunicação jurídica, e pode haver o risco de que o uso de modelos automatizados possa alterar características fundamentais do Estado de Direito (LETTIERI, 2020). Como vimos acima, a "razão artificial da lei" não coincide com a racionalidade geral da sociedade ou mesmo com a coerência abstrata de um argumento lógico. A jurisprudência mecânica, entretanto, quando identifica e aplica as regras jurídicas relevantes ao caso em questão, não funciona com os argumentos retóricos eficazes que caracterizam o raciocínio e a interpretação jurídica (ASHLEY, 2017), que são possivelmente ambíguos e não totalmente coerentes. A autonomia da comunicação jurídica, com todas as suas implicações na estrutura da sociedade moderna, pode tomar uma forma diferente como consequência da intervenção de algoritmos na comunicação.

Que liberdade resta para aqueles que devem interpretar um argumento jurídico "mecânico"? E, em particular, como a decisão pode ser contestada? Os argumentos produzidos pelos algoritmos não são interpretações, contingentes e passíveis de revisão, mas descrições de uma série de etapas formais. O observador pode descobrir um erro formal e contestar a decisão a esse nível. Entretanto, não pode explorar e contestar a interpretação, porque a máquina não interpretou nada. Todos os argumentos que se referem a razões e motivos de interpretação, a saber, "os fatores que podem levar um tomador de decisão a

[235] Original: "We are well aware that in using the structured and formalistic argumentation approach there is the danger of confusing readers more than explaining to them how the courts can do a better job of grappling with the hard (so-called wicked) problems of statutory interpretation".

selecionar uma ou outra interpretação" (WALTON; MACAGNO; SARTOR, 2021, p. 97 et seq.), podem ser de fato desqualificados, e com eles um componente fundamental da comunicação jurídica na sociedade moderna.

6 Conclusão: comunicação com as máquinas

A observação do desafio colocado pelos algoritmos opacos sob a perspectiva da comunicação revela uma multiplicidade de perguntas fascinantes e difíceis. Algumas questões se dissolvem, como aquela baseada no teste *Turing*: interagimos rotineiramente com parceiros digitais sem nos perguntarmos se eles são seres humanos ou não. Outras questões tomam uma forma diferente, por exemplo, o complexo problema do viés, que envolve tanto a dimensão do viés algorítmico, refletindo os valores dos programadores (CRAWFORD, 2016), como a do viés de dados, dependendo da entrada descoordenada de bilhões de participantes, sensores e outras fontes digitais (MEHRABI MORSTATTER; SAXENA; LERMAN; GALSTYAN, 2021). Ainda, outras questões surgem relacionadas à experiência prática acumulada em muitos campos. O uso de algoritmos para tarefas específicas está quase inadvertidamente levando ao surgimento de diversos, e extremamente complexos, problemas relacionados ao seu envolvimento na comunicação. A questão da interpretação na argumentação jurídica é um exemplo particularmente significativo. O problema não é como as máquinas funcionam, mas como elas participam da comunicação jurídica.

Referências

ALETRAS, N.; TSARAPATSANIS, D.; PREOȚIUC-PIETRO, D.; LAMPOS, V. Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing Perspective. ***PeerJ Computer Science***, 2:e93, 2016. Disponível em: https://doi.org/10.7717/peerj-cs.93 . Acesso em: 18 nov. 2022.

ANANNY, M.; CRAWFORD, K. Seeing Without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability. **New Media & Society**, v. 20, n. 3, p. 973-989, 2018. Disponível em: https://doi.org/10.1177/1461444816676645 . Acesso em: 18 nov. 2022.

ASHLEY, K. **Artificial Intelligence and Legal Analytics:** New Tools for Law Practice in the Digital Age. Cambridge: Cambridge University Press, 2017.

ASSMANN, J.; GLADIGOW, B. (eds.). **Text und Kommentar.** Archäologie der Literarischen Kommunikation IV. Leiden: Brill; Fink, 1995.

AUSTIN, J. L. **How to Do Things with Words.** Oxford: Oxford University Press, 1962.

BATESON, G. **Steps to an Ecology of Mind.** Chicago: University of Chicago Press, 1972.

BERMAN, D.; HAFNER, C. Obstacles to the Development of Logic-Based Models of Legal Reasoning. *In*: WALTER, C. (ed.). **Computer Power and Legal Language.** Westport: Greenwood Press, 1988.

BINNS, R. Analogies and disanalogies between machinedriven and human-driven legal judgement. **Journal of Cross-disciplinary Research in Computational Law**, v. 1, n. 1, p. 1-16, dez. 2020. Disponível em: https://journalcrcl.org/crcl/article/view/5 . Acesso em: 21 nov. 2022.

BOELLSTORFF, T. Making Big Data, in Theory. **First Monday**, v. 18, n. 10, set. 2013. Disponível em: https://doi.org/10.5210/fm.v18i10.4869 . Acesso em: 21 nov. 2022.

BREIMAN, L. Statistical Modeling: The Two Cultures. **Statistical Science** 199, v. 16, n. 3, p. 199-215, ago. 2001. Disponível em: https://www.jstor.org/stable/2676681 . Acesso em: 21 nov. 2022.

BUHRMESTER, V.; MÜNCH, D.; ARENS, M. Analysis of Explainers of Black Box Deep Neural Networks for Computer Vision: A Survey. **Computer Science**, arXiv:1911.12116, p. 1-22, 2019. Disponível em: https://doi.org/10.48550/arXiv.1911.12116 . Acesso em: 21 nov. 2022.

BURRELL, J. How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. **Big Data & Society**, v. 3, n. 1, p. 1-12, 2016. Disponível em: https://doi.org/10.1177/2053951715622512 . Acesso em: 21 nov. 2022.

BUSUIOC, M. Accountable Artificial Intelligence: Holding Algorithms to Account. **Public Administration Review**, v. 81, n. 5, p. 825-836, 2020. Disponível em: https://doi.org/10.1111/puar.13293 . Acesso em: 21 nov. 2022.

CANALE, D.; TUZET, G. **La Giustificazione della Decisione Giudiziale.** Torino: Giappichelli, 2020.

CARDON, D.; COINTET J.-P.; MAZIERES, A. La revanche des neurons. L'invention des machines inductives et la controverse de l'intelligence artificielle. **Réseaux**, v. 211, n. 5, p. 173-220, 2018. Disponível em: https://doi.org/10.3917/res.211.0173 . Acesso em: 21 nov. 2022.

CARUANA, R.; LOU, Y.; GEHRKE, J.; KOCH, P.; STURM, P.; ELHADAD, N. Intelligible Models for Healthcare: Predicting Pneumonia Risk and Hospital 30-day Readmission. *In*: PROCEEDINGS OF ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING, 21, 2015, Sydney. **Proceedings** […]. Sydney, Association for Computing Machinery, 2015. Disponível em: https://doi.org/10.1145/2783258.2788613 . Acesso em: 21 nov. 2022.

CIMIANO, P.; RUDOLPH, S.; HARTFIEL, H. Computing Intensional Answers to Questions – An Inductive Logic Programming Approach. **Data & Knowledge Engineering**, v. 69, n. 3, p. 261-278, mar. 2010. Disponível em: https://doi.org/10.1016/j.datak.2009.10.008 . Acesso em: 21 nov. 2022.

CRAWFORD, K. Artificial Intelligence's White Guy Problem. **The New York Times**, New York, 25 jun. 2016. Disponível em: https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html . Acesso em: 21 nov. 2022.

DEANGELIS, S. F. Artificial Intelligence. How Algorithms Make Systems Smart. **Wired**, Boone, 2014. Disponível em: https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/ . Acesso em: 23 jun. 2021.

DOSHI-VELEZ, F.; KIM, B. Towards A Rigorous Science of Interpretable Machine Learning. **Statistics**, arXiv:1702.08608v2, p. 1-13, 2017. Disponível em: https://doi.org/10.48550/arXiv.1702.08608 . Acesso em: 21 nov. 2022.

DOSHI-VELEZ, F.; KORTZ, M.; BUDISH, R.; BAVITZ, C.; GERSHMAN, S.; O´BRIEN, D.; SCOTT, K., SCHIEBER, S.; WALDO, J., WEINBERGER, D.; WELLER, A.; WOOD, A. Accountability of AI Under the Law: The Role of Explanation. **Computer Science**, arXiv:1711.01134v3 , p. 1-21, 2017. Disponível em: https://doi.org/10.48550/arXiv.1711.01134 . Acesso em: 21 nov. 2022.

DREYFUS, H. **What Computers Can't Do**. Cambridge: The MIT Press, 1972.

EASTERBROOK, F. H. The Absence of Method in Statutory Interpretation. **Chicago Law Review**, v. 84, n. 81, p. 81-97, 2017. Disponível em: https://lawreview.uchicago.edu/publication/absence-method-statutory-interpretation . Acesso em: 21 nov. 2022.

EISENSTEIN, E. L. **The Printing Press as an Agent of Change.** Communications and Cultural Transformations in Early-Modern Europe. Cambridge: Cambridge University Press, 1979.

ESPOSITO, E. **Soziales Vergessen.** Formen und Medien des Gedächtnisses der Gesellschaft. Berlin: Suhrkamp, 2002.

ESPOSITO, E. Artificial Communication? The Production of Contingency by Algorithms. **Zeitschrift für Soziologie**, v. 46, n. 4, p. 249-265, ago. 2017. Disponível em: https://doi.org/10.1515/zfsoz-2017-1014 . Acesso em: 21 nov. 2022.

ESPOSITO, E. **Artificial Communication.** How Algorithms Produce Social Intelligence. Cambridge: MIT Press, 2021.

FRIED, C. Artificial Reason of the Law or: What Lawyers Know. **Texas Law Review**, v. 60, n. 1, p. 23-32, 1981. Disponível em: https://informallogic.ca/index.php/informal_logic/article/view/2598/2039 . Acesso em: 21 nov. 2022.

GARFINKEL, H. **Studies in Ethnomethodology.** Hoboken: Prentice Hall, 1967.

GILPIN, L. H.; BAU, D.; YUAN, B. Z.; BAJWA, A.; SPECTER, M.; KAGAL, L. Explaining Explanations: An Overview of Interpretability of Machine Learning. **Computer Science**, arXiv:1806.00069v3, p. 1-10, 2018. Disponível em: https://doi.org/10.48550/arXiv.1806.00069 . Acesso em: 21 nov. 2022.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. **Deep Learning** (Adaptive Computation and Machine Learning). Cambridge: MIT Press, 2016.

HAMMOND, K. **Practical Artificial Intelligence for Dummies.** Hoboken: Wiley, 2015.

HAO, K. The UK exam debacle reminds us that algorithms can't fix broken systems. **MIT Technology Review**, Cambridge, 20 ago. 2020. Disponível em: https://www.technologyreview.com/2020/08/20/1007502/uk-exam-algorithm-cant-fix-broken-system/#:~:text=Tech%20policy-,The%20UK%20exam%20debacle%20reminds%20us%20that%20algorithms%20can't,for%20standardization%20above%20all%20else.&text=When%20the%20UK%20first%20set,the%20premise%20seemed%20perfectly%20reasonable . Acesso em: 2 out. 2020.

HEIMSTÄDT, M.; DOBUSCH, L. Transparency and Accountability: Causal, Critical and Constructive Perspectives. **Organization Theory**, v. 1, n. 4, p. 1-12, 2020. Disponível em: https://doi.org/10.1177/2631787720964216 . Acesso em: 21 nov. 2022.

HILDEBRANDT, M. **Law for Computer Scientists and Other Folk.** Oxford: Oxford University Press, 2020.

HILDEBRANDT, M. The Adaptive Nature of Text-Driven Law. **Journal of Cross-disciplinary Research in Computational Law**, v. 1, n. 1, p. 1-15, nov. 2020. Disponível em: https://journalcrcl.org/crcl/article/view/2 . Acesso em: 21 nov. 2022.

HOFFMANN-RIEM, W. Legal Technology/Computational Law: Preconditions, Opportunities and Risks. **Journal of Cross-disciplinary Research in Computational Law**, v. 1, n. 1, p. 1-16, nov. 2020. Disponível em: https://journalcrcl.org/crcl/article/view/7 . Acesso em: 21 nov. 2022.

HOLZINGER A.; LANGS, G.; DENK, H.; ZATLOUKAL, K.; MÜLLER, H. Causability and explainability of artificial intelligence in medicine. **WIREs Data Mining and Knowledge Discovery**, v. 9, n. 4, e1312, abr. 2019. Disponível em: https://doi.org/10.1002/widm.1312 . Acesso em: 21 nov. 2022.

LATOUR, B. **Pandora's Hope:** Essays on the Reality of Science Studies. Harvard: Harvard University Press, 1999.

LETTIERI, N.; ALTAMURA, A.; GIUGNO, R.; GUARINO, A.; MALANDRINO, D.; PULVIRENTI, A.; VICIDOMINI, F.; ZACCAGNINO, R. Ex Machina: Analytical Platforms, Law and the Challenges of Computational Legal Science. **Future Internet**, v. 10, n. 5, p. 1-25, 2018. Disponível em: https://doi.org/10.3390/fi10050037 . Acesso em: 21 nov. 2022.

LETTIERI, N. Law, Rights, and the Fallacy of Computation. **Jura Gentium**, v. XVII, n. 2, p. 72-87, 2020. Disponível em: https://www.juragentium.org/Centro_Jura_Gentium/la_Rivista_files/JG_2020_2/JG_2020_2_Lettieri.pdf . Acesso em: 21 nov. 2022.

LIPTON, Z. C. The Mythos of Model Interpretability: In machine learning, the concept of interpretability is both important and slippery. **ACM Queue**, v. 16, n. 3, p. 31-57, 2018. Disponível em: https://doi.org/10.1145/3236386.3241340 . Acesso em: 21 nov. 2022.

LUHMANN, N. **Die Gesellschaft der Gesellschaft.** Berlin: Suhrkamp, 1997.

LUHMANN, N. **Recht und Automation in der öffentlichen Verwaltung.** Berlin: Duncker & Humblot, 1966.

LUHMANN, N. **Die Wissenschaft der Gesellschaft.** Berlin: Suhrkamp, 1990.

LUHMANN, N. **Das Recht der Gesellschaft.** Berlin: Suhrkamp, 1993.

LUHMANN, N. **Die Kontrolle von Intransparenz.** Berlin: Suhrkamp, 2017.

LUM, K.; ISAAC, W. To Predict and Serve. **Significance**, v. 13, n. 5, p. 14-19, out. 2016. Disponível em: https://doi.org/10.1111/j.1740-9713.2016.00960.x . Acesso em: 21 nov. 2022.

MARCH, J. G.; SIMON, H. A. **Organizations.** Hoboken: Wiley, 1958.

MATTARELLA, B. G. **La trappola delle leggi:** molte, oscure, complicate. Bologna: Il Mulino 2011.

MEHRABI, N; MORSTATTER, F.; SAXENA, N.; LERMAN, K.; GALSTYAN, A. A Survey on Bias and Fairness in Machine Learning. **ACM Computing Surveys**, v. 54, n. 6, p. 1-35, jul. 2021. Disponível em: https://doi.org/10.1145/3457607 . Acesso em: 21 nov. 2022.

MILLER, T. Explanation in Artificial Intelligence: Insights from the Social Sciences. **Artificial Intelligence**, v. 267, p. 1-38, fev. 2019. Disponível em: https://doi.org/10.1016/j.artint.2018.07.007 . Acesso em: 21 nov. 2022.

MONROE, D. AI, Explain Yourself. **Communications of the ACM**, v. 61, n. 11, p. 11-13, nov. 2018. Disponível em: https://doi.org/10.1145/3276742 . Acesso em: 21 nov. 2022.

MONTAVON, G.; SAMEK,W.; MÜLLER, K.-R. Methods for Interpreting and Understanding Deep Neural Networks. **Digital Signal Processing**, v. 73, p. 1-15, fev. 2018. Disponível em: https://doi.org/10.1016/j.dsp.2017.10.011 . Acesso em: 21 nov. 2022.

MUGGLETON, S.; DE RAEDT, L. Inductive Logic Programming: Theory and Methods. **The Journal of Logic Programming**, v. 19-20, p. 629-679, maio/jun.1994. Disponível em: https://doi.org/10.1016/0743-1066(94)90035-3 . Acesso em: 21 nov. 2022.

O'HARA, K. Explainable AI and the Philosophy and Practice of Explanation. **Computer Law & Security Review**, v. 39, 105474, nov. 2020. Disponível em: https://doi.org/10.1016/j.clsr.2020.105474 . Acesso em: 21 nov. 2022.

O'NEIL, C. **Weapons of Math Destruction.** New York: Crown Publishing Group, 2016.

OLSEN, J. P. Accountability and Ambiguity. In: Bovens, M.; Goodin, R. E.; Schillemans, T. (eds.). **The Oxford Handbook of Public Accountability.** Oxford: Oxford University Press, 2014.

PASQUALE, F. **The Black Box Society.** The Secret Algorithms That Control Money and Information. Harvard: Harvard University Press, 2015.

PEARL, J. **Causality.** Cambridge: Cambridge University Press, 2000.

PEARL, J.; MACKENZIE, D. **The Book of Why:** The New Science of Cause and Effect. New York: Basic Books, 2018.

PREY, R. Nothing Personal: Algorithmic Individuation on Music Streaming Platforms. **Media, Culture & Society**, v. 40, n. 7, p. 1086-1100, 2018. Disponível em: https://doi.org/10.1177/0163443717745147 . Acesso em: 21 nov. 2022.

QUINLAN, J. R. Induction of Decision Trees. **Machine Learning**, v. 1, p. 81-106, 1986. Disponível em: https://doi.org/10.1007/BF00116251 . Acesso em: 21 nov. 2022.

ROBBINS, S. A Misdirected Principle With a Catch: Explicability for AI. **Minds and Machines**, v. 29, p. 495-514, 2019. Disponível em: https://doi.org/10.1007/s11023-019-09509-3 . Acesso em: 22 nov. 2022.

ROHLFING, K. J.; CIMIANO, P.; SCHARLAU, I.; MATZNER, T.; BUHL, H. M.; BUSCHMEIER, H.; ESPOSITO, E.; GRIMMINGER, A.; HAMMER, B.; KERN, F.; KOPP, S.; THOMMES, K.; NGOMO, A.-C. N.; SCHULTE, C.; WACHSMUTH, H.; WAGNER, P.; WREDE, B. Explanations as a Social Practice: Toward a Conceptual Framework for the Social Design of AI Systems. **IEEE Transactions on Cognitive and Developmental Systems**, v. 13, n. 3, p. 717-728, set. 2021. Disponível em: https://doi.org/10.1109/TCDS.2020.3044366 . Acesso em: 22 nov. 2022.

ROSCHER, R.; BOHN, B.; DUARTE, M. F.; GARCKE, J. Explainable Machine Learning for Scientific Insights and Discoveries. **IEEE Access**, v. 8, p. 42200-42216, 2020. Disponível em: https://doi.org/10.1109/ACCESS.2020.2976199 . Acesso em: 22 nov. 2022

RUDIN, C. Stop Explaining Black Box Machine Learning Models for High Stake Decisions and Use Interpretable Models Instead. **Nature Machine Intelligence**, v. 1, p. 206-215, maio 2019. Disponível em: https://doi.org/10.1038/s42256-019-0048-x . Acesso em: 22 nov. 2022.

RUSSELL, S.; NORVIG, P. **Artificial Intelligence:** A Modern Approach. Hoboken: Prentice Hall, 2003.

SHMUELI, G. To Explain or to Predict? **Statistical Science**, v. 25, n. 3, p. 289-310, ago. 2020. Disponível em: https://doi.org/10.1214/10-STS330. Acesso em: 22 nov. 2022.

SILVER, D.; HASSABIS, D. AlphaGo: Mastering the Ancient Game of Go with Machine Learning. **Google DeepMind**, 27 jan. 2016. Disponível em: https://ai.googleblog.com/2016/01/alphago-mastering-ancient-game-of-go.html . Acesso em: 23 jun. 2021.

SOBER, E. **Ockham's razors:** a user's manual. Cambridge: Cambridge University Press 2016.

SOLAN, L. Pernicious Ambiguity in Contracts and Statutes. **Chicago-Kent Law Review**, v. 79, n. 3, p. 859-888, 2004. Disponível em: https://scholarship.kentlaw.iit.edu/cklawreview/vol79/iss3/22 . Acesso em: 22 nov. 2022.

SUSSKIND, R. **The End of Lawyers?** Rethinking the Nature of Legal Services. Oxford: Oxford University Press, 2008.

WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. Transparent, Explainable and Accountable AI for Robotics. **Science Robotics**, v. 2, n. 6, eaan6080, maio 2017. Disponível em: https://doi.org/10.1126/scirobotics.aan6080 . Acesso em: 22 nov. 2022.

WALTON, D.; MACAGNO, F.; SARTOR, G. **Statutory Interpretation.** Pragmatics and Argumentation. Cambridge: Cambridge University Press, 2021.

WEINBERGER, D. Our Machines Now Have Knowledge We'll Never Understand. **Wired**, Boone, 18 abr. 2017. Acesso em: 23 jun. 2021. Disponível em: https://www.wired.com/story/our-machines-now-have-knowledge-well-never-understand/ . Acesso em: 22 nov. 2022.

WEYER, J.; SCHULZ-SCHAEFFER, I. (eds.). **Management Komplexer Systeme:** Konzepte Für die Bewältigung von Intransparenz, Unsicherheit und Chaos. Berlin: De Gruyter, 2009.

ZUMTHOR, P. **Introduction à la poésie orale.** Paris: Seuil, 1972.

9. Os sentidos do direito da proteção de dados pessoais: desmembrando a complexidade do direito e dos direitos

Rafael A. F. Zanatta[236]

Introdução

Em preparação para uma aula inaugural realizada na pós-graduação em direito da Pontifícia Universidade Católica do Rio de Janeiro em 2022, a professora Caitlin Mulholland me fez uma pergunta aparentemente simples, mas profundamente desafiadora: o que, afinal, é o direito de proteção de dados pessoais?

Apesar da simplicidade da questão – as perguntas aparentemente simples geralmente são as mais difíceis de responder –, penso que ela é crucial pois nos coloca diante de perguntas muito basilares. Proteção de dados pessoais *para quê*? Proteção de dados *para quem* em uma democracia? Por que declarar que todo cidadão possui o direito de ter seus dados tratados de forma leal e justa, tal como feito na Carta de Direitos Fundamentais da União Europeia em 2000? O que isso significa, afinal? Como tal direito (*law*) se transmuta em direitos (*rights*)?

Trazendo a discussão para o nosso território e sistema jurídico: por que afirmarmos, em nossa Constituição Federal, que a proteção de dados pessoais é um direito fundamental previsto no art. 5º, ao lado de outros direitos fundamentais como a livre manifestação do pensamento, a inviolabilidade da liberdade de crença, a livre expressão da atividade intelectual, a inviolabilidade do domicílio, a inviolabilidade do sigilo das comunicações e a vida íntima, entre

[236] Pesquisador de Pós-Doutorado do Departamento de Filosofia e Teoria Geral do Direito da Faculdade de Direito da USP. Doutor pelo Instituto de Energia e Ambiente da USP, com período de formação no Instituto do Direito da Informação da Universidade de Amsterdam. Mestre pela Faculdade de Direito da USP. Mestre em Direito e Economia Política pela Universidade de Turim. Bacharel pela Universidade Estadual de Maringá. É diretor da Data Privacy Brasil.

outros direitos fundamentais? Qual o sentido desse novo direito constitucional que exige que seja assegurado o direito à proteção de dados pessoais (art. 5º, LXXIX, CF)? E por que ele pode ser visto como "fundamental" (Albers & Sarlet, 2022)? Por que o direito da proteção de dados pessoais pode promover dignidade e justiça nas relações sociais em uma comunidade política?

A proteção de dados pessoais possui um conjunto de finalidades teleológicas, concebidas em uma teoria política democrática. Ela não é um fim em si mesmo, mas busca fazer avançar certos tipos de ideais democráticos, como os direitos de liberdade, de devido processo, de igualdade e de redução de desigualdades entre pessoas, que devem ser tratadas com dignidade. Este capítulo se dedica a essas questões maiores, explorada há muitas décadas por autores como Stefano Rodotà[237] e Alan Westin[238] e retomada por filósofos contemporâneos. Não é meu objetivo, portanto, uma análise técnica, em estilo puramente jurídico, da Lei Geral de Proteção de Dados Pessoais, a Lei 13.709, aprovada em 2018 após quase dez anos de discussões no Poder Executivo e no Legislativo no Brasil.[239] Será preciso dar um passo atrás para uma investigação um pouco mais ampla sobre os sentidos do direito da proteção de dados pessoais de um ponto de vista teórico e filosófico. Portanto, adoto um recorte específico de reflexão da proteção de dados pessoais a partir da Filosofia e Teoria Geral do Direito.

A proteção de dados pessoais será conceitualizada aqui, de forma bastante ampla, como um conjunto integrado de práticas jurídicas, tecnológicas, éticas e sociais que visam proteger a dignidade, os direitos e os interesses das pessoas naturais, tanto de forma individual quanto coletiva, diante dos processos de

[237] Stefano Rodotà (1933-2017) foi um jurista italiano, professor da Universidade de Roma e presidente da Autoridade Italiana de Proteção de Dados Pessoais. Foi um dos pioneiros da disciplina jurídica da proteção de dados pessoais na Itália e atuou por mais de quatro décadas no tema. Foi um dos autores da legislação italiana de proteção de dados pessoais na década de 1990.
[238] Alan Westin (1929-2013) foi um cientista político estadunidense, professor da Universidade de Columbia e pioneiro do campo de *informational privacy*. Westin foi um dos mais renomados acadêmicos no tema de privacidade e proteção de dados pessoais. Teve presença ativa nos debates no Congresso dos EUA que deram origem ao *Fair Credit Reporting Act* de 1970 e o *Privacy Act* de 1974.
[239] Para uma análise da trajetória da legislação do ponto de vista de processo legislativo e ideias mobilizadoras, ver Doneda (2022) e Zanatta (2023).

datificação. Esses processos ocorrem através de fluxos complexos de dados pessoais (dados relacionados a uma pessoa natural identificada ou identificável) em ecossistemas informacionais, incluindo arquivos, sistemas computacionais, algoritmos e plataformas, que moldam interações e produzem efeitos em diversas esferas da vida.

Já o direito da proteção de dados pessoais, em sentido também bastante amplo, pode ser definido como um campo normativo que emerge dentro de um contexto social e tecnológico dinâmico, constituído por um conjunto de práticas, discursos e mobilizações ancoradas em um saber jurídico específico, orientado à promoção de certos tipos de direitos das pessoas naturais com relação às múltiplas situações jurídicas que envolvem o tratamento de seus dados pessoais.[240] Este saber jurídico, por sua vez, se traduz em normas jurídicas como leis, tratados e acordos internacionais, bem como regimes interpretativos dessas normas pelo sistema de justiça.[241] Nesse sentido, o direito da proteção de dados pessoais não se esgota em leis específicas sobre proteção de dados pessoais. Está absolutamente além disso pois envolve todas essas práticas institucionais e de adjudicação, incluindo o trabalho dos profissionais de interpretação das normas (MacCormick, 2005).

O direito de proteção de dados pessoais não é a mesma coisa que o direito de privacidade. Como ponto de partida, deve-se considerar que a privacidade é um dos componentes normativos da proteção de dados pessoais, mas não se confunde com ela. A proteção de dados pessoais busca avançar outros ideais normativos, como o livre desenvolvimento da personalidade, a redução das assimetrias de poder, a equidade e não discriminação, e as cláusulas assecuratórias de liberdade, em sentido amplo. A LGPD é categórica ao afirmar

[240] No sentido de Neil MacCormick, o direito é uma "ordem institucional normativa". O sistema jurídico não é uma entidade física tangível, mas uma construção ideal e um objeto do pensamento. Isso não o impede de existir no mundo social real (MacCormick, 2005).

[241] O saber jurídico oferece a estrutura formal e interpretativa que fundamenta e legitima esses discursos, mobilizações e práticas. Ele engloba a construção de normas, jurisprudência e doutrinas jurídicas que dão sentido às demandas sociais por proteção de dados, ao mesmo tempo em que molda as expectativas de conformidade e accountability dentro do sistema jurídico. Sobre o sentido do princípio de responsabilização (art. 6º) e as polissemias do termo accountability no direito de proteção de dados, ver Bioni (2023).

que a lei objetiva "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (art. 1º). Possui um "caráter complexo" (Albers, 2013) que será explorado a partir das lentes da filosofia do direito.

Para aprofundar os sentidos do direito da proteção de dados pessoais, começo explorando os pontos de vantagens de uma formulação jurídica tardia no Brasil, que tem se intensificado nos últimos dez anos. Após essa contextualização do campo, analiso algumas premissas filosóficas desse ramo do direito e exponho porque seus valores normativos são múltiplos – e, por isso, interconectados e "complexos" nos termos da filósofa Marion Albers (2013). Os dados não podem ser compreendidos de maneira isolada como simples objetos de propriedade ou controle, pois eles são profundamente entrelaçados com aspectos de identidade pessoal, direitos fundamentais e a própria constituição do sujeito, que está em permanente relação de "socialidade", nos termos de Albers.

Dados pessoais não são meros recursos econômicos ou bens de troca (Doneda, 2006); eles carregam implicações éticas e filosóficas que se relacionam com a dignidade humana e a autodeterminação informacional e são produzidos pelas relações sociais (Schertel Mendes, 2020). Metodologicamente, não faz sentido afirmar que um dado pessoal é *puramente individual*. Os dados pessoais são relacionais – o mero preenchimento de uma ficha de cadastro em um consultório de um dentista já seria uma produção dentro de uma relação social – e são produzidos em arranjos técnicos específicos, cada vez mais intensivos em técnicas de extração silenciosa de informação de dispositivos (como no caso dos metadados) e compartilhamento para sistemas autônomos pela Internet. Os dados pessoais também podem ser produzidos por sistemas computacionais de inferência, como as técnicas de clusterização e *profiling* inauguradas pela ciência da computação nos últimos vinte anos (Zanatta, 2023). Eles são capazes de produzirem grupos *ad hoc*, sem que os seus titulares possuam conhecimento dessas regras de associação (Mittelstadt, 2016). Parte de complexidade da proteção dos dados pessoais reside, também, no reconhecimento da insuficiência do "individualismo metodológico" e das concepções tradicionais de *personally*

identifiable information (Rouvroy, 2018). O argumento de que direitos só se aplicam quando há uma identificação da pessoa natural oculta camadas mais complexas de lesões e riscos que podem decorrer dessas técnicas computacionais de regras de associação e identificação de interesses por técnicas de *profiling* – um dos pilares das técnicas contemporâneas de tratamento automatizado de dados e sistemas de publicidade comportamental.

Na década de 2010 em diante, tornou-se evidente a exaustão do paradigma da identificabilidade individual em razão das técnicas de *group profiling* e as possibilidades de análises inferenciais que são decorrentes de processos de descoberta de conhecimento em bases de dados com grande volumetria e granularidade de informações (Hildebrandt, 2008). Por isso parte dos estudos filosóficos da proteção de dados volta-se à questão da "fixação da identidade" por esses "duplos digitais" e as proteções coletivas que devem ser construídas para evitar situações abusivas ou modulação do nosso próprio comportamento em razão deste processo de análise preditiva (uma "ecografia do futuro", como dizem os franceses) com base nos nossos perfis (Rouvroy, 2020).

Note-se que os problemas produzidos pelas técnicas de exploração econômica de dados e análises preditivas do comportamento de grupos pouco tem a ver com os dilemas da "privacidade individual", no sentido de uma análise de uma informação que seria puramente íntima, como o teor de uma comunicação escrita ou a exposição de uma informação que é tida como confidencial por uma pessoa. Por isso, filósofas como Julie Cohen (2013) e Antoinette Rouvroy (2018) insistem em um abandono das ideias tradicionais de *privacy* – no seu sentido mais estrito de intimidade e comunicações interpessoais – e uma construção teórica apta a considerar os valores de dignidade e de "florescimento humano", uma espécie de proteção coletiva para processos abusivos de fixação e permanência de nossas identidades enquanto grupos nessas técnicas computacionais amplamente usadas por empresas como Amazon, Meta, Google, X e outros. Na feliz expressão do filósofo italiano Luciano Floridi, para que possamos proteger os "peixes", precisamos proteger os

"cardumes", considerando que o capitalismo informacional desta geração se baseia em tipos e não necessariamente em tokens (Floridi, 2014).

Por fim, busco explorar os sentidos dos *direitos de proteção de dados pessoais* – que não se confunde com a ideia do "direito da proteção de dados" enquanto conjunto de práticas, discursos e mobilizações de um determinado saber jurídico apoiado em normas. O que tentarei argumentar é que precisamos voltar a construir uma boa teoria dos direitos de proteção de dados pessoais a partir da decomposição dos seus elementos fundamentais e uma concepção de teoria do direito de modo complexo, considerando que as "relações jurídicas" possuem uma natureza específica e relacional. Eles habilitam não só um conjunto de reivindicações para as pessoas, mas produzem "direitos correlatos". Essa ideia, tão bem desenvolvida por Wesley Hohfled no início do século XX, pode ser melhor desenvolvida para uma adequada compreensão dos *direitos de proteção de dados pessoais*. Por isso busco uma aproximação das ideias de Hohfeld com teorias de "direitos correlatos" elaboradas por juristas da informação como Antonio Herman Benjamin no Brasil.

Portanto, argumentarei neste texto que (i) a proteção de dados pessoais possui um conjunto de valores normativos específicos; (ii) que o direito de proteção de dados pessoais envolve um conjunto de práticas, discursos, mobilizações e normas interdependentes; e que (iii) os direitos de proteção de dados pessoais precisam ser analisados por uma teoria dos direitos (*theory of rights* e não uma *legal theory* ou uma *teoria do direito*). Defenderei que as teorias de Wesley Hohfeld podem auxiliar na compreensão de um outro tipo de complexidade distinto do analisado pela filósofa Marion Albers.

1. Os pontos de vantagens de uma formulação teórica tardia em proteção de dados

Para uma correta compreensão dos sentidos da proteção de dados pessoais no Brasil, é preciso reconhecer alguns elementos fundamentais que

formatam nosso campo jurídico.[242] O primeiro é que existe, no nosso país, uma formulação jurídica tardia, considerando que a disciplina jurídica da proteção de dados pessoais possui mais de cinquenta anos de experiência (Doneda & Zanatta, 2022). Tal formulação jurídica tardia apresenta uma interessante oportunidade no Brasil. Não há intenções de repetir erros do passado, como um enfoque excessivo nas regras de licenciamento de bancos de dados ou uma abordagem de *Datenschutz*, centralizada no "dado em si". Considerando os grandes saltos teóricos e as múltiplas "gerações de leis de proteção de dados" – um conceito amplamente debatido por autores como Danilo Doneda e Laura Schertel Mendes em seus trabalhos –, já existe uma acomodação a uma teoria robusta dos direitos da personalidade e o desenvolvimento de conceitos jurídicos cruciais, como a "autodeterminação informativa" (Menke, 2015; Schertel Mendes, 2020), uma ideia derivada da teoria constitucional do direito alemão.

A "autodeterminação informativa" é mais complexa do que parece ser. Uma explicação simplista é que ela se equivale ao controle individual sobre os dados pessoais. Essa concepção me parece fundamentalmente datada e falha. Ela faz sentido como uma aproximação das teorias de Alan Westin na década de 1960. No entanto, a década de 1980 permitiu uma formulação do conceito de "autodeterminação informativa" como uma barreira normativa intrinsicamente conectada com uma teoria democrática (Schertel Mendes, 2020). Conforme argumentado por Giovanni Sartor, no momento em que o Tribunal Constitucional Alemão formulou o conceito de "autodeterminação informativa" (*informationelle Selbstbestimmung*) no famoso caso do Censo de 1983, ele o fez a partir de uma concepção democrática sobre em que situações o consentimento dos cidadãos seria dispensável em razão uma política pública justa e necessária, como a execução do Censo.[243] Sendo uma decorrência do dever de promoção da

[242] Não detalharei a teoria do "campo jurídico", mas assumo como premissa teórica a formulação de Bourdieau (1986).

[243] "Restrições a esse direito à 'autodeterminação informativa' são permitidas somente se servirem a um interesse público primordial. Elas exigem uma base estatutária que deve ser constitucional e deve satisfazer o requisito de clareza jurídica sob o império da lei. No design da estrutura estatutária, o legislador deve, além disso, observar o princípio da proporcionalidade. Ele também deve prever salvaguardas organizacionais e processuais que combatam o risco de violação do direito geral de personalidade". BVerfG, BvR 209/83.

dignidade humana e o dever de proteção do livre desenvolvimento da personalidade, a autodeterminação informativa seria uma barreira normativa para garantia de "democraticidade", nos termos de Sartor (1986). É um princípio derivado dos direitos da personalidade que se personifica na imposição de limites, barreiras, procedimentos no momento de habilitar o fluxo de dados para causas justas. O princípio foi erigido para legitimar a imposição de "salvaguardas procedimentais adicionais" e não impedir a realização do Censo.

Quando a Lei Geral de Proteção de Dados Pessoais inclui a "autodeterminação informativa" como fundamento de todo o regime jurídico de proteção de dados, ela sinaliza algo muito importante: uma tradição constitucional de deveres estatais de promoção de direitos que se cristaliza no constante exercício de respeito à dignidade dos cidadãos, em razão do reconhecimento da existência de algo como a "autodeterminação informativa". Isso foi possível pois já havia uma doutrina jurídica relativamente bem consolidada, ao menos na Europa continental, sobre o significado da autodeterminação informativa dentro de uma tradição de direitos sobre livre desenvolvimento da personalidade (Schertel Mendes, 2020).[244] É essa concepção que é adotada pelo ministro Gilmar Mendes em seus votos sobre a natureza do direito à proteção de dados pessoais no Brasil, em especial o *leading case* da ADI 6387.

Como mostrado por diversos autores brasileiros, essa acomodação tardia da proteção de dados pessoais possui pontos de vantagem específicos, como uma conexão mais intrínseca a uma tradição de interpretação constitucional do direito civil. A jurista Laura Schertel Mendes (2014), por exemplo, argumentou como a teoria jurídica do direito do consumidor e seus institutos do direito econômico-constitucional produzem uma concepção da proteção de dados pessoais mais afeita ao reconhecimento do princípio da vulnerabilidade das pessoas, das obrigações positivas do Estado na promoção de direitos (o que se traduz em condutas e procedimentos que devem ser colocadas em marcha pelo Estado) e de

[244] Nos EUA, as noções filosóficas sobre autodeterminação concentram-se mais na ideia de liberdade e florescimento individual (Allen, 2003).

uma concepção desses direitos que é tanto "subjetiva" (relacionada aos direitos de controle sobre os dados) quanto "objetiva" (a proteção que o consumidor pode esperar por parte do poder público diante de situações opressivas com relação aos seus dados). Há, inclusive, muitos julgados do Superior Tribunal de Justiça que evidenciam esse tipo de raciocínio jurídico, como os votos de Ruy Rosado Aguiar da década de 1990 (Doneda & Schertel Mendes, 2013; Cueva, 2017).

Do mesmo modo, o jurista Bruno Bioni (2020) argumentou como os institutos dos direitos da personalidade e da boa-fé objetiva vão permitir uma análise muito mais complexa das relações obrigacionais no direito, permitindo que certos *standards* de conduta sejam avaliados em uma relação dinâmica entre o "titular de dados pessoais" e o "controlador de dados pessoais", ao invés de uma simples concepção estática centrada em elementos transacionais, como Termos de Uso e aceites em Políticas de Privacidade. Essa tradição progressista do direito civil – que encontra forte fundamento na escola gaúcha de direito civil capitaneada por Claudio Covis Couto, Claudia Lima Marques e Paulo de Tarso Sanseverino – permite que diversos princípios da proteção de dados pessoais sejam incorporados no ferramental de análise dos agentes decisórios, a partir de uma concepção do direito obrigacional (Bioni, 2020). Bioni ilustra essa relação obrigacional nos esforços empreendidos pelo controlador para garantir o máximo de transparência nas relações, bem como a utilização de ferramentas de *privacy by design*, que revelam um esforço significativo daquele que trata os dados pessoais para materializar os valores de autonomia e promoção da privacidade no manejo dos dados pessoais.

Os últimos estudos de Danilo Doneda (2022) também mostraram que o direito constitucional brasileiro teria um papel decisivo na acomodação da proteção de dados pessoais, considerando as cláusulas gerais de promoção da dignidade da pessoa humana e os esforços empreendidos pelo Supremo Tribunal Federal na interpretação do "conteúdo" da proteção de dados pessoais em casos como "OAB vs IBGE" (ADI 6387). Nesse caso, em específico, a discussão sobre a existência de um "direito fundamental autônomo" passou ao largo da interpretação específica da Lei Geral de Proteção de Dados Pessoais. O debate

feito pela Corte foi como as cláusulas assecuratórias de liberdades (habeas data) e devido processo previstas na Constituição, em conjunto com o direito de inviolabilidade dos dados, permitiria a compreensão de que, diante dos crescentes riscos associados ao uso indiscriminado de dados pessoais – incluindo dados tidos "triviais", como número de telefone, endereço e nome –, deveria existir uma espécie de "calibragem permanente" entre os mecanismos para diminuir esses riscos em uma dimensão preventiva.

Por fim, como argumentei em diversos outros estudos, a incorporação da proteção de dados pessoais em uma tradição jurídica afeita aos direitos difusos promove uma dupla oportunidade de acesso à justiça. Primeiro, em um plano processual, diante das inúmeras possibilidades trazidas pela ação civil pública e os mecanismos de tutela coletiva (Zanatta, 2019; Zanatta, 2020). Segundo, em um plano material, pela possibilidade de que certos tipos de ilícitos de dados sejam vistos pelas lentes dos "danos sociais" e por violações da ordem extrapatrimonial, cabendo não somente a reparação coletiva mas também o reconhecimento de certos tipos de danos que não são individuais homogêneos (Zanatta, 2023). No Brasil, a proteção de dados pessoais já é percebida com claríssima dimensão coletiva, permitindo que danos e ilícitos sejam emoldurados pelas lentes dos "direitos difusos" e dos "danos sociais". Autores como Pedro Bastos (2022) e Diego Machado (2023) também possuem formulações teóricas nesse sentido.

A proteção de dados pessoais no Brasil, portanto, compreende as práticas interpretativas da Constituição Federal e das diversas normas infraconstitucionais sobre o tema – como o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. O nascimento deste campo normativo se dá em um contexto de forte aplicação da teoria dos direitos fundamentais, de intervenção jurídica nas relações privadas, de centralidade da proteção da "pessoa humana" e adoção de teorias fortes sobre justiça social e acesso à justiça (Doneda & Zanatta, 2022). É nessa relação entre Constituição e normas infraconstitucionais que se busca uma

certa "unidade do ordenamento jurídico" no sentido de busca pelo "valor fundamental" da "dignidade da pessoa humana" (Doneda, 2006).

2. A compreensão da proteção de dados em seu caráter dinâmico e complexo

Um segundo elemento fundamental a ser compreendido é o caráter dinâmico e complexo do direito da proteção de dados pessoais. Trata-se de uma discussão teórica que independente de regimes jurídicos nacionais, seja ele o alemão ou o brasileiro. O debate sobre a "natureza complexa" da proteção de dados pessoais possui um regime de abstração maior.

No sentido dado pela filósofa do direito Mireille Hildebrant (2021), a proteção de dados pessoais pode ser concebida como um "artefato histórico" (Hildebrandt, 2011), cristalizado em uma produção normativa específica, textual, que produz um conjunto de normatividades dentro do sistema jurídico de uma comunidade política. Como ela sustenta em seu singelo livro *Law for Computer Scientists and Other Folks*, o direito da proteção de dados pessoais diz respeito a todo um conjunto de normas jurídicas, princípios, leis, acordos internacionais e posições doutrinárias interpretativas sobre os direitos fundamentais que pessoas possuem com relação ao fluxo de seus próprios dados (Hildebrandt, 2019). Tais normas estão intimamente relacionadas a teorias liberais sobre Estado de Direito e direitos fundamentais, porém são suscetíveis a variações significativas de concepções políticas, filosóficas e jurídicas.

Classicamente, as teorias liberais de fundo possuem relação com duas matrizes de pensamento ocidental no plano filosófico. Primeiro, as ideais de John Stuart Mill de um direito ao florescimento pessoal e autonomia individual. A garantia da privacidade informacional permite que uma pessoa seja menos suscetível ao controle de outros, fazendo com que suas liberdades civis possam ser exercidas a partir de uma noção específica de autonomia (Cohen, 2013). Segundo, as ideias de John Locke sobre características específicas de uma certa propriedade atribuída às pessoas, no sentido de domínio sobre recursos materiais e imateriais, e uma capacidade de repelir a intervenção estatal que

possam minar esse controle individual sobre um recurso.[245] Essas concepções são notáveis na noção de "direitos inalienáveis" de vida e de propriedade em declarações de direitos do século XVIII (Richardson, 2016).

Como observado por filósofos da privacidade, as teorias kantianas sobre dignidade da pessoa humana e sua não instrumentalização são bastante influentes no surgimento de teorias sobre "direitos da personalidade" do início do século XX e fundamentos filosóficos que dizem respeito a um tratamento digno, concebendo a informação como uma espécie de "corpo eletrônico" e um habilitador de liberdades e reconhecimento em uma comunidade política. Nos EUA, essa concepção kantiana da privacidade ganhou destaque na década de 1960 e auxiliou na desmobilização de uma noção puramente defensiva, como se a privacidade fosse o mero domínio exclusivo sobre um recurso informacional ou um direito defensivo de impedimento do acesso dos outros.[246] A proteção de dados pessoais não se fundamenta na ideia de privacidade enquanto solitude, reserva e sigilo. Na esteira do pensamento de Alan Westin, a ênfase no "controle sobre o fluxo dos dados" está associada a uma concepção liberal de direitos civis e direitos políticos (Doneda, 2006). Em sua origem, a *informational privacy* está muito mais associada às noções de transparência, *accountability* dos controladores de dados, não abusividade no manejo das informações e responsividade diante de solicitações legítimas, como a oposição ao tratamento indevido ou a exclusão de certas informações após um período de tempo.

A ideia de "dignidade da pessoa humana" é um fundamento da noção contemporânea de *informational privacy*. Há, no entanto, diferentes correntes filosóficas sobre dignidade, sendo a posição kantiana a mais famosa: temos uma dignidade especial pois somos seres dotados de racionalidade e capacidade de

[245] Para uma excelente análise sobre individualismo possessivo na teoria da privacidade em John Locke, ver Doneda (2006), argumentando que a "irrupção da privacidade não representa uma continuidade de uma tradição anterior", mas um "modo de reconhecimento da própria individualidade típico da burguesa, que a diferencia do corpo social e a qual é instrumentalizada com um forte componente individualista" (Doneda, 2006, p. 82).

[246] Além da noção kantiana básica de dotação de "intelecto moral e prático", no sentido de "autonomia prática", Danilo Doneda relembra a teoria da prestação de Hasso Hofman sobre a relação dinâmica entre "conquista da dignidade" e "autodeterminação do comportamento", no sentido de construção de identidade (Doneda, 2006).

autodeterminação. Há ainda posições religiosas sobre o caráter único do ser humano em razão de sua aproximação com Deus.[247] No entanto, há posições filosóficas menos antropocêntricas. O filósofo Luciano Floridi, por exemplo, possui uma concepção de dignidade "antropo-ecêntrica", no sentido de que não estamos em posição superior na natureza, mas sim em uma posição inferior. Nossa racionalidade e consciência não seria um estado evolutivo maior, mas um "acidente da natureza", uma possibilidade única de conseguir imaginar, criar mundos, fábulas, crenças e nos mantermos em constante posição de descontentamento e reinvenção (Floridi, 2016). Nossa dignidade seria justificável pelo nosso caráter enquanto "obra aberta" e uma "exceção na natureza" – e não uma posição superior do racionalismo de Immanuel Kant.

Para Stefano Rodotà, nossa concepção de dignidade advém de nossa capacidade de reconhecimento recíproco e nossa solidariedade (Rodotà, 2018). Devemos ser dignos pois aspiramos sermos tratarmos como iguais, como um "comum" (os seres humanos). A dignidade advém de uma concepção de necessidade de apoio mútuo e de respeito, para evitar situações de absoluta indignidade, como são as experiências de trabalho escravo e de extermínio étnico, presentes em muitos momentos da história. A afirmação pós-Guerra da dignidade na Alemanha e na Itália enquanto conceito jurídico advém de uma transformação mais profunda de primazia da "pessoa humana" – o que seria uma nova "antropologia jurídica" no sentido de uma nova forma de enxergar o homem e afirmar a categoria jurídica da dignidade, incluindo nos vínculos sociais constituídos por mediação das tecnologias da informação (Rodotà, 2014).

Como sustentado por Floridi, a proteção da privacidade informacional "deve ser baseada diretamente na proteção da dignidade humana", e não "indiretamente, por meio de outros direitos como o direito de propriedade e o direito de liberdade de expressão" (Floridi, 2016, p. 308). É um tronco primário do direito de dignidade, sustenta Floridi. pois "meus dados" não significa a mesma coisa que "meu" em "meu carro", mas sim "meu" em "meu braço"

[247] Para uma breve análise das críticas de Giorgio del Vecchio sobre as doutrinas cristãs de personalidade e dignidade (a ideia de proximidade com Deus), ver Doneda (2006).

(Floridi, 2016, p. 308) – uma ideia muito próxima do "corpo eletrônico" defendida por Stefano Rodotà (2014). A informação pessoal desempenha um "papel constitutivo do que eu sou e do que posso ser" (Floridi, 2016, p. 308). Floridi argumenta que nossa dignidade reside justamente no caráter "excêntrico" e "desajustado" de sermos humanos, uma "obra rara e improvável da natureza", uma espécie de "obra em progresso" que possui sempre a chance de reinvenção, de reescrita da própria história, de "sermos em muitas formas" (o *polytropon* da Odisséia de Homero).[248]

Como argumentado por Danilo Doneda no seu livro clássico *Da Privacidade à Proteção de Dados Pessoais*, os fundamentos filosóficos da proteção de dados pessoais estão profundamente conectados com noções de democracia, liberdade, igualdade e dignidade (Doneda, 2006). Além disso, como bem argumento por Stefano Rodotà em *Vivere la Democrazia*, o que se pretende atingir com a proteção de dados pessoais é a redução das assimetrias de poder e uma retomada do projeto do *homo dignus*, no sentido de que as pessoas devem ser respeitadas e consideradas agentes autônomos na decisão sobre o fluxo de seus dados, ao invés de uma concepção puramente mercadológica de que as informações são "coisas" ou meros "insumos" (Rodotà, 2018).

Nos EUA, devemos destacar a centralidade das teorias feministas na ressignificação dos conceitos de privacidade, como nos casos que envolviam a liberdade de gestão da privada e usos de anticoncepcionais (Allen, 2003). A criação de categorias jurídicas, como *sexual privacy*, se fundamentam em noções de igualdade e, ao mesmo tempo, de uma espécie de poder de "não divulgação" que é reservado às mulheres. Anita Allen tem argumento como as teorias feministas de não discriminação são centrais na construção de regimes de *informational privacy*, como na vedação de utilização de informações específicas em relações jurídicas (Allen, 2003). Um exemplo notório é o elemento de justiça introduzido em legislações como o *Fair Credit Reporting Act* que impede que

[248] Floridi analisa a importância do conceito de *polytropon* no grego antigo e no verso inaugural da Odisseia do Homero, um dos mais importantes poemas da história ocidental: "fala-me, Musa, do homem versátil que tanto vaguou". Na tradução de Robert Fagles, *polytropon* seria "a man of twists and turns".

informações sobre estado civil e raça possam ser utilizados para discriminação de mulheres no acesso ao crédito.

As normas e princípios da proteção de dados pessoais não possuem caráter estático e fixo. Trata-se de uma velha discussão filosófica no campo: os primeiros filósofos do direito da proteção de dados, como Spiros Simitis e Vittorio Frosini, já reconheciam que tal disciplina jurídica passaria por transformações permanentes. Isso por um duplo motivo. Primeiro, pois as inovações tecnológicas que produzem riscos à autonomia e dignidade produzem capacidades distintas e são sempre imbricadas em transformações tecnológicas constantes – nos tempos de Louis Brandeis os riscos estavam associados à fotografia, filmagem e os grampos; nos tempos de Alan Westin os riscos estavam associados à computação, novas técnicas de gerenciamento de informaações e bancos de dados integrados (*dataveillance*), nos tempos de Mireille Hildebrandt os riscos estão associados à computação ubíqua conectada à Internet e expansão das técnicas de *knowledge discovery in databases*; e assim por diante. Segundo, pois há uma constante expansão de estratégias regulatórias, que passam cada vez mais a um processo de "risquificação", de responsabilidade civil preventiva e de atribuição de obrigações *ex ante* aos controladores de dados pessoais. Por isso, é provável que a proteção de dados pessoais "não morra" em breve. Ela está intimamente relacionada à destruição criativa das inovações tecnológicas, suas *affordances* e nossos pactos sociais.

Como sustenta a filósofa Mireille Hildebrandt, o direito da proteção de dados envolve uma série de requisitos legais para o desenvolvimento e design, para as configurações padrão e para o emprego de arquiteturas computacionais. Mais especificamente, trata-se de um direito que institui um regime de *transparência* que é bastante conectado com os ideais democráticos de Estado de Direito:

> Alguns autores argumentam que, enquanto, por padrão, o direito à privacidade é, antes de tudo, um direito de opacidade, a proteção de dados é um direito de transparência. Como um direito de opacidade, o direito à privacidade visa salvaguardar uma esfera privada para cidadãos individuais, onde eles podem basicamente evitar a interferência de outros, principalmente o estado. Reconhecemos a ideia de que a privacidade é um direito de liberdade, um direito negativo que obriga outros a se absterem de interferir no bem que é protegido.

> Como um direito de transparência, o direito à proteção de dados visa garantir que sempre que dados pessoais forem tratados (o que inclui coleta, acesso, manipulação e qualquer outro uso), tal tratamento deve ser feito de forma transparente, em conformidade com um conjunto de condições que devem garantir um tratamento justo e legal. (...) Embora a proteção de dados seja um direito de transparência que deve permitir que indivíduos e outros atuem em seus dados pessoais (liberdade positiva), ao mesmo tempo em que impõe uma série de obrigações positivas àqueles que determinam a finalidade do processamento, o direito à proteção de dados pode, no entanto, exigir que outros se abstenham de processar dados pessoais, impondo-lhes, assim, obrigações negativas (Hildebrandt, 2019).

O tratamento de dados pessoais tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Doneda, 2022; Doneda & Zanatta, 2022). Por isso, impõe a observância da boa-fé e princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Também institui obrigações específicas (Bioni, 2020). O tratamento de dados pessoais só pode ocorrer se obedecer a hipóteses específicas previstas na legislação (os "requisitos para tratamento de dados pessoais" também chamados de "bases legais" de tratamento de dados). Sem esses requisitos, o tratamento de dados torna-se irregular, produzindo um ilícito – um ato contrário ao direito.

Note-se que a proteção de dados pessoais objetiva a promoção de valores múltiplos, pois isso ela possui um "caráter complexo", nos termos da filósofa Marion Albers. Tome-se como exemplos alguns casos distintos no Brasil, por exemplo. Os direitos de proteção de dados pessoais foram mobilizados em 2018 para impedir que mais de 10 milhões de usuários do metrô de São Paulo tivessem suas informações biométricas identificadas para um sistema de publicidade chamado "Portas Interativas Digitais" (Zanatta, 2023). Aqui neste caso, houve o reconhecimento da inexistência dos elementos básicos de transparência e a abusividade da exploração comercial de informações sensíveis, considerando que a detecção facial envolve a análise de informações biométricas. Mais recentemente, os direitos de proteção de dados pessoais foram mobilizados pelas Defensorias Públicas de São Paulo e da União em uma ação civil pública que objetiva impedir a utilização de sistemas de reconhecimento facial na linha

vermelha, em razão dos efeitos detrimentais produzidos à população negra, que é empiricamente mais suscetível a falhas de acurácia (falsos positivos no processo de *matching*) e violência de forças policiais associadas à interpretação desses dados.[249] Aqui, a proteção de dados pessoais passa a dialogar muito mais com os direitos antidiscriminatórios e as cláusulas constitucionais de igualdade perante a lei.

Essa amplitude de valores normativos – que podem ser orientar ao bem-estar do consumidor de serviços públicos, a maximização da transparência nas relações negociais, a oposição aos efeitos antidiscriminatórios, a garantia do controle individual e coletivo sobre usos justos dos dados – constitui a complexidade da proteção de dados pessoais. Outro elemento crucial é que há uma complexa combinação entre princípios e direitos, que assumem formas variadas entre reivindicações, liberdades, poderes e imunidades. A seguir, exploro o argumento sobre a natureza específica dos *direitos de proteção de dados pessoais* retomando um debate clássico da teoria dos direitos.

3. Os direitos de proteção de dados pessoais: uma análise a partir de Hohfeld

Nesta seção, apresentarei uma síntese da teoria do direito de Wesleu Hohfeld, um autor ainda pouco estudando no direito brasileiro. A partir de sua teoria sobre direitos correlatos (opositores e correlatos jurídicos), abordarei algumas distinções entre "direitos-privilégios" e "direitos-reivindicações" nos direitos de proteção de dados pessoais. Argumentarei que a moldura analítica hohfeldiana pode ser útil para uma elaboração teórica mais sofisticada sobre os direitos subjetivos de proteção de dados pessoais.

3.1. Contornos principais da teoria do direito de Hohfeld

Na tradição da teoria dos direitos formulada no século passado nos EUA, em especial no trabalho de Wesley Hohfeld (1879-1918), encontramos uma teoria analítica dos direitos a partir da concepção de "relações jurais" que possuem uma natureza própria. Para Hohfeld, usamos a expressão *rights* de muitas formas

[249] Para uma análise de diferentes ações civis públicas em proteção de dados, ver Zanatta (2023).

distintas, porém há características próprias nas relações jurídicas. Para Hohfeld, os direitos podem ser desmembrados em oito "componentes atômicos", que são o mínimo denominador comum do direito. Essas concepções jurídicas fundamentais são os conceitos de *right*, *no-right*, *power*, *disability*, *duty*, *priviledge, liabiity* e *immunity* (Cullison, 1967). Esses conceitos sempre descrevem as relações jurídicas entre pessoas com relação a atos.

Esses "incidentes hohfeldianos" possuem uma forma lógica distintiva e eles compõem uma estrutura molecular complexa de direitos. Essas ideias foram desenvolvidas por Hohfeld no influente ensaio *Fundamental legal conceptions as applied in judicial reasoning* (Hohfeld, 1913), publicado enquanto era professor da Universidade de Columbia.[250]

A inovação metodológica de Hohfeld foi pensar que os direitos são sempre exercidos em relações sociais e posições específicas entre as pessoas, ao mesmo tempo que o direito obedece a um conjunto de regras lógicas que são muito próprias (regras lógicas introduzidas pela própria ideia de sistema jurídico e de relações jurídicas no sentido de *rights and duties*). Portanto, um tipo específico de direito só pode ser conceitualizado se forem analisadas as relações condicionantes com uma outra parte e o tipo específico de "direito", com suas regras de opostos jurídicos e correlativos jurídicos (que serão explicadas a seguir). Apesar de pouco disseminada no Brasil – Wesley Hohfled não é um autor tão popular em teoria do direito como Hans Kelsen, Norberto Bobbio ou Herbert Hart –, a teoria de Hohfeld é bastante útil para pensarmos os direitos de proteção de dados pessoais de forma mais analítica.[251] Esse reconhecimento é feito também por autores contemporâneos do direito civil, que analisam as limitações das teorias europeias sobre "pretensão" contraposta a um "dever" no estudo dos direitos. Tal dualismo é distinto da teoria dos direitos subjetivos formulada por Hohfeld:

> Hohfeld delineia os seus conceitos jurídicos fundamentais como forma de demonstrar os usos inadequados do termo *right*, e de alcançar maior precisão nos

[250] Hohfeld faleceu precocemente aos 39 anos de idade.

[251] A minha aproximação com a teoria do direito de Hohfeld ocorreu no curso do professor Talha Syed, da Universidade da Califórnia, que ministrou um curso de teoria do direito de propriedade na Universidade de Turim no período que fui estudante de mestrado em 2015.

> conceitos basilares do Direito. O resultado conquistado por Hohfeld, no alvorecer do século XX, foram oito conceitos jurídicos fundamentais, que podem ser claramente considerados como oito sentidos ou aspectos distintos dos direitos subjetivos. São, em outras palavras, distintas faces que os múltiplos direitos subjetivos concretos podem assumir na perspectiva do titular e do sujeitado, dependendo da situação fática e dos agentes a que se referirem. Harmônicas entre si, formam, conjuntamente, o conceito geral" (Gomes *et al*, 2022, p. 99).

A teoria do direito de Hohfeld busca solucionar ambiguidades no uso da expressão direitos, como nas expressões "direito à terra" ou "direito ao matrimônio". Um dos problemas dessa ambiguidade é que as palavras surgem para descrever relações sociais no mundo real e, posteriormente, passam a ser usadas para descrever relações jurídicas sem uma teoria analítica de qualidade. Hohfeld, nesse sentido, busca superar as teorias de Jeremy Bentham sobre as relações entre direitos e deveres adicionando camadas lógicas adicionais.

A teoria de Hohfeld é sofisticada, pois introduz a relação social como elemento de análise e introduz um rigor lógico sobre a relação entre os incidentes. Ele o faz por meio da introdução dos opositores jurídicos, os *jural opposites*, com quatro regras lógicas:

(i) se A possui um *claim*, então A carece de um *no-claim*;

(ii) se A possui um *privilege*, então A carece de um *duty*;

(iii) se A possui um *power*, então A carece de uma *disability*;

(iv) se A possui uma *immunity*, então A carece de uma *liability*.

Os opostos jurídicos (que são premissas teóricas e conceituais) devem ser vistos ao lado dos "correlativos jurídicos", os *jural correlatives*, também concebidos com quatro regras lógicas que dizem respeito ao modo ocorrem as perspectivas entre as pessoas:

(i) se A possui um *claim-right*, então uma pessoa B possui um *duty*;

(ii) se A possui um *priviledge*, então uma pessoa B possui um *no-claim*;

(iii) se A possui um *power*, então uma pessoa B possui uma *liability*;

(iv) se A possui uma *immunity*, então uma pessoa B possui uma *disability*.

Daniel Brantes Ferreira, em estudo feito pela Pontifícia Universidade Católica do Rio de Janeiro, traduziu o conceito de *claim* de Hohfeld como "pretensão" (prefiro a expressão "reivindicação"[252]). Ao interpretar as regras lógicas de Hohfeld, Brantes defende que "as relações correlatas e opostas devem ser consideradas em um esquema único", assim por ele sistematizado em nossa língua:

Conceitos fundamentais opostos	**Conceitos fundamentais correlatos**
Pretensão [reivindicação] x ausência de pretensão [reivindicação]	Pretensão [reivindicação] e Dever
Privilégio x dever	Liberdade e ausência de pretensão
Poder x incompetência	Poder e sujeição
Imunidade x sujeição	Imunidade e incompetência

Adaptado de Ferreira (2007)

Essas relações são lógicas nas posições jurídicas. Se eu possuo um direito-reivindicação, significa que *careço de uma não-reivindicação*. Se possuo um privilégio, significa que *careço de um dever*. Se possuo um poder, então careço de uma incompetência (a incapacidade de criar). Se possuo uma imunidade, então careço de uma sujeição. Essas regras lógicas básicas servem para identificar as posições fundamentais das relações jurídicas do ponto vista dos opositores, evitando contradições (Ferreira, 2007; Gomes *et al*, 2022).

Enquanto os conceitos fundamentais opostos evitam contradições lógicas na relação do indivíduo com o seu direito, os conceitos fundamentais correlatos analisam as relações sociais que compõem as relações jurídicas. O foco de análise são as relações entre as pessoas. Portanto, se possuo um direito-reivindicação, significa que as outras pessoas possuem um dever com relação a minha pretensão, formando um vínculo obrigacional. Se possuo um poder, significa que careço de uma incompetência (o direito assegura a capacidade de criar ou fazer algo), e, ao mesmo tempo, o direito-poder produz uma sujeição, no sentido de

[252] Utilizarei a expressão "direito-reivindicação" como tradução de *claim-right*.

liability. A outra parte se torna sujeita a essa criação e não pode contestá-la legitimamente, fazendo valer uma pretensão contrária.

3.2. Aplicabilidade da teoria dos direitos de Hohfeld à proteção de dados pessoais

Analisemos mais especificamente as características desses direitos na teoria geral de Hohfeld. Por exemplo, o direito de pegar uma concha na praia é um direito-privilégio, pois não há um dever de pegar a concha estabelecido com nenhuma outra pessoa ou autoridade. Não se viola o direito de outros ao não pegar a concha ("*A has a privilege to φ if and only if A has no duty not to φ*"). O elemento característico do privilégio é a inexistência de deveres, pois, se existir um dever, há uma obrigação, mas não um privilégio no sentido de Hohfeld.[253] Por exemplo, o direito de exibição de suas próprias informações pessoais em uma plataforma como X ou Instagram é um direito-privilégio, pois não há nenhum tipo de dever estabelecido com relação àquela conduta. Se um direito-privilégio é reconhecido, então as pessoas passam a possui uma "não-reivindicação". Ninguém "teria o direito" de exigir que uma pessoa deixasse de exibir suas informações pessoais no X ou no Instagram. O mesmo não pode ser dito com relação ao direito de um registro civil no período de nascimento. Não se trata de um direito-privilégio, nos termos de Hohfeld, mas de uma obrigação civil, pois existe um dever imposto pela legislação. Há uma norma jurídica que diz que os pais devem registrar o nascimento dos filhos no registro civil.

[253] O conceito de dever (*duty*) em Hohfeld é bastante específico. Como explica um intérprete: "Os deveres hohfeldianos sempre envolvem duas pessoas, uma que se diz ter ou dever o dever, e outra a quem se diz que o dever é devido. Assim, A pode dever um dever hohfeldiano a B, mas ele não pode dever tal dever a si mesmo, e A pode dever dois deveres separados a B e C, mas ele não pode dever o mesmo dever a ambos. A razão para esse uso fica clara quando se lembra que (1) um dever hohfeldiano de fazer algo surge quando a lei positiva tornaria uma pessoa civilmente responsável por não fazê-lo, e (2) Hohfeld estava tentando reduzir a conceitualização legal aos seus menores denominadores comuns. Se sob as regras da lei A seria responsável a B por não fazer algo, então A deve um dever especificamente a B de fazê-lo. Quando as regras da lei tornariam A responsável a B e C por não fazer algo, Hohfeld preferiu dizer que A deve deveres separados a B e C, uma vez que sua responsabilidade para com eles em caso de violação seria separável. Suas causas de ação seriam independentes umas das outras, então os deveres de A (se eles devem ser "menores denominadores comuns") também devem ser independentes uns dos outros" (Cullister, 1967, p. 563).

Não há, por exemplo, um "direito-privilégio" de bater nos próprios filhos a seu bel prazer ou suas próprias convicções sobre educação e violência. Há deveres legais reconhecidos no direito com relação à educação adequada dos filhos e há normas específicas que proíbem a violência doméstica contra crianças. Nesse sentido, é ilógico afirmar que se trata de um "direito-privilégio" e uma liberdade fundamental. Um "direito-privilégio" deve produzir, necessariamente, a ausência de reivindicações por outros. No caso dos pais que batem nos filhos, há plenas possibilidades jurídicas de que o Conselho Tutelar reivindique a perda do poder familiar e a transferência das crianças para um ambiente seguro, por exemplo.

Hohfeld também diferencia os incidentes do direito-reivindicação. Um contrato entre empregador e empregado confere ao empregado o direito de ser pago, no sentido de um *claim-right*. A reinvindicação produz o dever do empregado de pagar. Esse direito-reivindicação envolve necessariamente um dever acoplado ("*A has a claim that B φ if and only if B has a duty to A to φ*"). A reinvindicação exige uma relação prévia e uma noção obrigacional, como nos casos de deveres de transparência. Portanto, uma solicitação de exclusão de seus dados pessoais de uma plataforma está associada a um dever de realizar aquela conduta. Esse tipo de direito se configura como um "direito-reivindicação" pois há relações jurídicas de caráter obrigacional e vinculativos.

Ao analisar as contribuições de Hohfeld, Cullison (1967) argumenta que a clareza sobre a identificação das relações jurídicas (direito-reivindicação ou direito-privilégio) permite definir claramente a existência ou não de deveres e obrigações:

> Os *rights, duties, priviledges e no-rights* de Hohfeld são simplesmente termos abreviados para dizer quais responsabilidades a lei prescreve entre duas pessoas para fazer ou não fazer um ato. Quando A falha em fazer um certo ato, a lei o tornará responsável perante B por isso ou não. Ele não pode ser responsável e não responsável perante B, mas ele deve ser um ou outro. Se ele seria responsável por não fazer o ato, dizemos que ele deve a B um "dever" de fazê-lo (uma relação direito-dever); mas se ele não seria responsável perante B por não fazê-lo, dizemos que ele tem um "privilégio" em relação a B de não fazê-lo (uma relação privilégio-não-direito). Como A seria responsável ou não responsável, um ou outro, mas não ambos, é claro que A tem o dever de fazer ou o privilégio de não fazer o ato, um ou outro, mas não ambos. Da mesma forma, a lei pode predicar a responsabilidade sobre A fazer o ato (Cullison, 1967, p. 565).

A LGPD estipula que "o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição", o "acesso aos dados" (art. 18, II). Esse direito é qualificado pelo princípio do livre acesso (garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais). Nesse sentido, o "direito-reivindicação" do art. 18, II, da LGPD produz um dever perante o controlador no sentido de provê-lo. O provimento de informações que não sejam integrais produz um ato contrário ao direito, bem como a tentativa de imposição de obstáculos ao exercício desse direito-reivindicação, como a imposição de formulários, assinaturas em documentos físicos, reconhecimento facial mandatório e outras medidas inadequadas.

A inexistência de cumprimento de um dever faz surgir uma violação do direito e uma pretensão de reparação? Sim, conforme os precedentes do Superior Tribunal de Justiça sobre ilícitos de dados, essa situação pode ocorrer. No caso HSBC, julgado pelo STJ em 2017, o banco entendia que possui uma "direito-privilégio" sobre o fluxo dos dados dos seus clientes, podendo livremente transferi-los para operadoras de cartão de crédito. O STJ decidiu que esse "direito-privilégio" inexiste. As partes estão em uma relação obrigacional e existem direitos básicos dos consumidores sobre seus próprios dados. O "direito-reivindicação" significa que o consumidor pode reivindicar que sejam prestadas informações claras sobre as intenções do uso dos dados, as informações sobre as razões econômicas desses dados e a capacidade de bloquear e não consentir com o uso desses dados. Partindo da ideia de "direitos correlatos" desenvolvida por Antonio Herman Benjamin em sua interpretação do Código de Defesa do Consumidor, o STJ entendeu que existem deveres associados aos direitos dos consumidores sobre os dados. Esses deveres associados seriam a maximização da transparência e a garantir de um consentimento livre e informado, capaz de nutrir a boa-fé objetiva e as relações de confiança entre as partes. Justamente por

ter violado um conjunto de deveres associados ao tratamento de dados, faz nascer a pretensão de reparação.

Note-se que, no direito civil brasileiro, a ideia de "direitos correlatos" é plenamente aceita e utilizada por juristas como Claudia Lima Marques, Paulo de Tarso Sanseverino, Antonio Herman Benjamin e muitos outros. Conforme já teorizado por Herman Benjamin com relação ao Código de Defesa do Consumidor, a estrutura do art. 43 produz não somente um conjunto de direitos subjetivos com relação aos dados pessoais – como o direito de ser informado após a constituição de um cadastro de consumidores, o direito de modificação de uma informação pessoal imprecisa ou o direito de ter uma limitação temporal sobre o uso dos dados pelos birôs de crédito –, mas também produz um conjunto de obrigações e deveres aos agentes econômicos. O "ato do arquivamento", segundo o ministro Benjamin, implica direitos correlatos de "respeito à finalidade notocioso-prospectiva dos arquivos" e manutenção de "informações adequadas" (Benjamin, 2019, p. 623). O descumprimento desses deveres produz o ilícito, cabendo a reparação.

Já o direito-poder (*power*) é o incidente que habilita mudar as regras, como o direito do capitão de impor um novo dever a um marujo no curso da navegação. Essa capacidade de impor novos deveres anula privilégios ou outros incidentes ("*A has a power if and only if A has the ability to alter her own or another's incidents*"). Atualmente, no direito contemporâneo, é admitido que uma empresa possa mudar constantemente as normas associadas ao tratamento de dados pessoais por meio das Políticas de Privacidade. Em termos hohfeldianos, empresas como Microsoft, Meta e Google possuem um certo "direito-poder" em razão da capacidade de modificação dos incidentes dos outros. Mas seria justo qualificar tal prática como um "direito-poder"?

Por exemplo, a Meta anunciou em 2024 sua intenção de utilizar os dados pessoais dos usuários do Instagram para treinamento de seus sistemas de inteligência artificial. Para tanto, a Meta se arrogou em um "direito-poder". A empresa acredita que possui a capacidade de modificação dos incidentes das pessoas (é um poder que determina quais são as liberdades e as reivindicações

possíveis). A empresa acredita que possui o direito de determinar que a base legal de tratamento de dados é o legítimo interesse e que as pessoas que discordarem poderão exercer uma solicitação de oposição ao tratamento de dados pessoais (o direito de oposição previsto no §2º do art. 18 da LGPD). Nesse sentido, o "direito-poder" modifica as condições pelas quais um "direito-reivindicação" poderia ocorrer.

Atualmente, um dos grandes debates jurídicos no campo da proteção de dados pessoais é determinar se empresas como X, Meta e LinkedIn podem utilizar os dados pessoais dos usuários de suas plataformas para treinamento de sistemas de IA. O debate tem girado em torno de discussões sobre a viabilidade do legítimo interesse como uma base legal adequada, considerando que o direito impõe uma série de obrigações como produção de um "teste de legítimo de interesse" e a ponderação sobre liberdades e direitos fundamentais dos titulares que podem se sobrepor aos interesses corporativos. Trata-se de uma discussão tecnocrata pouco útil. Uma das formas de dissolver esse impasse é reconhecer que as empresas não possuem tal "direito-poder", pois isso implicaria na modificação das condições de fruições de direitos e das condições de liberdade e de direitos-reivindicações. Considerando as finalidades originárias do tratamento de dados pessoais e o fundamento da autodeterminação informativa, reconhecer esse "direito-poder" implicaria em reduzir as condições de dignidade das pessoas, tornando-as meras "turbinas de produção de dados" em sistemas comodificados. Como dito anteriormente, a tradição filosófica da proteção de dados pessoais impede este grau extremo de transformação dos nossos corpos eletrônicos em meras commodities (Floridi, 2016; Rodotà, 2016).

Por fim, o "direito-imunidade" (*immunity*) formulado por Hohfeld ocorre quando um agente não possue a habilidade de modificar incidentes de outrém, gerando uma imunidade e pressupondo uma ausência de habilidade de alteração de incidentes, nos termos hohfeldianos ("*B has an immunity if and only if A lacks the ability to alter B's incidents*"). Logicamente, a imunidade pressupõe a carência de obrigação (*liability*). Com relação aos outros, a imunidade significa que, com relação a uma pessoa A, a pessoa B é incompetente para qualquer tipo de criação

de regras que objetivem modificar as fruições de liberdades e de deveres. Nesse sentido, os direitos de imunidade estão em uma categoria de segunda ordem – pressupõem a distinção básica entre regras primárias e regras secundárias da teoria institucional, adotadas por teóricos tão distintos como Herbert Hart e Elinor Ostrom.[254]

Exemplificando, o Congresso não possui a habilidade (ou a competência) de impor ao cidadão o dever de ajoelhar diante da cruz. Considerando a *ausência de poder*, o cidadão possui a imunidade (a imunidade do sujeito A implica a *ausência de sujeição* no sentido opositor, e também implica que o outro possui a *ausência de poder*, no sentido correlativo). Analisando o mesmo exemplo da Meta e as mudanças das Políticas de Privacidade, se tivéssemos regras mais rigorosas sobre a impossibilidade de modificação desses incidentes, poderíamos dizer que as pessoas possuem um "direito-imunidade" se assumirmos que a Meta não possui a habilidade de alterar os incidentes das pessoas.

Esses incidentes atomizados podem ser reunidos para formar "direitos complexos", com direitos de "primeira ordem" (relacionados ao objeto) e direitos de "segunda ordem" (direitos sobre os direitos de primeira ordem). Por exemplo, o "direito de propriedade" seria molecular e complexo, envolvendo diversas relações de interdependência, pois envolveria o privilégio de usar um computador (há uma liberdade de utilização) e um direito-reivindicação (*claim-right*) contra outros utilizarem o computador, o que produz um dever, para os outros, de não utilizarem este computador (um direito exigível). Ao mesmo tempo, envolveria um direito-poder (*power*) de anular ou transferir um direito-reivindicação (*claim-right*), como nas situações de formulação de contratos de licenciamento do uso legítimo de um computador dentro de determinadas condições (uma determinação de que o computador só pode ser utilizado nos finais de semana por um período máximo de oito horas). Envolveria também a *immunity* contra outros de alterar o *claim-right*.

[254] Por caminhos distintos, tanto Herbert Hart (filósofo do direito) quanto Elinor Ostrom (prêmio Nobel de economia) irão elaborar distinções fundamentais entre normas primárias (aqueles que prescrevem um comportamento, uma conduta ou uma ação) das normas secundárias (aquelas normas que são capazes de modificar normas primárias).

Os "direitos de segunda ordem" possuem uma característica distintiva. Hohfeld concebe o direito (*right*) no "sentido restrito de pretensão, juridicamente protegida, a uma conduta a que outrem esteja adstrito" (Rego, 2008), sempre a partir das relações jurídicas e a dinâmica entre opostos e correlativos. Conforme explicado por William Edmunson em *An Introduction to Rights*, Hohfeld desejava superar a análise de Jeremy Bentham sobre a relação entre *legal rights* e *legal duties*, no sentido de correlações ("to say that someone had a right of certain kind was simply to say that he stood to benefit from a legal duty imposed on someone else"). Ele acreditava que havia identificado as "relações jurídicas fundamentais, e que todas as outras relações jurídicas poderiam ser analisadas por meio desses elementos fundamentais" (Edmundson, 2012, p. 91).

Conclusão

Em termos analíticos, e de forma muito abrangente em Teoria do Direito, podemos diferenciar a "proteção de dados pessoais" do "direito da proteção de dados pessoais" e os "direitos de proteção de dados pessoais". Nesses dois últimos, há complexidades distintas que podem ser desmembradas. Grande parte da teoria do direito tem se dedicado à explorar a complexidade do *data protection law*, em especial a diferencial do direito da privacidade (*privacy law*). Como visto neste texto, há uma farta literatura que explora a natureza autônoma do direito de proteção de dados pessoais e sua natureza multifacetada em comunidades políticas democráticas.

Além da complexidade no sentido dado por Marion Albers, no sentido de uma multiplicidade de valores normativos e funções da proteção de dados pessoais, poderíamos dizer que a proteção de dados pessoais possui uma complexidade específica com relação ao exercício *dos direitos*, seguindo a teoria analítica de Hohfeld (com uma ênfase a uma teoria dos direitos no sentido de uma *theory of rights*). A titularidade sobre os dados pessoais prevista no art. 17 da LGPD é um direito-privilégio no sentido dado por Hohfeld. As pessoas possuem liberdades e não estão sujeitas a um dever perante outros quando estão em situações de exercício e controle dos seus dados. Elas podem, por exemplo, criar

contas no Instagram e X e livremente disporem da exposição de suas informações pessoais pois não há um dever com relação a outros. Os direitos previstos no art. 18 da LGPD são exemplos claros de "direitos-reivindicações" que criam direitos correlatos. Ao passo que uma pessoa possui o direito de obtenção de informações claras e precisas sobre as finalidades do tratamento de dados pessoais e a garantia de que os dados sejam utilizados de forma leal, seguindo o princípio da minimização, entre outros.

Atualmente, há grandes impasses interpretativos na intersecção entre proteção de dados pessoais e sistemas de inteligência artificial em razão de falhas interpretativas sobre os limites das liberdades corporativas e uma concepção de direitos que se aproximam da ideia de "direitos-privilégio" no sentido hohfeldiano. Se formos capazes de desmembrar as relações jurídicas fundamentais, encontraremos uma rica discussão sobre opostos jurídicos e correlatos jurídicos aplicáveis à proteção de dados pessoais. Essa diferenciação nos ajuda a pensar nas relações entre reivindicação (pretensão jurídica), dever, poder e imunidade; bem como nos ajuda a delimitar melhor as capacidades de modificação dos incidentes de reivindicação e privilégio quando há "direitos-poder" e "direitos-imunidade". Alguns problemas que se apresentam hoje, como a utilização de dados pessoais para treinamento de sistemas de IA à revelia dos princípios de autodeterminação informativa e consentimento livre e informado, parecem estar relacionados a uma teoria implícita de "direitos-privilégio" que precisa ser modificada, se o objetivo final do direito da proteção de dados é a garantia do direito fundamental ao livre desenvolvimento da personalidade e a redução das assimetrias de poder.

Referências

ALBERS, Marion. Realizing the complexity of data protection. In: **Reloading data protection: Multidisciplinary insights and contemporary challenges**. Dordrecht: Springer Netherlands, 2013. p. 213-235.

ALBERS, Marion; SARLET, Ingo Wolfgang. Personality and Data Protection Rights on the Internet: Introduction. In: **Personality and Data Protection Rights**

on the Internet: Brazilian and German Approaches. Cham: Springer International Publishing, 2022. p. 1-16.

ALLEN, Anita. **Why Privacy Isn't Everything: feminist reflections on personal accountability**. Maryland: Rowman & Littlefield Publishers, 2003.

BENJAMIN, Antonio Herman. Comentários ao art. 43. In: GRINOVER, A. P. (org.). **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto**. Rio de Janeiro: Forense, 2019. p. 556-658.

BIONI, Bruno**. Proteção de dados pessoais: as funções e os limites do consentimento**. Rio de Janeiro: Forense, 2020.

BOURDIEU, Pierre. The force of law: Toward a sociology of the juridical field. **Hastings Law Journal**, v. 38, p. 805, 1986.

COHEN, Julie. What Privacy is For. **Harvard Law Review**, Cambridge, v. 126, n. 7, p. 1904-1933, 2013.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, v. 13, n. 4, p. 59-67, 2017.

CULLISON, Alan D. A Review of Hohfeld's Fundamental Legal Concepts. **Cleveland-Marshall Law Review**, v. 16, p. 559, 1967.

DONEDA, Danilo; SCHERTEL MENDES, Laura. Data protection in Brazil: new developments and current challenges. In: **Reloading data protection: multidisciplinary insights and contemporary challenges**. Dordrecht: Springer Netherlands, 2013. p. 3-20.

DONEDA, Danilo; ZANATTA, Rafael A. F. Personality rights in Brazilian data protection law: a historical perspective. In: ALBERS, M.; SARLET, I. **Personality and Data Protection Rights on the Internet**. Cham: Springer, 2022. p. 35-53.

EDMUNDSON, William A. **An Introduction to Rights**. Cambridge: Cambridge University Press, 2012.

GOMES, Marcella; SANTOS, Igor; FONSECA, João. A evolução histórica das teorias do direito subjetivo e a contribuição de Hohfeld. **Revista de Direito Civil Contemporâneo** , [S. l.], v. 30, n. 9, p. 55–103, 2022. Disponível em: https://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/1052

.

FERREIRA, Daniel Brantes. Wesley Newcomb Hohfeld e os conceitos fundamentais do Direito. **Revista Direito, Estado e Sociedade**, n. 31, 2007.

FLORIDI, Luciano. Open data, data protection, and group privacy. **Philosophy & Technology,** Oxford, v. 27, n. 1, p. 1-3, 2014.

FLORIDI, Luciano. On human dignity as a foundation for the right to privacy. **Philosophy & Technology**, v. 29, p. 307-312, 2016.

HILDEBRANDT, Mireille. Defining Profiling: a new type of knowledge? In: HILDEBRANDT, M (org). **Profiling the European Citizen**. Dordrecht: Springer, 2008. p. 42-70.

HILDEBRANDT, Mireille. Legal protection by design: Objections and refutations. **Legisprudence**, v. 5, n. 2, p. 223-248, 2011.

HILDEBRANDT, Mireille. The adaptive nature of text-driven law. **Journal of Cross-disciplinary Research in Computational Law**, v. 1, n. 1, 2021.

HOHFELD, Wesley. Some Fundamental Legal Conceptions as Applied in Judicial Reasoning, **Yale Law Journal**, n. 16, b. 23, 1913.

RICHARDSON, Janice. **Law and the Philosophy of Privacy**. New York: Routledge, 2015.

MACCORMICK, Neil. **Rhetoric and the rule of law: a theory of legal reasoning**. Oxford: Oxford University Press, 2005.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In:* FERREIRA MENDES, G.; SARLET, I. W.; COELHO, A. Z. **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 205-230.

RODOTÀ, Stefano. **Il Mondo nella Rete: quali i diritti, quali i vincoli**. Roma: Laterza, 2014.

RODOTÀ, Stefano. **Vivere la Democrazia**. Roma: Laterza, 2018.

ROUVROY, Antoinette. Homo juridicus est-il soluble dans les données? In: TERWANGNE, C.; DEGRAVE, E.; DUSOLLIER, S. **Droit, normes et libertés dans le cybermonde**. Bruxelas: Larcier, 2018. p. 417-444.

ROUVROY, Antoinette. Governamentalidade algorítmica e a morte da política. **Revista de Filosofia Moderna e Contemporânea**, Brasília, v. 8, n. 3, p. 2-20, 2020.

SARTOR, Giovanni. La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del'Datenschutz'. **Informativa e Diritto**, Florença, v. 12, n. 3, p. 95-118, 1986.

SCHERTEL MENDES, Laura. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

SCHERTEL MENDES, Laura. Autodeterminação informativa: história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, 2020.

ZANATTA, Rafael A. F. **A proteção coletiva dos dados pessoais no Brasil:** vetores de interpretação. Belo Horizonte: Letramento, 2023.

10. Privacidade e proteção de dados na academia: considerações sobre a cooperação Google Workspace for Education – USP

Raphael Marques de Barros[255]

> If postal workers read our letters in the way that Gmail and third-party app developers have scanned our emails, they would go to jail. (VELIZ, 2022, p. 57)

Introdução

A proteção de dados pessoais tornou-se uma das questões centrais no debate sobre o impacto das tecnologias digitais na sociedade contemporânea. Desde o escândalo da Cambridge Analytica em 2016 até o crescente uso de dados pessoais em ferramentas educacionais, como o Google Workspace for Education ("GWFE"), emergem preocupações éticas, legais e técnicas sobre os limites da coleta e do tratamento de dados.

Discussões acerca da proteção a dados pessoais são parte importante do debate sobre o papel desempenhado por empresas de tecnologia ao redor do mundo. De escândalos eleitorais sobre *fake news* e utilização indevida de dados de redes sociais ao rastreamento de geolocalização durante a pandemia de Covid-19, tal debate nunca esteve tão presente no cenário político-social. Sua expressão jurídica se deu na promulgação de regulações como a *General Data Protection Regulation* europeia ("GDPR") em 2016 e de sua análoga brasileira, a Lei Geral de Proteção de Dados ("LGPD") em 2018.

Assim, tais discussões, permeando todas as esferas sociais, penetram também no ambiente educacional. Na última década, inovações em poder

[255] Bacharel e Mestrando pela Faculdade de Direito da Universidade de São Paulo.

computacional e coleta de dados permitiram a inserção em massa de tecnologias de processamento e armazenamento de dados aplicadas ao ambiente estudantil. Dentre estas inovações ofertadas está o Google Workspace ("Workspace").

De início, o Workspace é uma plataforma de serviços de produtividade *online* ofertada pelo Google. Além do Gmail, tal plataforma inclui serviços de processamento de texto, planilhas, apresentações de slides, anotações, formulários, montagem de websites, canvas colaborativo, agenda, serviços de videoconferência, armazenagem de dados.

Dado o panorama acima, cumpre afirmar: o Gmail é uma plataforma monumental e talvez o principal serviço ofertado pelo Google[256] no âmbito do Workspace. Com mais de 1,8 bilhões de usuários em 2020,[257] hospeda quase 40% dos usuários de *e-mail* no mundo. Dentre estes usuários estão diversos clientes corporativos, entidades educacionais e de pesquisa, pequenas empresas e pessoas físicas. Sem contar as demais empreitadas do Google, a utilização de contas Gmail é grande parte de seus serviços ofertados, para além, obviamente, de sua *search engine* homônima, absolutamente dominante em seu respectivo mercado.

O Google também possui planos do Workspace voltados especificamente a instituições de educação, o GWFE. Tais planos, além de incluir todos os serviços ofertados para as edições do Workspace, ainda possui ferramentas para a simulação de atividades em salas de aula e envio de tarefas.

Todos esses serviços são oferecidos de forma gratuita a partir da criação de uma conta Google, mas possuem versões pagas por meio de assinaturas institucionais (a princípio voltadas a empresas) do serviço Google Workspace.

Assim, dada a quantidade de recursos oferecidos e os baixos custos envolvidos para a assinatura de tais serviços (considerando que alguns seriam "de graça"), é compreensível a adoção em massa desta plataforma por entidades

[256] A expressão "Google" se referirá ao próprio Google LLC., empresa responsável pela oferta dos serviços mencionados no presente trabalho, mas abrangerá a Alphabet, Inc., entidade sucessora do Google e sociedade-mãe das entidades do grupo econômico Alphabet/Google, bem como outras entidades do grupo quando oportuno.
[257] PETROVA, 2019 e GILBERT, 2020.

educacionais mundo afora. Entretanto, o poderio destes serviços por si só não serve como fundamento único de sua adoção em massa. Tal adoção encontra-se ancorada também em um ambiente de crescente terceirização e privatização de serviços "não essenciais" em universidades (MONTEIRO, 2020), com uma procura por redução de custos e busca por "eficiências" na esfera acadêmica.

No entanto, o avanço acelerado de tecnologias baseadas em inteligência artificial ("IA") apresenta novos desafios a essas estruturas legais, especialmente quando dados pessoais, como os coletados em ambientes educacionais, são potencialmente utilizados para treinar modelos de aprendizado de máquina.

Este artigo tem como objetivo analisar, a partir do estudo de caso da relação Google-USP, os impactos da coleta e do uso de dados pessoais no ambiente acadêmico, expandindo a discussão para o uso desses dados no treinamento de ferramentas de IA. Por meio de uma abordagem crítica e interdisciplinar, são discutidos os limites éticos e legais impostos pela LGPD, bem como as implicações práticas para a privacidade dos titulares. O principal objetivo aqui é servir de trampolim, impulsionando problemas para análises futuras e mais profundas.

1. Quadro teórico e jurídico

Nesta seção, conectaremos os fundamentos apresentados no seu TCC com as novas questões relacionadas ao uso de dados em IA, mantendo a relevância da LGPD e da autodeterminação informativa.

Assim, iniciamos aqui propriamente primeira parte de nosso trabalho, a nossa análise acerca da relação jurídica que justifica o tratamento de dados a ser realizado dentro das relações que são objeto do presente trabalho. Tal análise será feita de forma a compreender a cadeia de relações entre os usuários finais, a USP e o Google, abarcando documentos e regulações que explicitem tal encadeamento.

Nesse sentido, a subsunção de normas atuais de proteção de dados à relação de tratamento de dados aqui analisada se inicia a partir de uma análise dual: primeiramente analisaremos (a) o atual quadro normativo brasileiro quanto

à regulação da proteção de dados, realizada primariamente pela LGPD, para então nos atermos aos (b) instrumentos documentais e contratuais que fundamentam a relação para o tratamento de dados no âmbito da relação Google-USP. Tais análises evidenciarão quais dados são tratados por essa relação e quais são as principais características deste tratamento.

1.1. Privacidade e proteção de dados

A introdução da LGPD trouxe princípios e normas que orientam o tratamento ético e legal de informações pessoais. Inspirada na GDPR da União Europeia, a LGPD define conceitos fundamentais, como o de dados pessoais, dados sensíveis e tratamento de dados, além de prever princípios que regem essas atividades, como finalidade, transparência e segurança. Teceremos alguns comentários sobre quatro conceitos fundamentais.

No campo da IA, o uso de dados pessoais é amplamente empregado no treinamento de modelos de aprendizado de máquina.[258] Embora tais aplicações prometam avanços significativos em personalização e eficiência, levantam questões cruciais sobre o tratamento ético e legal dos dados e o respeito a essa autodeterminação.

Ao longo desta análise, os princípios da LGPD, como necessidade, adequação e não discriminação, serão empregados como lentes para avaliar o uso de dados em ambientes educacionais e no treinamento de IA. Será discutida também a aplicação prática desses princípios, considerando o contexto normativo e ético no qual a relação Google-USP está inserida.

1.1.1. Dado pessoal

Dado pessoal, conforme afirma o enunciado legal, é qualquer informação que permita a identificação de uma pessoa natural. Talvez o mais crucial dos elementos da LGPD, primeiro inciso do artigo 5º, o conceito de "dado pessoal" é o determinador das fronteiras da análise jurídica em matéria de proteção de dados, na medida em que um "dado que não avoque tal qualidade não poderia

[258] Ver LEFFER, 2023.

ser cogitado como um prolongamento da pessoa por lhe faltar tal centro de imputação" (BIONI, 2018, p. 100)

Tal determinação é consideravelmente abrangente, não limitando categorias de dados tratados. Assim, informações das mais variadas podem ser consideradas dados pessoais. Isso inclui, por exemplo, cookies, dados de acesso, geolocalização e qualquer informação que possa se referir a uma determinada pessoa física. Dessa forma, "verificar se um dado pode ser adjetivado como pessoal é uma análise contextual que depende de qual tipo de informação pode ser extraída de uma base de dados." (BIONI, 2018, p. 104)

Possui um tratamento especial também os dados pessoais sensíveis. uma categoria específica de dado pessoal, isto é, todo dado pessoal que informe ou permita informar acerca de alguma característica específica listada. Essa categoria expõe uma das preocupações centrais do legislador ao promover esta lei: a possibilidade de discriminação por conta de determinados aspectos referentes à personalidade.

Isso permite uma noção abrangente do que poderia ser considerado dado sensível ou não, na medida em que informações "triviais", como curtidas de redes sociais, poderiam ter um impacto significativo na descoberta destas características. Assim, dados pessoais sensíveis podem ser inferidos a partir de certos tipos de dados que seriam, à primeira vista, inócuos para sua determinação: históricos de compras, navegação na internet, *cookies* de rastreio, geolocalização, dentre inúmeros outros. Nesse sentido:

> [U]m dado "trivial" pode também se transmudar em um dado sensível; particularmente, quando se têm disponíveis tecnologias (e.g., Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos, tal como ocorreu com a loja de departamentos que identificou quais consumidoras estariam grávidas, precisando, inclusive, o período gestacional.
> [...]
> O mesmo pode suceder com outros "registros digitais", tais como o histórico de navegação, os termos de pesquisa ou mesmo as compras realizadas por um consumidor. **Todos esses dados têm o potencial de revelar muitos atributos da personalidade de um indivíduo, dentre os quais informações sensíveis a seu respeito**. (BIONI, 2018, p. 103. Grifos nossos)

Essa consideração a respeito da necessidade de contextualização para a caracterização e determinação da relevância do dado pessoal também deve ser feita quanto aos dados anonimizados. De acordo com a ANPD, esses dados são aqueles "inicialmente vinculados à pessoa natural, mas que foram posteriormente submetidos a processo de anonimização a partir de técnicas ou paradigmas como generalização e privacidade diferencial" (GUEDES; MACHADO; COSTA, 2023, p. 12).

O principal problema aqui reside na possibilidade de tais dados deixarem de ser anonimizados, expondo os titulares a que se referem. Tal risco é inerente à premissa destes dados, algo que é exposto há décadas[259] e é reconhecido também pela ANPD. Em particular, essa reidentificação se faz manifesta em duas formas relevantes para nossa análise, quais sejam a i) possibilidade de ligação (*linkability*) entre dois ou mais registros de um indivíduo e ii) a inferência de atributos a partir de outros valores anonimizados.

1.1.2. Autodeterminação informativa

Um dos pilares da LGPD é a autodeterminação informativa, que garante aos indivíduos controle sobre como seus dados são utilizados. Tal conceito possui sua origem em uma decisão de 1983 do Tribunal Constitucional Alemão (Bundesverfassungsgericht). Essa decisão se referia à constitucionalidade da Lei do Censo alemã, de forma a reconhecer a proteção de dados como direito subjetivo fundamental. A ementa da decisão afirma, em essência, o seguinte:

> 1. Nas condições do processamento de dados moderno, a proteção do indivíduo contra a coleta, armazenamento, uso e divulgação ilimitados de seus dados pessoais está coberta pelo direito de personalidade do Art. 2, §1º, da Lei Básica, em conexão com o Art. 1, §1º, da Lei Básica. **A este respeito, o direito fundamental garante o direito do indivíduo de decidir por si mesmo como os seus dados pessoais são divulgados e utilizados.**
> 2. Restrições a este direito de '**autodeterminação informativa**' são permitidas apenas no interesse geral predominante. Exigem uma base jurídica constitucional que deve corresponder ao requisito do Estado de Direito de clareza das normas. Nos seus regulamentos, o legislador deve também respeitar o princípio da

[259] Ver SCHNEIER, 2007.

> proporcionalidade. Ele também deve tomar cuidados organizacionais e processuais que neutralizem o risco de violação dos direitos pessoais.[260] (ALEMANHA, 1983, tradução livre, grifos nossos)

Sendo um direito individual para dispor da divulgação e utilização de dados pessoais, a autodeterminação informativa é "uma tutela positiva e proativa, que garanta ao titular dos dados o conhecimento pleno das formas de tratamento, finalidade e destino de seus dados." (SANTOS JR.; SANTOS, 2021, p.28).

1.1.3. Bases legais para coleta de dados

O artigo 7º da LGPD lista as hipóteses nas quais o tratamento de dados poderá ser realizado, ou seja, as bases legais para eventuais tratamentos.19 Não serão explicitadas aqui todas as bases legais para tratamentos de dados, mas apenas as que seriam mais relevantes para o estudo a ser desenvolvido. Considerando o tema de tratamento de dados de usuários do GWFE no ambiente acadêmico de educação pública superior, notadamente oferecida pela USP, três bases legais foram selecionadas dentre as demais: Consentimento, Execução de Políticas Públicas e Legítimo Interesse. Estas bases legais serão analisadas primariamente frente ao disposto no artigo 7º da LGPD, considerando o tratamento de dados pessoais não sensíveis.[261]

---

[260] No original: "1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs. 1 in Verbindung mit GG Art 1 Abs. 1 umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. [...] 2. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken."

[261] O tratamento de dados pessoais sensíveis, explicitados em *II.a.i.2*, possui suas próprias bases legais, dispostas no artigo 11 da LGPD. Algumas, como o consentimento (dadas as devidas particularidades para os dados pessoais sensíveis), se assemelham às bases legais de dados pessoais "regulares".

A) Consentimento

O consentimento, para a LGPD, está definido em seu artigo 5º, XII, como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Nesse sentido, o consentimento deve ser dado (i) livremente, isto é, sem vícios, considerando a posição entre o titular e os agentes de tratamento e priorizando a granularidade de escolha para o titular de quais dados pessoais serão tratados; (ii) de maneira informada, tendo o titular acesso facilitado a informações a respeito do controlador, da finalidade e duração do tratamento, do uso compartilhado de seus dados, bem como a quais os dados que serão tratados; (iii) inequivocamente, isto é, de maneira assertiva e positiva por parte do titular.

Assim, mostra-se como a expressão última da autodeterminação informativa de um indivíduo, delimitando a extensão da esfera personalíssima da privacidade pessoal e a maneira de disposição de seus dados pessoais. Tal extensão deverá se dar dentro de limites pactuados e previamente informados, *não podendo o controlador se beneficiar de um consentimento desatualizado ou deturpado*. Deste modo,

> a interpretação do consentimento deverá ocorrer de forma restritiva, não podendo o agente estender a autorização concedida a ele para o tratamento de dados para outros meios além daqueles pactuados, para momento posterior ou para finalidade diversa. (TEFFÉ; VIOLA, 2020, p. 6)

Considerando a dimensão da liberdade do consentimento a ser dado, é interessante compararmos a dicotomia entre a LGPD e a GDPR a respeito do condicionamento da execução de um contrato ao consentimento do titular no que se refere ao tratamento de dados pessoais. O considerando nº 43 da GDPR afirma que:

> […] **Consent is presumed not to be freely given** if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or **if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance**. (Grifos nossos)

No mesmo sentido, o artigo 7º, §4º, da GDPR dispõe:

> When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Já o artigo 9º, §3º, da LGPD dispõe que:

> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Para a LGPD, esse condicionamento contratual ao tratamento de dados pessoais não afetaria a liberdade do indivíduo ao consentir ao tratamento de seus dados, desde que informado com destaque, diferentemente do que ocorreria em uma análise de contratos sujeitos à GDPR. Da mesma forma, o §2º do mesmo artigo afirma que:

> §2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

Assim, alterações de políticas de privacidade que alterem a finalidade ou outras informações conforme disposto no artigo 8º, §6º, da LGPD, do tratamento deverão somente ser notificadas ao titular, que somente então poderá revogar seu consentimento, não havendo uma confirmação ativa por parte daquele. Isso pode ser um embaraço ao titular de dados na medida em que se adota intensamente na indústria de processamento de dados um modelo de *notice and consent*, fadigando o usuário.[262]

[262] Cf. item 0 abaixo.

B) Tratamento pela Administração Pública

Esta hipótese de tratamento de dados está disposta no artigo 7º, III, da LGDP:

> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

Talvez a principal discussão a ser tida no que tange ao tratamento de dados pela administração pública seja a questão da conciliação entre o interesse público na execução de ditas políticas públicas e a autodeterminação informativa do indivíduo:

> O que tanto o princípio da eficiência como o da supremacia do interesse público têm em comum é o fato de remeterem a ideias como interesse geral e bem comum, conceitos jurídicos dotados de elevado grau de indeterminação e que por vezes são apresentados de maneira a confrontar direitos e princípios que tutelam de maneira mais direta o indivíduo. [...] Nos últimos anos, diversos autores têm vindo a problematizar a ideia de que o interesse público se beneficiaria de uma prevalência a priori, em abstrato, em face de direitos fundamentais dos particulares. O mesmo argumento pode ser invocado com relação ao princípio da eficiência, que deve ser ponderado, nos casos concretos, com os princípios e direitos fundamentais eventualmente em jogo. (WIMMER, 2021, p. 436)

Assim, há que se falar em uma conciliação do conceito de privacidade e proteção de dados como fundamentais para a democracia, ao "encorajar a autonomia moral do cidadão e viabilizar direitos políticos, como a liberdade de associação e a criação de espaços de discussão cívica sem temor de represálias" (WIMMER, 2021, p. 438). Nesse sentido, considerando a expansão de serviços como o GWFE para dentro de ambientes acadêmicos e educacionais públicos, o tratamento de dados pessoais realizados neste âmbito deverá, por parte da administração pública responsável pela execução de políticas de educação, observar essa conciliação.

C) Legítimo Interesse

Por último, trataremos da base legal do legítimo interesse. O legítimo interesse do controlador está previsto no artigo 7º, IX, da LGPD: "IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

As condições para a aplicação do legítimo interesse como base legal de tratamento de dados estão dispostas no artigo 10º da LGPD:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II- proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1° Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

Considerando as condições expostas acima, apesar de ser a base legal mais "flexível", considerando um leque maior de aplicabilidade, o legítimo interesse deve ser aplicado somente diante de uma situação concreta e legítima que se atenha aos interesses do controlador ou de terceiros. O controlador deverá também zelar pela transparência do tratamento a ser realizado, reforçando o princípio explicitado pelo artigo 6º, VI, da LGPD.

2. Estudo de Caso: Google Workspace for Education e USP

A implementação do GWFE na Universidade de São Paulo (USP) representa um exemplo significativo de integração de tecnologias digitais no ambiente acadêmico. Firmado em 2016, o Termo de Cooperação Técnica entre a USP e o Google permitiu a utilização gratuita de ferramentas como Gmail, Google Drive, Google Classroom e outras, com o objetivo de aprimorar a produtividade e a eficiência educacional.

Em 9 de dezembro de 2016, foi anunciado pela Assessoria de Imprensa da USP que um termo de cooperação entre a Universidade e o Google foi firmado. Tal termo possibilitaria a "alunos, alumni [ex-alunos], docentes e servidores técnicos e administrativos da Universidade a utilização dos recursos que compõem a ferramenta G Suite for Education." (USP, 2016) De acordo com o anúncio, tais recursos incluiriam "uso ilimitado" de serviços de e-mail, calendário, contatos, comunicação digital, e armazenamento e compartilhamento de documentos.[263] Tal projeto supostamente apresentaria uma economia de aproximadamente R$6 milhões por ano em gastos pela USP com o gerenciamento de mensagens, sem envolver qualquer transferência de recursos pela USP ao Google.

Começaremos nossa análise com a contratação do serviço GWFE pela USP. Tal contratação se manifesta por meio de dois documentos disponíveis publicamente: o Termo de Cooperação Técnica e o Contrato Google Apps for Education.

2.1. Termo de Cooperação Técnica[264]

O primeiro documento a analisarmos será o Termo de Cooperação Técnica ("Termo"). O Termo constitui um instrumento jurídico formalizado entre entidade da Administração Pública indireta que é a Universidade de São Paulo, em sua qualidade de autarquia estadual, e uma entidade privada, que é o Google, visando, por meio de cooperação técnica, a execução de um projeto do qual não decorre qualquer obrigação de repasse de recursos ou transferência de crédito. Suas cláusulas relevantes serão analisadas abaixo.

O contrato afirma em sua Cláusula 1.1 que seu objeto será o "intercâmbio e a cooperação técnica entre os partícipes por meio da utilização do GWFE por estudantes, docentes e servidores técnico-administrativos da Universidade de São Paulo."

[263] Em 2023, esse uso ilimitado de armazenamento foi reduzido a apenas 20GB de armazenamento em nuvem.
[264] USP; GOOGLE, INC, 2016a.

Limitados aos ciclos da educação superior, tal intercâmbio e cooperação estão detalhados na Cláusula 2 e deverão "focar a qualificação de educadores, o acesso e a conclusão da educação superior, a melhoria do processo de ensino e aprendizagem, com vistas à adoção de novas estratégias, práticas e ferramentas por docentes e estudantes, buscando contribuir para uma educação de qualidade."

O Termo afirma também, na cláusula 1.2, que não haverá qualquer desembolso financeiro por parte da USP, sendo os serviços "disponibilizados de maneira gratuita pelo Google à USP durante toda a relação contratual entre as partes", suplantando eventuais disposições em contrário no Contrato Google Apps for Education.

De acordo com ofício da Superintendência de Tecnologia da Informação da USP ("STI"), o contrato permanece vigente até hoje, tendo sido renovado em 23 de dezembro de 2021 (STI, 2022).

2.2. Contrato Google Apps for Education[265]

O Contrato Google Apps for Education ("Contrato") é o corolário do Termo acima. O Contrato possui como objetivo regular a utilização dos serviços disponibilizados pelo Google à USP, bem como o acesso desta a eles. Assim como no caso do Termo, listaremos e analisaremos somente cláusulas mais relevantes do contrato, em especial aquelas que se refiram ao tratamento de dados dos usuários finais.

No Contrato, o termo "Dados do Cliente" é definido como "dados, incluindo e-mails, fornecidos, gerados, transmitidos ou exibidos através dos Serviços pela USP ou pelos Usuários Finais." De maneira breve, há aqui uma dificuldade de diferenciar o que seriam de fato tais dados: por exemplo, se estes incluiriam metadados, se seriam somente os arquivos gerados e armazenados pelos usuários finais (como conteúdo de e-mails, documentos escritos, fotos, etc.) ou se incluiriam informações sobre as atividades destes usuários.

[265] USP; GOOGLE, INC, 2016b.

Considerando que a obrigação principal do Google neste Contrato é a oferta gratuita dos Serviços, passaremos agora a analisar as obrigações da USP para com a execução do Contrato. Um ponto relevante está na cláusula 2.3, afirmando que a USP "concorda que as responsabilidades da Google não se estendem à gestão ou administração interna dos Serviços para a USP e que a Google é apenas um processador de dados." Isso é problemático na medida em que o Google trata os dados e toma decisões a respeito de seu uso de maneira distinta e separada daquelas da USP.

A Cláusula 2.4 do Contrato trata acerca da obtenção de consentimento por parte do Usuário Final. Desta cláusula decorrem dois pontos importantes: (i) a responsabilidade da USP pela obtenção e manutenção do consentimento dos Usuários Finais para os tratamentos de dados mencionados acima; e (ii) o fato de que a USP tem acesso aos dados armazenados por e disponíveis aos usuários. Em comunicações de e-mail realizadas com a STI-USP, foi informado que tal consentimento é realizado por meio da concordância com termos de uso no momento da solicitação de conta de e-mail pelo usuário final:

> 3) A cláusula 2.4, do Contrato do Google Apps for Education, afirma que "[a] USP deverá receber e manter todos os consentimentos necessários dos Usuários Finais que permitam: (i) que a USP acesse, monitore, use e divulgue esses dados, o que será permitido pela Google, e (ii) que a Google forneça os Serviços". Quais documentos a USP mantém para a comprovação desse consentimento? Esse consentimento é revogável pelos alunos? Eu poderia ter acesso, como aluno da USP, ao documento em que forneço esse consentimento?
> R: **Para completar a solicitação de e-mail o usuário final deve concordar com os termos de uso no passo 3.** Os termos de uso estão sempre disponíveis no portal de solicitação: https://id.usp.br/restrito/faq.xhtml. A revogação pode ser obtida por meio de solicitação da exclusão da conta de e-mail. (grifos nossos) (STI-USP, 2021)

Dados pessoais decorrentes de registros educacionais permitem a aquisição de uma gama de informações acerca um indivíduo, e, considerando recursos como o Google Atividades e Google Classroom, disponibilizados pelos serviços do Contrato, tais informações estariam possivelmente disponíveis ao

Google, devendo haver restrições quanto a sua divulgação ou utilização. Conforme afirma João Paulo Bachur (2021, p. 731):

> A vida escolar, portanto, nada mais é do que uma sequência de vestígios registrados pelas secretarias de educação de estados e municípios ou pelas escolas e universidades: notas, frequência, observações comportamentais (advertências, elogios etc.), ocorrências médicas e psicológicas, aptidões físicas, score financeiro da família (inadimplência no setor privado ou acesso a serviços conexos no setor público, tais como auxílios financeiros, frequência ao restaurante universitário ou moradia estudantil etc.); enfim, a educação pode ser a porta de entrada para inúmeras técnicas de profiling. E mais: [...] veremos que a educação pode fornecer dados pessoais complexos e altamente sofisticados.

Por fim, é inegável que o Google é uma empresa cuja principal atividade se relaciona ao mercado publicitário. Seu faturamento com anúncios atingia aproximadamente US$238 bilhões e é 77% de sua receita. O Google atinge tais números a partir do direcionamento personalizado de anúncios, fomentado a partir da construção de perfis com gostos e preferências daqueles a quem os anúncios são mostrados.[266] Estes perfis são construídos a partir de uma gama de dados a respeito destes indivíduos, desde cookies, histórico e atividades de navegação,[267] dados de e-mails (remetentes, destinatários, assuntos e palavras-chave),[268] geolocalização (seja por GPS ou IP), *fingerprinting*, etc; em suma, a partir de uma gama de dados pessoais.

Tendo isso em mente, o Contrato afirma, em sua Cláusula 1.4, que o "Google não exibe Anúncios nos Serviços nem usa Dados de Clientes para fins publicitários." Que anúncios não são exibidos nos Serviços é algo atestável por qualquer um que faz uso do GWFE. Entretanto, a segunda parte da afirmação acima é um tanto mais problemática. Não é claro quais dados estariam sendo processados (ou não) para fins publicitários. Pelo discutido acima, isso significaria que o Google não analisa arquivos e eventuais documentos criados

[266] Ver ELIAS; GRAHAM, 2021 e ZANDT, 2024
[267] Ver AMADEO, 2021.
[268] O Google deixou de escanear o conteúdo de e-mails no Gmail em 2017, mas ainda permite que terceiros o façam. Isso não se aplica a informações sobre tais e-mails, como os remetentes e destinatários, assunto, etc. Ver YURIEFF, 2018.

ou processados pelo usuário final, mas isso não significa (pois não há clareza na definição destes Dados do Cliente), que o Google não analise metadados referentes a estes arquivos, ou monitore a utilização dos Serviços pelo usuário, algo que certamente renderia dados pessoais para o processamento publicitário. Dada a oferta gratuita dos serviços e o fato de que o Google é uma empresa motivada por lucro, é forçoso reconhecer que tal vagueza de definição permite um vácuo sobre a determinação de como o Google processaria dados no âmbito do contrato. Isso será mais bem explorado ao analisarmos políticas de privacidade e termos acerca do processamento de dados do Google.

2.3. Termos referenciados

Tendo em vista o discutido acima, trataremos agora dos termos referenciados no Contrato e no Termo, de modo a verificar como é realizado o tratamento de dados dos usuários finais dos serviços GWFE no âmbito da USP.

A) Cloud Privacy Notice[269]

O Cloud Privacy Notice ("CPN") é um aviso de privacidade que engloba os serviços de nuvem do Google, dentro dos quais está o GWFE. O CPN dispõe acerca das medidas de segurança, hipóteses de compartilhamento e sobre dados de serviço ("Service Data"), coletados em conexão com a execução dos serviços. Tal Service Data é defina da seguinte forma: "Service Data is the personal information Google collects or generates during the provision and administration of the Cloud Services, excluding any Customer Data and Partner Data. […]".

O CPN apresenta também várias razões para o processamento desses dados, dentre as quais estão recomendações para otimização do uso dos serviços, manutenção e melhorias, obrigações legais e contratuais, e outras razões que contem com o consentimento do usuário. Nesse sentido:

> To achieve these purposes, **we may use Service Data together with information we collect from other Google products and services. We may use algorithms to recognize patterns in**

[269] GOOGLE LLC. 2024a

> **Service Data**. Manual collection and review of Service Data may also occur, such as when you interact directly with our billing or support teams. **We may aggregate and anonymize Service Data to eliminate personal details**, and we may use Service Data for internal reporting and analysis of applicable product and business operations.

Assim, há aqui menções à correlação de dados coletados em outros serviços Google, processamento algorítmico e processos de anonimização destes dados. Não é certo quando tais processos são aplicados.

B) Aviso de Privacidade do GWFE[270]

O Aviso de Privacidade do Google Workspace for Education ("Aviso GWFE") é outro documento relevante do ponto de vista do tratamento de dados dos usuários finais. Aqui é necessário fazer a distinção entre os serviços principais e os serviços adicionais do GWFE. Os serviços principais são aqueles serviços nucleares ao auxílio concedido pela contratação destes serviços à realização da prestação educacional, enquanto os adicionais seriam aqueles disponibilizados, via de regra, a consumidores em geral "como a Busca, Google Maps e YouTube". Nesse sentido, há uma diferença entre o tratamento de dados no âmbito de cada uma dessas categorias de serviços. De acordo com o visto nos documentos acima, é afirmado novamente que "nenhuma das informações pessoais coletadas nos serviços **principais** é usada para fins de publicidade." Entretanto, no caso da utilização de serviços **adicionais**,

> [...] coletamos informações quando os estudantes e educadores usam serviços adicionais, incluindo o que você fornece, conteúdo criado ou enviado e conteúdo recebido de outros. Por exemplo, se você fizer login em um serviço adicional com uma conta do Google Workspace, usaremos o seu nome e as informações do perfil do Google Workspace para identificar a conta que você está usando.

De acordo com o Aviso GWFE, tais informações podem ser utilizadas para fins de publicidade. Vale mencionar também que o documento realiza também a

[270] GOOGLE LLC. 2024b

diferenciação entre dados do cliente (Customer Data) e dados do serviço (Service Data), aludindo ao CNP:

> *À medida que alunos, educadores e administradores usam os serviços principais do Google Workspace, coletamos dois tipos de dados:*
> *• O que você fornece ou cria com os serviços principais (dados do cliente);*
> *• Informações que coletamos quando você usa os serviços principais (dados do serviço)*

Os mesmos tipos de dados são coletados pelos serviços adicionais.

C) Política de Privacidade do Google[271]

A Política de Privacidade ("Política") apresenta 3 categorias diferentes de dados a serem coletados através dos serviços: (i) identificadores, (ii) atividade e (iii) localização.

Sobre os identificadores, a Política afirma que o Google coleta dados sobre apps, navegadores e dispositivos utilizados para acessar os serviços, o que inclui, para além do IP, "identificadores exclusivos, tipo e configurações de navegador, tipo e configurações de dispositivo, sistema operacional, informações de rede móvel, incluindo nome e número de telefone da operadora e número da versão do aplicativo". Esses dados não se limitam à identificação somente da conta Google, mas permitem também uma identificação única do dispositivo ou navegador utilizado e, de acordo com a Política de Privacidade, "podem ser usados para diversas finalidades, inclusive segurança e detecção de fraudes, sincronização de serviços, como a caixa de entrada de e-mails, **memorização das suas preferências e exibição de anúncios personalizados**" (grifos nossos).

Sobre a atividade do usuário, considerando o amplo escopo de atuação dos serviços providos pelo Google, são fornecidos apenas exemplos sobre as informações coletadas. Dentre estas, estão termos pesquisados, visualizações e interações com conteúdo e anúncios, pessoas com quem se comunica ou compartilha conteúdo, atividades em sites e aplicativos de terceiros que usam os serviços, históricos de navegação, de chamadas e mensagens, endereços de e-

[271] GOOGLE LLC. 2024c

mail do remetente e destinatário, bem como números de telefone, registros, horários, datas e durações de chamadas e mensagens, entre outros.

O mesmo documento afirma que o Google "[usa] várias tecnologias para coletar e armazenar informações, incluindo cookies,[272] *tags* de pixel, armazenamento local como armazenamento do navegador da Web ou caches de dados de aplicativos, bancos de dados e registros do servidor."

Assim, a Política traz também as finalidades para o tratamento dos dados mencionados acima. Diversos exemplos concretos de finalidades são apresentados ao longo das explicações, entretanto, dentre as finalidades oficiais descritas estão o fornecimento, manutenção e melhoria dos serviços atuais, o desenvolvimento de serviços futuros e o "fornecimento de serviços personalizados, incluindo conteúdo e anúncios". Sobre esta última finalidade, a Política de Privacidade afirma que anúncios personalizados podem ser exibidos com base em interesses passados pelos usuários. Pontos relevantes sobre esse quesito são os seguintes:

> • Não mostramos anúncios personalizados com base em categorias sensíveis, como raça, religião, orientação sexual ou saúde.
> • Não mostramos anúncios personalizados com base no seu **conteúdo** do Drive, Gmail ou Fotos.
> • Não compartilhamos informações que identifiquem você pessoalmente para anunciantes, como nome ou e-mail, a menos que você nos peça. [...]

Nesse sentido, ainda que seja possível que dados pessoais sensíveis possam acabar sendo coletados (dado o imenso volume de dados mencionados pela Política de Privacidade), é de extrema relevância que estes não seriam processados para fins de publicidade.

---

[272] "*Cookies*" podem ser definidos como "pequenos arquivos de texto que são armazenados no terminal do usuário (cliente) e que são deixados pelo servidor web antes que o ciclo da comunicação por meio do protocolo HTTP se encerre." (PALHARES, 2020, p. 12). Em essência, isso significa que estes arquivos, pequenos pacotes de informação, são capazes de "armazenar diversas informações sobre os hábitos de utilização da internet do usuário, desde os links que foram clicados, os produtos que foram comprados, os termos que foram pesquisados, a região em que vive o usuário, e tantos outros dados valiosos para uma eventual segmentação de publicidade, que vão muito além dos objetivos para os quais foram inicialmente concebidos, de meramente viabilizar algumas funcionalidades específicas." (Id., p. 13). São uma peça fundamental para a coleta de dados realizada pelo Google.

Sobre o segundo ponto (Drive, Gmail...), a palavra utilizada é "conteúdo". A Política de Privacidade se utiliza dessa expressão quando se refere àquilo que os usuários criam ou consomem através dos serviços. Não é negada aqui, entretanto, a utilização de dados de atividade, localização ou identificadores (normalmente referidos como "informação") para estes fins.

É importante frisar aqui que o documento traz diversos recursos para que o usuário tenha controle sobre o tratamento de seus dados, inclusive para fins de anúncios e publicidade. As soluções apresentadas se resumem a ações a serem tomadas pelo usuário para evitar a coleta de dados, como deletar ou bloquear cookies por exemplo. Algumas são mais "eficazes" do que outras, entretanto.[273]

3. Considerações Críticas e Valorativas

Considerando o quadro normativo e instrumental descrito acima, passaremos agora por certos pontos que podem ser de interesse no que concerne à relação de tratamento de dados. Isso servirá para verificarmos possíveis consequências à privacidade e à autodeterminação informativa dos usuários finais do serviço GWFE no âmbito da USP.

3.1. Retórica das Políticas de Privacidade (conteúdo vs. informação)

Primeiramente, é relevante falarmos a respeito da retórica aplicada nos instrumentos contratuais analisados acima. Conforme discutido *ad nauseam* neste trabalho, há uma diferença entre "conteúdo dos usuários" e "informações sobre os usuários". Ambos os conceitos podem conter dados pessoais. Tal distinção é apontada como crucial por Lindh e Nolin (2016). Para as autoras, há uma distinção acerca de como os conceitos são explorados pela Política de Privacidade:

> Whenever the concept (your) 'data' is used, Google usually refers to numerous ethical principles of non-surveillance and non-commercial exploitation.

[273] As configurações de localização, por exemplo, não permitem controle total sobre dados de localização, sendo possível ainda a obtenção destes por meio de IP. Ainda que a localização esteja "desligada", "[v]ocê poderá receber resultados da pesquisa e anúncios com base em informações como seu endereço IP. Aprenda a gerenciar sua localização ao pesquisar no Google."

> However, (collected) 'information' refers to something completely different than (your) 'data', namely the things that people do, i.e., their behaviour. In their privacy policy, Google lists at length 'information that we collect' […] (LINDH; NOLIN, 2016, p. 652)

Há diversas menções acerca de como o Google não utiliza conteúdo para fins de publicidade ou até mesmo dados pessoais. Conforme visto acima, o mesmo não pode ser dito acerca das informações sobre os usuários. Informações identificadoras, de atividade e localização são constantemente utilizadas para esses fins. Em essência, isso significaria que tais informações servem ao propósito de formação de identidades algorítmicas:

> Our interpretation is that 'personal information' as well as 'collected information' in these policy documents means algorithmic identities. It is then emphasised that 'sensitive personal information' is not used as a source in the construction of algorithmic identities, although it is not clear how this filtering is performed.
> When Google asserts 'we do not share personal information placed in our systems with third parties' (Google for Education: Tools schools can trust, 2016) it can be interpreted as: we do not sell our algorithmic identities of users. However, this does not mean that Google abstains from utilising these resources in order to produce targeted advertisement (LINDH; NOLIN, p. 653)

Nesse sentido, "Google is less interested in exploiting this data and much more concerned with the monitoring of behaviour, i.e., to exploit the collected and personal information, creating algorithmic identities of individual users" (LINDH; NOLIN, p. 657).

Ao longo dos documentos contratuais são usados diversos exemplos para ilustrar certas finalidades do tratamento de dados. De certo modo, estes exemplos servem para enfatizar certos aspectos das proposições apresentadas pelo documento, enquanto minimiza ou não menciona outros aspectos relevantes. Por outras vezes, afirmações são feitas de maneira "clara", isto é, afirmações que, à primeira vista, permitiriam apenas uma interpretação. A Política ao falar da finalidade do tratamento de dados também traz constantemente um enquadramento para o tratamento destes dados que seria sempre beneficial ao usuário. A utilização da linguagem acima, para além de

eventuais contradições entre os documentos, é uma das dificuldades em analisar o impacto à privacidade dos usuários finais.

3.2. *Profiling*, *Fingerprinting* e Anúncios

Considerando o acima e tendo em mente que os dados coletados são, em sua maioria, conectados a uma conta Google, a qual é em si relacionada ao serviço GWFE, que identifica usuários com relação ao ambiente estudantil, é possível argumentar que a interconexão entre as informações coletadas sobre os usuários sirva para a criação de uma identidade algorítmica para usuários finais relacionados ao ambiente acadêmico. Isso, pois não é negado que, no âmbito da relação GWFE, dados de usuários finais, mais especificamente, as informações sobres estes usuários, sejam usados para fins de anúncios ou publicidade.64 Não obstante, informações sobre contas Google no ambiente GWFE que tenham relação com serviços adicionais podem ser utilizadas para fins de anúncios.

Em essência, isso significaria uma segmentação destes usuários, permitindo revelações acerca de seus hábitos de consumo, históricos de navegação, localização, círculos sociais e mais. Todas essas revelações são, conforme discutido acima, possíveis através da "mera" coleta de informações sobre o usuário, considerando as informações identificadoras, de atividade e localização descritas acima. Nesse sentido, o que de um lado seria uma atividade de processamento e aprimoramento do ambiente estudantil, de outro se torna uma porta de entrada para riscos de Profiling (isto é, a literal criação de perfis e identidades algorítmicas), bem como permitiria um insight maior a respeito do funcionamento deste grupo segmentado para fins de publicidade direcionada, a principal atividade econômica do Google.

As ponderações acima são ainda mais válidas ao considerarmos a possibilidade de correlação de informações de identificação entre contas. Isso se daria através da técnica de *fingerprinting*:

> Por sua vez, fingerprinting é uma técnica que usa detalhes do navegador e dos dispositivos utilizados pelo usuário (como o modelo do notebook do usuário, a versão do navegador e a lista de plug-ins que estão instalados no navegador, a resolução da

> tela, o sistema operacional do dispositivo, entre outros) para identificar o usuário e lhe mostrar publicidades específicas, sem a necessidade de armazenamento de cookies para esse fim. (PALHARES, 2020, p. 17)

Nesse sentido, ao reconhecer através de informações identificadoras, por exemplo, que duas contas Google separadas, sendo uma delas uma conta relacionada ao GWFE, utilizam o mesmo dispositivo, seria possível, ao menos em tese, realizar a correlação entre as atividades de cada uma destas contas para a criação de um perfil ou identidade algorítmica mais completa. Seria possível, desse modo, a correlação de informações obtidas por meio de contas que estivessem fora da relação GWFE-USP. Essa correlação de contas em um mesmo dispositivo através de *fingerprinting* permitiria, em conjunto com outras ferramentas de rastreio mencionadas, como cookies, um retrato mais profundo acerca dessa classe de usuários finais relacionados ao ambiente GWFE e ao ambiente estudantil como um todo.

3.3. *Notice and Consent*

Considerando os riscos e possibilidades de tratamento postuladas acima, deve-se levar em consideração o modelo de notice and consent aplicado aqui. O modelo é construído a partir de usuários finais e titulares de dados realizando decisões individuais a respeito de sua privacidade e dados pessoais a partir de informações disponibilizadas por agentes de tratamento. Em essência, isso traz dois aspectos a serem analisados, a escolha (*consent*) e as informações providas (*notice*).

Considerando primeiramente o aspecto acerca das informações providas, é certo que há aqui diversos desafios para uma interpretação concisa da realização do tratamento de dados. Há informações conflitantes ou não claras entre os documentos analisados, diferentes expressões utilizadas que se referem a dados ou informações idênticas, linguagem simplificadora ou minimizadora. Documentos referentes ao processamento destes dados também podem, em alguns casos, alterados em qualquer momento. Não obstante, conhecimento

acerca do funcionamento de processos de coleta dessas informações, o que elas constituem e qual seu significado, apesar da constante inserção social deste debate, é limitado, sendo, muitas vezes, difícil para o titular de dados, usuário final dos serviços, ter uma compreensão do que significaria aceitar (ou consentir) aos termos para fins do processamento de seus dados.

É importante deixar claro que os problemas mencionados acima não impedem que informações fundamentais sejam respondidas, mas o esforço para descobri-las é um tanto significativo, depositando sobre o usuário o ônus de se manter atualizado constantemente sobre o processamento de seus dados:

> If the moral legitimacy of notice and consent stems from the belief that it respects individual autonomy, specifically, that it reflects rational and informed agency required of a competitive marketplace, OBA simply does not meet these requirements. This finding does not in itself imply that OBA is unethical, only that the particular approach to addressing privacy threats so favored by businesses and even consumer advocates is seriously flawed. (BAROCAS; NISSENBAUM, 2009, p. 6)

Considerando a decisão da USP por realizar o tratamento de dados por meio do GWFE, há, assim, uma transferência de responsabilidade ao indivíduo, inserido no ambiente estudantil, de concordar e ter consciência por meio da adoção deste modelo de *notice and consent* de todos os aspectos relacionados ao tratamento de seus dados.

Da mesma forma, caso o consentimento seja aplicado como base legal, é possível falar ainda em um consentimento "livre", considerando que a única alternativa seria, supostamente, revogar o consentimento para o tratamento de dados? Para a LGPD, parece que, desde que os requisitos do artigo 9º, §3º, sejam cumpridos, sim. No caso da GDPR, este ponto seria um tanto mais controverso. A discussão sobre tal liberdade é afetada ainda ao considerarmos o serviço ao qual o tratamento de dados é condição para o fornecimento: a prestação educacional de ensino superior. Logicamente, não se imagina um caso no qual tal prestação seja recusada pela USP, entidade pública, por meio do não consentimento ao tratamento de dados acima, mas ela é certamente afetada. Isso, em especial, considerando a utilização dos serviços GWFE para a realização de

comunicações institucionais, bem como, como restou provado durante a pandemia, a realização de aulas à distância, por meio da plataforma Google Meet por exemplo.

3.4. Legitimidade, Interesse Público e Autodeterminação informativa

Outra questão interessante a ser notada é a ausência de uma determinação acerca do valor comercial dos dados e informações a serem processadas pelo Google. Considerando a utilização destes dados e informações coletados para fins de exibição de anúncios e formação de identidades algorítmicas, é possível argumentar a sua conexão com um valor econômico.

Não obstante, a autodeterminação informativa, em sua dimensão de invisibilidade, isto é, o controle pelo titular de dados acerca de quais dados pessoais seus serão tratados em um dado momento, é um dos pilares da legislação de proteção de dados, de acordo com o já mencionado artigo 2º da LGPD. É possível falar em autodeterminação informativa quando as condições para a informação de como dispor sobre os próprios dados são comprometidas? Nesse sentido, qual seria a "legitimidade" para a opção realizada pela USP no que tange à contratação do serviço GWFE tratamento de dados em um primeiro momento, em especial considerando que a prestação de valor econômico a ser concretizada, isto é, a entrega de dados pessoais a serem tratados pelo Google, é realizada pelos usuários finais? Trata-se de uma discussão anterior à questão sobre bases legais, refletindo a decisão sobre a contratação dos serviços GWFE pela USP.

Logicamente, uma primeira resposta se encontraria na consideração de que dados pessoais em si não possuiriam um valor econômico intrínseco, de modo que somente o seu tratamento de acordo com determinadas finalidades é o que geraria tal valor. Nesse sentido a prestação realizada pelo usuário pelo recebimento dos serviços é verdadeiramente gratuita, de certo ponto de vista, sem qualquer transferência de valor entre os titulares e os agentes de tratamento. Tal ponto é em si questionável, em particular considerando o conjunto de

massivo de dados envolvendo ainda milhares de usuários, que certamente possui valor econômico, mas merece nota.

Outra razão para tal "legitimidade" se centraria na questão do interesse público, um dos pilares que legitimariam o tratamento de dados pela administração pública. O interesse público por uma realização mais "eficiente" da prestação educacional suplantaria a autodeterminação informativa e o consentimento dos usuários, dados os grandes benefícios a serem obtidos pela prestação de serviços, isto é, uma então economia anal de R$6 milhões e a prestação de serviços computacionais de qualidade.

Nesse sentido, qual seria a vantagem mínima a ser obtida pela administração pública (e isso se limita à questão do ambiente público) para que o interesse público suplante a autodeterminação informativa de alunos professores e servidores e permita a contratação de um serviço que será condicionado ao tratamento de seus dados? Tratar-se-ia somente de uma vantagem econômica ou há outros quesitos a serem avaliados?

Essas questões se tornam ainda mais relevantes ao considerarmos a redução da "eficiência econômica" da contratação inicial quando comparada com uma contratação superior pretendida pela USP, a qual exigirá a realização de pagamentos calculados com base no número de usuários, bem como a recente redução da capacidade de armazenamento pela universidade, antes ilimitado e agora restrito a 20GB por aluno.

Finalmente, é de se notar que há aqui uma questão de soberania envolvida, em particular considerando a transferência internacional de dados de uma instituição produtora de conhecimento e inovação como a USP, parte da administração pública estadual e, portanto, publicamente financiada, para uma empresa de tecnologia. Como vimos, o monitoramento de informações a respeito dos usuários finais pode trazer um conjunto de dados colossal a respeito não só de um usuário em específico, mas de toda uma gama de usuários, nesse caso, de toda a comunidade acadêmica da USP. Em que medida a ausência de uma infraestrutura informacional própria afeta a soberania das pesquisas realizadas no país?

O levantamento de tais dificuldades e quesitos são relevantes para compreendermos a atuação concreta de princípios, fundamentos e conceitos da legislação de proteção de dados no Brasil e as respostas que serão dadas a esses ditarão, possivelmente, futuras disputas e discussões regulatórias em matéria de proteção de dados.

3.5. Breves Considerações sobre IA

Os dados gerados por usuários do GWFE, como interações em plataformas digitais, conteúdo de e-mails e documentos criados, possuem alto valor para o desenvolvimento de algoritmos preditivos e sistemas personalizados. No entanto, a utilização desses dados em treinamentos de IA requer atenção a vários aspectos críticos.

A LGPD exige que os titulares dos dados sejam informados de forma clara e inequívoca sobre o uso de suas informações pessoais, incluindo quaisquer finalidades secundárias, como o treinamento de IA. No caso da relação Google-USP, não há evidências de que os usuários sejam informados sobre o potencial uso de seus dados para desenvolver sistemas de IA. Tal lacuna compromete o direito à autodeterminação informativa, conforme explícita acima, pois os titulares não têm controle sobre os usos futuros de seus dados.

Apesar das repetidas (e às vezes contraditórias) afirmações de que "dados" dos clientes não seriam utilizados para fins de publicidade, o Google mantém firmemente a possibilidade de tratamento de dados pessoais com base no legítimo interesse, para a melhoria e oferta de serviços. O treinamento de ferramentas de IA com base nesses dados, fornecidos em um contexto de privatização da infraestrutura acadêmica, sem uma verdadeira possibilidade de negativa por parte dos seus titulares, estaria encoberto pela base do legítimo interesse?

Conforme os documentos analisados acima, não há nenhuma menção aos dados que seriam utilizados pelo Google para o treinamento de suas ferramentas de inteligência artificial. A ausência de mecanismos robustos de auditoria e supervisão sobre o uso de dados na relação Google-USP agrava os riscos

associados ao treinamento de IA. Modelos de IA, muitas vezes descritos como "caixas-pretas", tornam difícil identificar como os dados dos usuários são tratados e quais decisões são tomadas com base nesses dados.

Conclusão

A partir das análises apresentadas no decorrer do capítulo, foi possível notar as diversas particularidades contidas na relação de tratamento de dados GWFE-USP. Com essas particularidades, foi possível trabalhar e manusear diversos dos conceitos apresentados pela LGPD, em particular o conceito primordial de dados pessoais e o fundamento da autodeterminação informativa. Da mesma forma, a análise de instrumentos contratuais e publicações referentes ao tratamento de dados pessoais, como políticas de privacidade e documentos congêneres, contrastados à luz das disposições da LGPD, permitiu a compreensão de diversos possíveis impactos para a privacidade dos usuários finais da relação GWFE-USP. Tal compreensão é fundamental para compreender a inserção destas tecnologias e interesses negociais no ambiente educacional e acadêmico.

A partir da análise foi também possível suscitar diversas questões e instigar novas discussões sobre o tema. Deve-se notar, entretanto que há uma perceptível dificuldade de operar os conceitos abordados pela LGPD em um contexto comercial e contratual. Considerando a imaturidade regulatória a respeito do tema, tal dificuldade operacional é, de certa forma, natural. Essa, entretanto, não foi a única dificuldade encontrada ao longo da pesquisa. Diversos documentos contratuais foram analisados, os quais eram constantemente atualizados e modificados. Essas dificuldades, entretanto, não foram um impedimento a uma análise concreta que produzisse avaliações e conclusões críticas sobre a relação GWFE-USP.

Por fim, espera-se que este capítulo sirva, de alguma forma, para uma melhor compreensão acerca do debate sobre proteção de dados e, mais precisamente, sobre a inserção de tecnologias no ambiente acadêmico.

Referências

ALEMANHA. Bundesverfassungsgericht. **Julgamento do Primeiro Senado 15 de dezembro de 1983 – 1 BVR 209/83 –, Rn. 1-21**. Decisão sobre o censo populacional de 1982. Karlsruhe. 1983. Disponível em: https://www.bverfg.de/e/rs19831215_1bvr020983.html , acesso em 19/10/2021.

AMADEO, R. **Judge rules $5 billion Google Chrome Incognito mode lawsuit can go forward**. Disponível em: <https://arstechnica.com/gadgets/2021/03/judge-rules-5-billion-google-chrome-incognito-mode-lawsuit-can-go-forward>. Acesso em: 25 nov. 2024.

BACHUR, J. P. Proteção de Dados Pessoais na Educação. Em: BIONI, B. R. (Ed.). **Tratado de Proteção de Dados Pessoais**. 1. ed. Rio de Janeiro: Forense, 2021.

BAROCAS, S.; NISSENBAUM, H. **On Notice: The Trouble with Notice and Consent**. Rochester, NYSocial Science Research Network, , 2009. Disponível em: <https://papers.ssrn.com/abstract=2567409>. Acesso em: 25 nov. 2024

BIONI, B. R. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. 1ª edição ed. Rio de Janeiro, RJ: Editora Forense, 2018.

ELIAS, M.; GRAHAM. **How Google's $150 billion advertising business works**. Disponível em: <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html>. Acesso em: 25 nov. 2024.

GOOGLE LLC. **Cloud Privacy Notice**. [*s.l.*], 2024a. Disponível em: https://cloud.google.com/terms/cloud-privacy-notice. Acesso em 20/11/2024.

GOOGLE LLC. **Política de Privacidade do Google**. [s.l.], 2024b. Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em 20/11/2024..

GOOGLE LLC. **Aviso de Privacidade do Google Workspace for Education**. [s.l.], 2024c. Disponível em: https://workspace.google.com/terms/education_privacy.html. Acesso em 20/11/2024.

GILBERT, N. **Number of Active Gmail Users 2019 & 2020: Statistics, Demographics, & Usage**. Disponível em:

<https://financesonline.com/number-of-active-gmail-users/>. Acesso em: 24 nov. 2024.

GUEDES, M. S.; MACHADO, D. C.; COSTA, A. F. J. **ESTUDO TÉCNICO SOBRE A ANONIMIZAÇÃO DE DADOS NA LGPD: ANÁLISE JURÍDICA**. Brasília, DF: ANPD, nov. 2023.

LEFFER, L. **Your Personal Information Is Probably Being Used to Train Generative AI Models**. Disponível em: <https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/>. Acesso em: 24 nov. 2024.

LINDH, M.; NOLIN, J. Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education. **European Educational Research Journal**, v. 15, n. 6, p. 644–663, 1 nov. 2016.

MONTEIRO, J. R. Terceirização na universidade pública: limites de eficiência e de qualidade, com ênfase na experiência da UnB. 1 jul. 2020.

PALHARES, Felipe. Cookies: contornos atuais. In: FELIPE PALHARES (org.). **Temas Atuais de Proteção de Dados**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 17.

PETROVA, J. E., Magdalena. **Google's rocky path to email domination**. Disponível em: <https://www.cnbc.com/2019/10/26/gmail-dominates-consumer-email-with-1point5-billion-users.html>. Acesso em: 24 nov. 2024.

SANTOS JR., B. DOS; SANTOS, J. V. DOS. Cap. I - Autodeterminação Informativa: surge um novo direito fundamental. Em: **Aspectos relevantes da Lei Geral de Proteção de Dados**. São Paulo: Editora Contracorrente, 2021.

SCHNEIER, B. Why "Anonymous" Data Sometimes Isn't. **Wired**, 2007.

STI-USP. **Ofício STI/008/2022**. 1 fev. 2022. Disponível em: <https://eesc.usp.br/comunicacao-admin/wp-content/uploads/2022/02/Oficio-STI-008_2022-Renovacao-do-Termo-de-Cooperacao-Tecnica-USP_Google.pdf>

STI-USP. **TCC | Informações à USP | Aguardando Resposta**, Mensagem recebida por e-mail em 29 de outubro de 2021.

TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, v. 9, n. 1, p. 1–38, 9 maio 2020.

USP, A. DE. **USP faz parceria com Google para uso do G Suite for Education**. Disponível em: <https://jornal.usp.br/institucional/press-release/usp-estabelece-cooperacao-com-a-google-para-uso-dos-recursos-g-suite-for-education/>. Acesso em: 24 nov. 2024.

USP, Assessoria de Imprensa. USP faz parceria com Google para uso do G Suite for Education. **Jornal da USP**, São Paulo, 2016. Disponível em: https://jornal.usp.br/institucional/press-release/usp-estabelece-cooperacao-com-a-google-para-uso-dos-recursos-g-suite-for-education/. Acesso em: 10 out. 2021.

USP; GOOGLE, INC. **Termo de Cooperação Técnica**. 2016a. Disponível em: http://www.sti.usp.br/wp-content/uploads/sites/46/2017/01/USP-Google-Termo_de_Cooperacao_Tecnica.pdf. Acesso em 21/04/2021

USP; GOOGLE, INC. **Contrato Google Apps for Education**. 2016b. Disponível em: http://www.sti.usp.br/wp-content/uploads/sites/46/2017/01/USP-Google-Contrato_do_Google_Apps_for_Education.pdf. Acesso em 15/12/2020

VELIZ, C. **Privacy Is Power: Why and How You Should Take Back Control of Your Data**. Brooklyn, NY: Melville House Publishing, 2022.

WIMMER, M. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. Em: BIONI, B. R. (Ed.). **Tratado de Proteção de Dados Pessoais**. 1. ed. Rio de Janeiro: Forense, 2021.

YURIEFF, K. **Google still lets third-party apps scan your Gmail data**. Disponível em: <https://money.cnn.com/2018/09/20/technology/google-gmail-scanning/index.html>. Acesso em: 25 nov. 2024.

ZANDT, F. **Infographic: Google's Ad Revenue Dwarfs Competitors**. Disponível em: <https://www.statista.com/chart/33017/annual-advertising-revenue-of-selected-tech-companies-offering-search-solutions>. Acesso em: 25 nov. 2024.

11. Sociologia política do direito e sociedade digital: as *fake news* no Brasil

Wanda Capeller[274]

João Pedroso[275]

Andreia Santos[276]

Introdução

As *fake news* constituem um fenómeno político com efeitos no funcionamento da democracia e do Estado de Direito. A disseminação intencional de desinformação, rumores e teorias da conspiração atinge não só a inteligibilidade da política, mas também o funcionamento das instituições democráticas e as formas de participação cidadã que podem ser manipuladas. Este fenómeno não é novo, dado que a instrumentalização e propagação de falsas informações existiram em todos os tempos. Todavia, o advento da sociedade digital criou as condições de sua globalização em razão da superação de suas dimensões espaço-temporais e emergência de *glocalismos políticos digitais*[277]; esta transversalidade tempo-espaço alia-se às novas formas de sua disseminação, não mais piramidais, mas em redes (OST e VAN DER KERCHOV, 2010). A internet e as redes sociais tornaram-se veículos privilegiados da massificação de toda e qualquer informação, sem necessidade de recorrer a meios tradicionais como os jornais, a rádio ou a televisão - os denominados "*old media*" que funcionavam, até

[274] Professora Emérita da Sciences-Po Toulouse, Centre de Théorie et Analyse du Droit, Université de Paris X; Investigadora colaboradora do Centro de Estudos Sociais da Universidade de Coimbra.

[275] Professor da Faculdade de Economia da Universidade de Coimbra e investigador do Centro de Estudos Sociais da Universidade de Coimbra; cocoordenador do Doutoramento em Sociologia do Estado, Direito e Justiça (FEUC/CES).

[276] Socióloga e doutora em Sociologia, no âmbito do Programa de Doutoramento em "Relações de Trabalho, Desigualdades Sociais e Sindicalismo" da Faculdade de Economia da Universidade de Coimbra.

[277] Ver a noção de glocalismo em Roland Robertson (1995, p. 25-44) "*Glocalization: Time-Space and Homogeneity- Heterogeneity*".

então, como *gatekeepers* da informação (cf. CRUZ, 2020). O caráter *rizómico* dessas redes é perceptível em razão da horizontalidade, heterogeneidade e multiplicidade (cf. DELEUZE e GUATTARI, 1980) que determinam suas formas de utilização, divulgação e maximização da informação, de amplo alcance e persuasão (cf. MARTINS e NAIFF, 2023, p. 30). Tal excesso de informação, destituído de qualquer responsabilidade e controlo editorial relativamente à qualidade e veracidade do seu conteúdo, evidencia a falta de reforço das competências digitais e a capacidade de discernir conteúdos originais e fidedignos de informações falsas ou não verificadas (cf. RENDA, 2018).

A conceitualização de *fake news* é evolutiva. Basicamente definida como "notícias intencionalmente falsas, que podem ser verificadas como falsas, podendo enganar os leitores" (cf. ALLCOTT e GENTZKOW, 2017, p. 213), a ideia central é de uma "informação fabricada" que imita conteúdo jornalístico no seu formato, mas não no seu processo organizacional em razão da falta de normas editoriais e processos que facultam informação rigorosa e credível (LAZER *et al.*; CRUZ, 2020). A ênfase é dada ao adjetivo "intencional", o qual torna a ação premeditada, as *fake news* sendo informações falsas intencionalmente divulgadas de modo a atingir interesses de indivíduos ou grupos, assumem três elementos fundamentais: o uso da narrativa jornalística; a falsidade total ou parcial da narrativa; e a intencionalidade de enganar ou criar falsas percepções através da divulgação em rede dessas informações (cf. PIRES, 2022, p. 116). Sua conceitualização exige, igualmente, o exame das formas discursivas, que misturam três noções: desinformação [*disinformation*], informação falsa [*mis-information*] e informação maliciosa [*mal-information*], insistindo na ideia que a desinformação define-se como informação falsa e deliberadamente criada para causar danos a uma pessoa, grupo social, organização ou país[278]; a informação falsa, não é criada com a intenção de causar danos; e a informação maliciosa apresentando-se como informação baseada na realidade, mas usada para causar

[278] O termo "desinformação" foi definido pelo Grupo de Peritos de Alto Nível em *fake news* e desinformação online da União Europeia como todas "as formas de informação falsa, imprecisa ou enganadora que são concebidas, criadas e promovidas para causar intencionalmente dano público ou para lucro" (HILEG, 2018).

danos a uma pessoa, organização ou país (cf. WARDLE e DERAKHSHAN, 2023, p. 28).

Este estudo, centrado no campo político do direito, pretende analisar o impacto causado pelas *fake news*, não somente em termos de suas mutações, mas também de suas novas configurações enquanto espaço aberto do político. Com base na sociologia política do direito (cf. COMMAILLE, 1994), paradigma crítico que situa o direito e a justiça no âmago das ciências da vida social, formulamos a pergunta inicial: podem o direito e a justiça, através da regulação, controlar o impacto massivo das *fake news* no campo socio-político-jurídico? No contexto da nossa análise encontra-se a seguinte tese: a inteligência artificial (IA), ao estruturar de forma rizómica múltiplas comunidades virtuais, gera de maneira exponencial as condições de massificação da desinformação, doravante projetada em escalas glocais. A sociedade digital, baseada na aceleração tecnológica e alienação do mundo social (cf. ROSA, 2014; ZUBOFF, 2019), conduz à de-subjetivação (cf. AGAMBEN, 2007) política, e a falhas na consciência legal dos indivíduos e grupos sociais (SILBEY, 2001).

Essa tese funda-se em cinco premissas, a saber: (1) o Homem, *mendax ab initio*; (2) com a colonização algorítmica da política, a sociedade digital inaugura a sociedade da pós-verdade; (3) as *fake news* desconstroem o mito da neutralidade algorítmica; (4) a ordem digital leva à desordem do Estado de Direito; (5) os problemas globais exigem soluções globais[279] e locais: estudo de caso sobre Direito e Justiça face às notícias falsas no Brasil. Sua análise permite identificar cinco efeitos perversos que, em nossos dias, atingem a sociedade digital, a saber: o *efeito de desordem informativa*, o *efeito de fratura social*, o *efeito de confusão cognitiva*, o *efeito de dissenso político* e o *efeito de exceção no Estado de Direito*.

[279] A título ilustrativo pode mencionar-se o *Digital Services Act*, cujo objetivo é evitar as atividades ilegais e nocivas *online* e a propagação da desinformação na União Europeia (cf. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digitalage/digital-services-act_pt), bem como o designado *AI ACT*, o qual estabelece um regime jurídico uniforme, em particular para o desenvolvimento, a colocação no mercado, a colocação em serviço e a utilização de sistemas de inteligência artificial na União Europeia (cf. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689).

Do ponto de vista metodológico, nossa reflexão adota uma perspetiva interdisciplinar que integra aspectos filosóficos, político-históricos, psicossociológicos e sociojurídicos, todos necessários à apreensão da força política e de desordem social e jurídica das *fake news* nas sociedades contemporâneas. Como estudo de caso destacamos o Brasil, onde as *fake news* tornaram-se um elemento incontornável da análise das perturbações ocorridas no campo político, do direito e da justiça.

Premissa 1 - O Homem, *mendax ab initio*

Desde a Antiguidade buscou-se compreender as razões que levam à mentira política. Em Platão encontramos a ideia de que a responsabilidade político-ética do rei-filósofo não elimina certas técnicas políticas, inclusivamente a mentira. Assim, tanto a República como as Leis justificam o uso da mentira ou do mito (PADREAU, 2004, p. 26), pois recorrer à mentira significa que os homens não são deuses, e que não podem viver como deuses. Segundo o filósofo, há dois tipos de mentira, a "mentira verdadeira" e a "mentira em palavras": a primeira consiste em instalar a ignorância e o erro na alma de quem está sendo enganado. Enganar o ser humano permite extraviar e ocultar as causas da mentira e seus danos. O "mentir em palavras" é uma prática política legítima, reservada aos dirigentes, que devem preservar e consolidar a harmonia da *Polis*. Essa mentira não é vista, portanto, como imoral, mas sim como um ato justo, uma vez que "os amantes do conhecimento podem mentir aos liderados com vistas ao bem de toda a comunidade" (PIOTTE, 1997, p. 23). Também Aristóteles, em sua obra *Retórica*, procura perceber esta faculdade humana de "dizer o que não é", tendo analisado a estrutura psicológica da mentira, suas técnicas e seu contágio (KOYRE, 2004, p. 8).

Em sua visão fenomenológica da mentira, Alexandre Koyré sublinha em *Réflexions sur le mensonge,* texto escrito em 1943, uma das características mais relevantes da mentira política moderna: o de ser produzida em massa e dirigida às massas. Segundo ele, a observação deste fenómeno se baseia em três premissas: "a mentira política nasce com a própria cidade"; as "mentiras políticas

são de todos os tempos"; as "mentiras são armas" (Idem, p. 16)[280]. Neste sentido, a História dá-nos vários testemunhos da relevância das *fake news* em períodos de conflitos de alta intensidade, tais como as guerras. Marc Bloch, em suas *Reflexões de um historiador sobre as notícias falsas da guerra*, escritas em 1921, relata como, através de múltiplas formas, espalhavam-se falsas notícias durante a Primeira Guerra Mundial, desde simples rumores até imposturas e lendas criadas em torno deste acontecimento. Pergunta-se, então, o autor: como nascem? De que elementos tiram sua substância? Como se propagam e ganham amplitude na medida em que passam de boca em boca ou de escrita em escrita? (BLOCH, 1921, p. 11). Para ele, o contágio social das falsas notícias corresponde a anteriores representações coletivas baseadas em um "caldo de cultura" que define o estado de consciência coletiva, que pode ser percebida através da "psicologia do rumor" (idem, p. 25). Como afirmou Koyré (2004, p. 10), nada é mais refinado do que a moderna técnica de propaganda da qual os regimes totalitários fazem amplo uso.

Com efeito, em seu estudo sobre as origens do totalitarismo, Hanna Arendt mostra que a propaganda mentirosa é instrumento de ação dos movimentos totalitários nos espaços sociais não-totalitários. A difusão da propaganda mentirosa é um elemento essencial da "guerra psicológica" (ARENDT, 2002, p. 95). Segundo o testemunho dado por Wolfgang Langhoff em seu livro *Les soldats du marais sous la schlague des nazis: treize mois de captivité dans les camps de concentration (*1935), o regime nazista utilizou o "mentir como normalidade", pois com isso estabelecia uma "normalidade aceita e endossada". Ao referir-se à tortura que ele próprio sofreu, este autor lembra que, poucos dias antes da sua primeira sessão de tortura, Rudolf Hess afirmou: "Elementos judeus e marxistas infiltraram-se nas fileiras da SS e da SA e estão a tentar, através de provocações, prejudicar o prestígio do nosso exército castanho. É indigno de um alemão maltratar prisioneiros indefesos. Os casos de maus-tratos devem ser denunciados e os culpados serão severamente punidos" (cf. MELKEVIK, 2024).

[280] *As Reflexões sobre a mentira* foram publicadas inicialmente em Nova Iorque, no primeiro volume da revista trimestral Renaissance, publicada pela *École libre des Hautes Études* (vol. 1, fascículo 1, janeiro-março de 1943). Edição francesa aqui citada, *Réflexions sur le mensonge*, Paris, Ed. Allia, 2024. Em português, *Reflexões sobre a mentira*, tradução Diogo Paiva, VS. Editor, 2021.

Contudo, a propaganda enganosa não nasceu com os regimes totalitários do século XX, mas sim no coração da democracia liberal norte-americana. Em sua obra *Propaganda* (1928), Edwards Bernays mostra como as democracias enganam a opinião pública com o intuito de gerar consentimento social, notadamente através da manipulação mental das massas[281].

Na época da guerra do Vietnã (1955-1975), Hanna Arendt, em seu texto "A mentira na política: reflexões sobre os Documentos do Pentágono"[282] retoma a análise da mentira política da guerra ao mostrar maneiras não propriamente totalitárias de mentir politicamente, através de técnicas de manipulação e criação de imagens que afectam a opinião pública (cf. JAY, 2010 *apud* NOBRE GAMA, 2019, p. 31). A desinformação e a informação maliciosa são disseminadas com o intuito de manipular e sensacionalizar factos que reforçam a narrativa central e ficcional de modo a obter ganho social, financeiro ou político através de uma distribuição massiva (cf. NORMANDIN, 2022, p. 294). Torna-se, portanto, uma força destrutiva que enfraquece a confiança na política, que passa por três fases – criação, produção e distribuição – e necessita de três elementos – agente, mensagem e intérprete (cf. WARDLE e DERAKHSHAN, 2023). É neste contexto que observamos a complexidade rizômica das *fake news*, dos seus autores e dos seus objetivos, o que representa um dos maiores desafios para o direito e para a justiça. Caracteriza-se, portanto, o *efeito de desordem informacional*, há muito, aliás, observado por autores como Bloch e Arendt (supracitados).

Premissa 2 - Com a colonização algorítmica da política, a sociedade digital inaugura a sociedade da pós-verdade

Cerca de dez anos depois do impulso do neoliberalismo à escala global, Fukuyama no seu livro *O Fim da História e o Último Homem* (1992) lançou as bases teóricas do fim das ideologias, dissolvidas na concepção de democracia global.

[281] Cf. Edição francesa, de 2007.

[282] Inicialmente publicado no *The New York Review of Books*, este texto foi posteriormente incluído no livro *Crises of the Republic; lying in politics, civil disobedience on violence, thoughts on politics, and revolution*, New York, Harcourt Brace Jovanovich, 1972. Cf. *Du mensonge à la violence. Essais de politique contemporaine*, Paris, Calmann Lévy, 5ème édition, 2023, p. 11-68.

Segundo ele, o fim da Guerra Fria marcou a vitória ideológica da democracia e do liberalismo, tendo a doutrina da democracia liberal cancelado as demais ideologias políticas, e a História dos conflitos políticos ideológicos chegado ao fim em razão do consenso universal sobre a democracia. Essa nova ideologia do cancelamento das ideologias serviu para reforçar o credo da supremacia da democracia liberal, que permitiu a afirmação global do anarco-capitalismo (FOUCAULT, 2004, p. 166). Desde então, os conflitos ideológicos centram-se, principalmente, no confronto civilizacional Oriente/Ocidente, o que esvaziou o lugar tradicional do debate político. Neste sentido, Samuel Huntington afirmou que, com o fim da Guerra Fria a "ideologia da cortina de ferro" foi substituída pela "cortina de veludo da cultura" (*apud* ZIZEK, 2014, p. 116). Assim, o "choque de civilizações" tornou-se a política do fim da História (Idem).

Com o advento da "dromo sociedade" (VIRILIO, 1996; 1977), o vácuo político ampliou-se, acentuando a alienação social provocada pelas inovações tecnológicas, interconectadas e interdependentes, que criam espaços de comunicação em rede que produzem, transmitem e recebem informação (cf. CARDOSO *et* al., 2018, p. 6). Esta alienação é reforçada pelos canais digitais de comunicação, onde proliferam as redes sociais com a difusão de conteúdos sem verificação de factualidade e compartilhadas inúmeras vezes (cf. MARTINS e NAIFF, 2023, p. 30). Assim, a internet e os mídia sociais alteram significativamente a forma como a informação é produzida e distribuída, dado o "fácil acesso às tecnologias de edição, publicação e distribuição de conteúdo; consumo de informação público registado pelos media sociais; velocidade na disseminação da informação; informação transmitida em tempo real pelos pares, o que confere credibilidade e maior confiança na partilha com outros pares" (AMARAL e SANTOS, 2019, p. 73).

Neste contexto, é visível a existência de uma injunção política paradoxal: os processos de despolitização das massas, resultantes da desinformação planificada e massificada dos meios de comunicação hegemónicos, geram um processo de repolitização perversa, cuja fonte se encontra no "ressentimento" social, conceito reabilitado por Zizek (2014: 148) que inclui as formas de

ressentimento antiglobalização, que manifestam uma reação às promessas não cumpridas das democracias formais[283]. A desinformação das massas realça as crenças pré-existentes dos leitores, os quais possuem um papel decisivo na tomada de decisão entre o que pode ser verdadeiro ou falso, desconsiderando as informações institucionais (cf. PASCOAL, POLONINI e OLIVEIRA, 2023, p. 36).

É esta colonização algorítmica da política que leva à sociedade da "pós-verdade", ela mesma correspondendo à fase da "pós-política" em que vivemos, expressão definida por Zizek (2014, p. 45) como "uma política que afirma deixar para trás os velhos combates ideológicos para se centrar [...] na gestão e administração especializadas, enquanto a «biopolítica» designa como seu objetivo principal a regulação da segurança e do bem-estar das vidas humanas". Essa mutação no interior do campo político tem um impacto no próprio sentido do político. Segundo Hanna Arendt (2017), esta velha questão já estava presente no pensamento pré-socrático, desde Parmênides (530 – 460 a. C.) e Platão (428/427 a. C. – 348/347 a. C.), não podendo mais ser tratada, nas sociedades contemporâneas, nos termos de *qual é o sentido da política,* mas sim *se a política ainda tem um sentido*. Nos últimos dez anos, de facto, o "sentido da política" se afronta à sociedade da "pós-verdade", fenómeno que se tornou banal e global em razão das estratégias de desinformação, propaganda e mentiras políticas e, também, do funcionamento dos veículos de informação que, ao pleitear pela desregulação massiva da comunicação, aposta na ignorância, na negação do saber e no desrespeito das regras do discurso público (TIERCELIN, 2023, p. 20). Ademais, não se pode ignorar que a proliferação das *fake news* se insere numa guerra de informação que cresceu com a "pós-verdade", isto é, as crenças e emoções passam a ter maior influência na interpretação dos fatos. Este mundo da pós-verdade surgiu em consequência dos seguintes fenómenos: as megatendências societais, o declínio do capital social, a crescente desigualdade

[283] A propósito do conceito de ressentimento, também António Casimiro Ferreira (2019, p. 141-142) afirma que as emoções ligadas ao ressentimento e ao medo traduzem uma desigual distribuição do impacto sociológico das mesmas na condução da vida social, que será tanto mais negativa quanto menores forem os recursos e proteções a que os grupos sociais e os indivíduos tiverem acesso para se posicionarem perante as ameaças.

económica, o aumento da polarização, o declínio da confiança na ciência e um panorama mediático cada vez mais fragmentado (cf. LEWANDOWSKY, ECKER e COOK, 2017).

Na sociedade digital instalou-se uma mentalidade e um sentimento de que toda a verdade é relativa, dado que os factos objetivos são preteridos face a perspetivas subjetivas sobre os mesmos (cf. NORMANDIN, 2022, p. 303; ROCHLIN, 2017). Tal reflete também o modo como o próprio termo "*fake news*" pode assumir significados diferentes dependendo do ponto de vista e da sua utilização por grupos que procuram obter controlo ideológico político e social. Quer isto dizer que membros de lados opostos do debate político definem notícias falsas de uma forma que lhes permite atacar e desacreditar uns aos outros, associando as mensagens internas do grupo à verdade e as mensagens externas ao grupo às notícias falsas (cf. LI e SU, 2020). Neste aspecto, pode-se estabelecer uma correspondência com a teoria do "significante flutuante", isto é, as *fake news* podem ser vistas como um fenómeno social que está a ser usado para articular o ponto de vista do orador e "amplificar as mensagens do grupo", enquanto ataca o "grupo externo" ao "definir a falsidade e atribuir a culpa de acordo com interesses do grupo" (cf. LI e SU, 2020, p. 10-12). Essa tendência das redes sociais digitais para a formação de bolhas de opinião, para a fragmentação das fontes de informação e para a polarização das comunidades epistémicas (cf. SANTOS e VAZ, 2023, p. 25) caracteriza a emergência dos *efeitos de fractura social, dissenso político e de exceção no Estado de Direito.*

Premissa 3 - As *fake news* desconstroem o mito da neutralidade algorítmica

O objetivo do algoritmo é gerar um maior envolvimento do utilizador, filtrando *feeds* de notícias para que estes sejam expostos apenas a informações que reforcem as suas crenças individuais e visão de mundo (cf. NORMANDIN, 2022, p. 305). Tudo o que é apresentado ao utilizador nas redes sociais é controlado por algoritmos, que não somente maximizam o seu interesse, mas também influenciam, preveem e manipulam o seu comportamento, criando inevitavelmente silos ideológicos de divisões políticas e culturais que carecem de

pontos de vista diversificados (idem). Segundo D'Ancona (2017, p. 4), em nossos tempos "a arte da mentira está a abalar as fundações da democracia". De facto, a algoritmização da informação permite que empresas como a Google e o Facebook reúnam dados sobre os hábitos, os interesses e as preferências dos utilizadores para programar algoritmos para fornecer ao *feed* dos mídia sociais dos utilizadores, conteúdo que reflita seus interesses. Por isso os "*echo chambers*" (câmaras de eco), que expõem o indivíduo apenas a opiniões concordantes com a sua, tornou-se uma preocupação no discurso político em países democráticos, dado que a opinião partilhada na câmara é reproduzida vezes sem conta por um determinado grupo da população, provocando lacunas de informação e conhecimento (cf. CRUZ, 2020).

Segundo cientistas políticos como Brendan Nyhan, as convicções tornaram-se um elemento de identidade pessoal, e um laço entre as pessoas que defendem a mesma posição, independentemente do consenso científico que possa existir sobre determinadas matérias (cf. FARIA, 2021). De um ponto de vista psicológico, as motivações que levam as pessoas a acreditar nas *fake news* está relacionada com esta capacidade cognitiva para criar e aceitar informação simbólica, como se da própria realidade se tratasse, ao que acresce o facto de emergirem especialmente durante tempos de incerteza, apresentando-se através de explicações simplistas sobre as situações - "Porque é que X aconteceu, quem beneficiou com isso e quem deve ser culpado" (ORDEM DOS PSICÓLOGOS, 2020). Desta forma, as *fake news* constituem um dispositivo primordial de manipulação política nas sociedades digitais, dado que as percepções são manipuladas para servir os objetivos dos poderosos em detrimento do bem comum, como assinalou Wright Mills (1959, p. 178-179). Quer dizer, as *fake news* alcançam a sua maior projeção face a objetivos políticos.

A título ilustrativo, uma das notícias falsas que ganhou ampla repercussão nos Estados Unidos e no mundo foi o caso apelidado de "Pizzagate". Em 2016, a *Wikileaks* divulgou os e-mails do chefe de campanha de Hillary Clinton, John Podesta, sendo que um nome que apareceu nas mensagens foi o de James Alefantis, dono de uma pizzaria em Washington, um dos arrecadadores de

fundos para o partido Democrata. De acordo com uma reportagem da BBC News (2016), a falsa notícia surgiu quando utilizadores do "*4chan*", um fórum de discussão que se baseia na publicação de imagens e texto, geralmente de forma anónima, publicaram notícias sobre uma suposta rede de pedofilia ligada a Alefantis. O site *Reddit* divulgou um longo documento com supostas evidências da existência dessa rede dias antes das eleições, dando assim ampla repercussão à notícia (BBC, 2016). A teoria conspiratória foi desmentida pelo *The New York Times* e *Fox News*, mas sem conseguir conter a sua disseminação. Segundo uma investigação divulgada pelo *Public Policy Polling*, em dezembro de 2016, 14% dos eleitores de Trump entrevistados acreditavam que Hillary Clinton estava ligada à rede de pedofilia dirigida a partir da pizzaria de Washington, e outros 32% não tinham certeza se era verdade ou não (cf. DELMAZO e VALENTE, 2017). No mesmo sentido, e amplamente conhecido, refira-se o caso da empresa *Cambridge Analytica*, a qual extraiu dados privados de 87 milhões de perfis do Facebook antes das eleições presidenciais americanas de forma a identificar o público-alvo (cf. WECKER, 2022). Através da filtragem de dados da *Cambridge Analytica*, foi identificado o público-alvo, sendo que os utilizadores eram massivamente expostos a notícias falsas, por meio da rede social, neste caso, favorecendo o candidato Donald Trump e prejudicando a sua adversária, a candidata Hillary Clinton. Esta "influência" tem sido assinalada como fator determinante na vitória de Trump.

Assim, ao inserir-se no *backend* de todas as formas de comunicação, a IA torna-se uma força estruturante das interações políticas e sociais (THIEL, 2022). Na verdade, a combinação da IA e a manipulação de *big da*ta pode influenciar vários processos de um Estado democrático de direito (MAGALHÃES, 2023, p. 84), sendo que o tema da desinformação ganha destaque a cada dia por meio de contas e *bots* falsos, "*microtargeting*" psicográfico e *deepfakes* (imagens alteradas) usados para manipular informações para diversos fins (BRKAN, 2019). A IA permite a análise e orientação do discurso público, uma vez que a sua capacidade de observar e analisar enormes quantidades de comunicações e informações em

tempo real permite detectar padrões e reações instantâneos e muitas vezes invisíveis.

Alguns afirmam a neutralidade algorítmica, o que pode ser entendido do ponto de vista estritamente tecnológico; mas o uso político dos algoritmos aponta para a falácia deste argumento, uma vez que a indústria algorítmica, sustentada pelo poder financeiro global, incide sobre o poder político. Consequentemente, a IA tornou-se uma grande força política, apta a criar novas formas poderosas de comunicação, mais subtis e subliminares, permitindo ao grande capital financeiro colocar em risco não somente a soberania dos Estados, como veremos posteriormente, mas também a consciência jurídica das pessoas (SILBEY, 2001). Bloch (cf. 2019: 17) avisou-nos há mais de um século: a massificação da desinformação "perturba os espíritos" ("*trouble les esprits*"). Ao agravar-se, na sociedade digital, a mentira moderna traz o perigo de destruição das faculdades de discernimento dos indivíduos, e consequentemente, a sua capacidade de ação. Neste contexto, observamos a emergência dos *efeitos de confusão cognitiva e dissenso político.*

Premissa 4 – A ordem digital leva à desordem do Estado de Direito

A ideia de Estado de exceção é fonte de estudo da sociologia política, ciência política e sociologia do direito, remetendo, em regra, para o trabalho de Carl Schmitt e para as diferentes formas de flexibilização das normas democráticas e dos princípios do Estado de Direito perante momentos de urgência e necessidade. Mais contemporaneamente, a noção de exceção foi também aprofundada pelo filósofo Giorgio Agamben (1998, p. 27), o qual afirma que "a exceção é uma espécie da exclusão. É um caso particular que é excluído da norma geral. Mas o que caracteriza propriamente a exceção é o facto de aquilo que é excluído não se subtrair absolutamente à relação com a norma; pelo contrário, esta mantém-se ligada à exceção sob a forma da suspensão. A norma aplica-se à exceção desaplicando-se, retirando-se dela. O Estado de exceção não é, portanto, o caos que precede a ordem, mas a situação que resulta da sua

suspensão. Neste sentido, a exceção é verdadeiramente, segundo o étimo, captada fora e não simplesmente excluída".

Nesta esteira, António Casimiro Ferreira (2014, 2019) tem utilizado a noção de exceção para estudar de que modo a regressão do direito democrático corresponde ao enfraquecimento da democracia e ao retrocesso temporal dos valores civilizacionais. Um dos seus argumentos centrais é o de que as linhas de força da relação entre o Estado e o direito é agora crescentemente condicionada pelo retomar da noção de Estado de exceção, fazendo com a que discussão sobre a noção de poder, nomeadamente no que diz respeito à teoria da separação de poderes e ao legítimo exercício do poder democrático, seja marcada pelas diferentes manifestações do poder dos não-eleitos e pelas diferentes formas de constrangimento exógeno (cf. FERREIRA, 2019, p. 306). Desta forma, o "excecionalismo assume uma forma paradoxal de juridificação, positivização e mobilização do direito e da política que força os limites do nosso mundo institucional e normativo, questionando o sentido e as funções do direito, a sua indissociabilidade das expetativas e práticas sociais, e dos bens e valores de justiça que protege" (FERREIRA, 2019, p. 320).

Pode afirmar-se que a sociedade digital dá origem a uma nova configuração entre poder e regulação, onde o poder dos não eleitos (empresas, *big tech*, instituições) entra em confronto com o poder dos eleitos (governos, Estados). As grandes plataformas digitais privadas e globais que recorrem à IA, movimentam-se num espaço social ainda muito pouco regulado, condicionando o próprio poder político e, por essa via, influenciando os processos de tomada de decisão. A "exceção algorítmica" assume-se pelo modo como a desinformação e informação maliciosa interferem no "normal" funcionamento de um Estado de Direito democrático. Trata-se de uma inter-relação entre política, poder e regulação visível nos processos democráticos, como não democráticos, aflorados pelo desenvolvimento da IA, que faz recurso à extrema velocidade da circulação e disseminação das comunicações. Esta arquitetura informacional e os parâmetros de funcionamento das plataformas potencializam conteúdos extremos, provocando vagas de adesão, replicação e de reação humana

atingindo, instantaneamente, milhões de utilizadores (BARBOSA; MARTINS; VALENTE, 2021, p. 9). Esses mecanismos visibilizam ideias e debates anti-democráticos, que, em geral, nada têm a ver com a realidade factual. Por influenciar a opinião pública e desviar o debate democrático, essas estratégias enganosas, à contramão das práticas democráticas, intensificam a violência simbólica e, mesmo, real (cf. PEDROSO, CAPELLER E SANTOS, 2022). Muito recentemente, a desinformação sobre um esfaqueamento provocou ataques islamofóbicos no Reino Unido e confrontos violentos com a polícia por parte de um grupo ligado à extrema direita, após informações falsas sobre o suspeito terem circulado nas redes sociais, sendo que as alegações de que o atacante seria muçulmano, migrante ou refugiado tinham chegado a mais de 27 milhões de pessoas (RIBEIRO, 2024). Segundo o *The Guardian*, um nome começou a correr na internet e surgiram comentários islamofóbicos e apelos a deportações em massa, facto que levou a Secretária de Estado dos Assuntos Internos do Reino Unido a condenar, no Parlamento, a disseminação de informação falsa (idem).

A questão é a de que a disseminação de *fake news* pode criar uma percepção de que os instrumentos convencionais do Estado não são confiáveis, minando o Estado de Direito democrático e a pluralidade política, abrindo espaço para a reafirmação de ideias ultraconservadoras e segregacionistas que assumem crescentemente um carácter de normalidade (cf. MOREIRA e JÚNIOR, 2023). Este é o efeito da exceção no Estado de Direito, a desinformação promove uma espécie de suspensão digital dos princípios democráticos através da manipulação da verdade, que se reflete no mundo real no exercício de direitos, conduzindo a um processo de erosão autofágico do Estado de Direito. Neste aspecto, torna-se visível o efeito *de exceção no Estado de direito.*

Premissa 5 – Problemas estruturais globais, as soluções locais: o direito e a justiça face às *fake news* no Brasil.

O fenómeno das *fake news* apresenta problemas estruturais que dificultam a conceção de intervenções que possam abordar eficazmente os seus efeitos, principalmente, a facilidade com que os seus criadores podem produzir conteúdo

online gerakdo pelos utilizadores e os riscos financeiros para as plataformas que advêm do facto de destacar e divulgar esse material (cf. VERSTRAETE, BAMBAUER E BAMBAUER, 2022). Da mesma forma, os seus criadores podem ter diferentes razões para produzir o conteúdo, o que dificulta uma solução única que seja efetiva para esta questão. Acresce que os próprios consumidores não têm incentivos suficientes para verificar ou questionar o seu conteúdo, em particular, as *fake news* que reforçam as suas perspetivas. Para além disso, as *fake news* estão incluídas num emaranhado de outras histórias que se apresentam como verídicas, o que pode dificultar a rejeição categórica de certas fontes (idem, p. 859).

Um relatório da *Law Library*[284] elaborado em 2019, intitulado "*Initiatives to Counter Fake News in Selected Countries*", sobre formas de combater as *fake news* em diferentes países, elencou quatro principais tipos de abordagem: recurso à legislação existente de regulação dos meios de comunicação social; publicação de legislação específica para as redes sociais, com previsão de sanções económicas e remoção de conteúdos; recurso a legislação e autoridades eleitorais e regulação das plataformas; e, por último, a via da educação dos cidadãos.

A primeira assenta no facto de que na ausência de legislação que aborde expressamente a objetividade das notícias publicadas nas redes sociais, alguns dos países inquiridos aplicam disposições relevantes das leis civis, penais, administrativas e outras leis existentes que regulam os meios de comunicação social, as eleições e a luta contra a difamação, mesmo que estas leis nem sempre reflitam os atuais desenvolvimentos tecnológicos e de telecomunicações. Aqui incluem-se países como o Canadá, o Japão, a Nicarágua, a Suécia e o Reino Unido. A segunda abordagem consiste em promulgar legislação nova e mais direcionada que impõe sanções às redes sociais que espalham notícias falsas, através da aplicação de multas e ordenando a remoção de informações identificadas como falsas. Aqui inserem-se países como a China, o Egito, a França, a Alemanha, Israel, a Malásia e a Rússia. A terceira abordagem assenta no envolvimento das

[284] Cf. https://www.loc.gov/discover/

autoridades eleitorais e das plataformas digitais com o objetivo de assegurar que os eleitores estão informados, seja através da identificação e bloqueio de notícias falsas, do fornecimento de recursos de verificação de factos (*fact-checking*) ao público em geral, ou através da publicação em massa de notícias "reais" durante e após a época eleitoral. Essa pesquisa demonstrou que a Argentina, o Reino Unido, a China e a Malásia seguem esta opção. Por último, alguns países estão, igualmente, a abordar a questão de uma forma mais geral, educando os cidadãos sobre os perigos das notícias falsas, como é o caso da Suécia e do Quénia (cf. LAW LIBRARY, 2019: 1).

Outros autores indicam soluções que englobam três campos principais: controlo de conteúdo, que abrange a remoção e desclassificação algorítmica de páginas, *posts* e contas de utilizadores, prevenindo também que criadores conhecidos de desinformação usem plataformas; a transparência, a qual inclui *fact-checking*, arquivos de publicidade e literacia dos mídia, a qual promove a transparência geral e a consciencialização do utilizador sobre o tema; e a criminalização que envolve sanções, *doxxing* (denunciar publicamente os indivíduos responsáveis) e outras táticas que impõem consequências diretas aos criadores da desinformação (cf. CAMPBELL, 2019). De um modo geral, pode afirmar-se que a criminalização das *fake news* parece ser a solução que permite resultados mais rápidos e que é mais abrangente, dado não depender da colaboração nem das plataformas, nem dos utilizadores, tendo um impacto direto na dissuasão de potenciais criadores de *fake news* (cf. MENESES, 2019: 5-6). A questão que se coloca sobre esta abordagem é se tal pode ser feito sem comprometer a liberdade de expressão, que pode resultar numa forma de censura à expressão do pensamento individual e aos meios de comunicação (PAIVA, 2023; FATHAIGH, HELBERGER, APPELMAN, 2021).

A proliferação das *fake news* torna-se, portanto, uma questão juridicamente e judicialmente relevante. Retomamos a questão inicial: como podem o direito e a justiça dar conta das *fake news*? O desafio do direito e da justiça assenta na aplicação da sua força coercitiva legitimada democraticamente no mundo digital, criando questões sobre o modo de identificação, regulação e, também, punição

de condutas reprováveis na internet e no modo de ação do Estado face aos atores principais na criação e divulgação de *fake news* (cf. PAIVA, 2023; SOARES, 2023). Assim, o direito e justiça buscam soluções para mitigar os efeitos perversos anteriormente enunciados.

Um estudo de caso: turbulências no campo político do Brasil

Em escala local, o estudo do caso brasileiro permite-nos observar as reações dos poderes legislativo e do judiciário no combate às *fake news*. De imediato, o estudo do impacto das *fake news* no campo político brasileiro não pode ignorar que o Brasil é um dos maiores mercados mundiais da plataforma *WhatsApp*, somente atrás da Índia, mas à frente da Indonésia. No *WhatsApp Summit*, em 2023, estimou-se que o Brasil se tornou uma potência digital, contando com 197 milhões de usuários das Apps que formam um vasto ecossistema de milhões de usuários ativos (cf. BEZERRA, 2023). Se esses dados são importantes para o estabelecimento de estratégias de mercado, em termos de cooptação dos usuários, eles são igualmente relevantes para a reflexão sobre a democracia. Se as interconexões ativas, via *WhatsApp* ou outros dispositivos da IA, impulsionam as atividades mercantis, elas impactam igualmente o campo político global e local.

No Brasil, as *fake news* modificaram a agenda político-institucional desde 2014, época de fortes protestos de rua em que 10% das interações no Twitter foram conduzidas por "robôs virtuais". O mesmo ocorreu por ocasião do golpe de Estado institucional de 2016, e em seguida nos períodos de campanha eleitoral para a Presidência da República, em 2018 e 2022 (CPMI, 2019). A título ilustrativo, refira-se a campanha eleitoral de Jair Bolsonaro, quando o candidato afirmou em entrevista na rede nacional num programa televisivo da rede Globo, que Fernando Haddad, seu adversário, teria criado e colocado em circulação de material escolar contra a homofobia no Brasil, a que apelidou de “kit gay”. Bolsonaro afirmou que o livro era “uma coletânea de absurdos que estimula precocemente as crianças a se interessarem pelo sexo”, acrescentando que se “(…)

é uma porta aberta para a pedofilia"[285]. Esta informação foi fortemente divulgada pelas redes sociais, tendo como base a mentira do candidato presidencial Bolsonaro, isto porque não existia nenhum "kit gay", apenas um projeto de iniciativa do poder legislativo, encomendado pela Comissão de Direitos Humanos da Câmara dos Deputados ao Ministério da Educação (MEC) e elaborado por um grupo de ONG's especializadas, em conformidade com as diretrizes de um programa do governo federal lançado anteriormente, em 2004. O material composto por um caderno e peças impressas e audiovisuais, tinha como principal objetivo promover "valores de respeito à paz e à não-discriminação por orientação sexual", não havendo no documento nenhuma orientação que justifique a alcunha "kit gay"[286]. Considerada *fake news*, o Tribunal Superior Eleitoral (TSE) determinou a suspensão de *links* de sites e redes sociais com a expressão "kit gay" usados pela campanha de Jair Bolsonaro para atacar o candidato Fernando Haddad[287]. Um ano após a vitória do candidato de extrema-direita, o WhatsApp admitiu ter permitido a divulgação massiva de mensagens de natureza política (cf. França 24, 2022). No entanto, com o acirrar do debate sobre a regulação das *fake news* no contexto brasileiro, os poderes legislativo e judiciário têm reagido de diversas formas.

A reação do legislativo: criminalização, criação de autoridade de supervisão, responsabilização das empresas tecnológicas e defesa de direitos

O Código Eleitoral (Lei Federal n.º 4.737/1965) sanciona dos artigos 323º a 327º a divulgação e propaganda de fatos falsos em relação a partidos ou candidatos capazes de influenciar; calúnia para fins de propaganda eleitoral (artigo 324.º), ao atribuir-lhe falsamente ato qualificado como delito; difamação de alguém (artigo 325º), agravada se ocorrer no âmbito de propaganda eleitoral ou para fins de propaganda, ao atribuir algo ofensivo à reputação da pessoa;

[285] Cf. https://veja.abril.com.br/politica/tse-manda-tirar-do-ar-fake-news-de-bolsonaro-sobre-kit-gay
[286] Cf. https://exame.com/brasil/haddad-nao-criou-o-kit-gay/
[287] Cf. https://congressoemfoco.uol.com.br/area/pais/tse-diz-que-kit-gay-nao-existiu-e-proibe-bolsonaro-de-disseminar-noticia-falsa/

insulto no âmbito da propaganda eleitoral (artigo 326º). De acordo com o artigo 327º, as penas previstas nos artigos 324º, 325º e 326º são aumentadas de um terço, se for cometido um dos crimes: I – contra o Presidente da República ou chefe de governo estrangeiro; II – contra funcionário público, em razão de suas funções; III – na presença de diversas pessoas, ou por meios que facilitem a difusão do delito. Contudo, parece que estes padrões repressivos permanecem, em geral, na letra da lei. Em 2019, foi introduzida uma alteração à legislação eleitoral, a Lei n.º 13.834/19, de modo a tipificar o crime de denúncia caluniosa com finalidade eleitoral, para quem "comprovadamente ciente da inocência do denunciado e com finalidade eleitoral, divulga ou propala, por qualquer meio ou forma, o ato ou fato que lhe foi falsamente atribuído" (artigo 3º), com pena de dois a oito anos prisão, e multa.

Contudo, vê-se que no direito brasileiro ainda não houve uma adaptação das normas penais ao fenómeno das *fake news*, não existindo uma tipificação específica sobre a criação ou disseminação das mesmas. Todavia, é possível o enquadramento da conduta em alguns dos tipos penais já existentes, como é o exemplo dos crimes contra a honra, ou eleitoral, podendo o autor da elaboração ou disseminação ser criminalmente responsabilizado nesses casos.

Neste cenário, com a proliferação do fenómeno das *fake news* no Brasil, foram apresentados inúmeros projetos de lei, quer pela Câmara dos Deputados, quer pelo Senado Federal, com objetivo de criminalizar a disseminação, ou partilha, de *fake news* na internet, bem como responsabilizar as plataformas digitais na remoção de conteúdos falsos.

O tema tem estado longe do consenso político. Vários projetos lei foram apresentados entre 2017 e 2020, os quais representam um amplo leque do espectro político brasileiro (Partido da Social Democracia Brasileira (PSDB), Partido Social Democrata (PSD), PODEMOS, Partido Popular Sindicalista (PPS), Partido Republicano Brasileiro (PRB), Democratas (DEM), Partido Trabalhista Brasileiro (PTB), CIDADANIA, Partido dos Trabalhadores (PT) e Partido Democrático Trabalhista (PDT)), e que, de forma direta ou indireta, todos foram

apensados ao Projeto Lei n.º 2630/2020[288] (cf. FILHO, CARVALHO E CARVALHO, 2022, p. 9). Em geral, na maior parte dos projetos propostos, os parlamentares optaram por uma abordagem penal, e não pela criação de estratégias de prevenção fundadas na educação e na disseminação de informação, dos quais se destaca o projeto Lei n.º 2630/2020 por problematizar em maior profundidade a questão das *fake news*, bem como prever mais soluções (idem: 11-12). Este projeto lei, também apelidado de "projeto lei das *fake news*", procura instituir a "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet", estando em tramitação desde 2020. A sua autoria é do Senador Alessandro Vieira (PSDB-SE), tendo como relator o deputado federal Orlando Silva (PCdoB – SP).

Os principais pontos do projeto são: proibição da criação de contas falsas nos media sociais para simular a identidade de pessoa ou entidade; proibição de uso de '*bots*', ou seja, contas automatizadas geridas por robôs; limitação do alcance de mensagens muito compartilhadas; assinala que as empresas devem manter o registo de mensagens encaminhadas em massa durante três meses; exige a identificação de utilizadores que patrocinam conteúdos publicados, com o objetivo de evitar anúncios falsos; proíbe que contas oficiais de organizações governamentais ou de pessoas de interesse público (como políticos) bloqueiem contas de cidadãos comuns; criação do Conselho de Transparência e Responsabilidade na Internet, entidade autónoma de supervisão para regulamentar e fiscalizar os provedores; determina que provedoras de redes sociais estabeleçam sedes no Brasil; e impõe sanções ou punições, como advertências ou multas, às empresas que não cumprirem as medidas previstas em lei (cf. HENRIQUE, 2023).

O projeto visa uma série de medidas e impõe responsabilidades às grandes empresas ("*big tech*"), propondo a regulação das plataformas digitais, como a Google, a Meta (Instagram e Facebook), X (ex-Twitter) e TikTok, e serviços de mensagens instantâneas, como o WhatsApp e o Telegram. O ponto principal é

[288] Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334

tornar obrigatória a moderação de conteúdos publicados na internet para que contas ou publicações com conteúdos considerados criminosos possam ser identificadas, excluídas ou sinalizadas. O projeto lei estabelece como objetivos no seu artigo 4º: "I – o fortalecimento do processo democrático e o fomento à diversidade de informações no Brasil; II – a garantia da transparência dos provedores em relação a suas atividades com o usuário, incluindo a elaboração e modificação de seus termos de uso, critérios de moderação e recomendação de conteúdos e identificação de conteúdos publicitários; III – o exercício do direito do usuário à notificação, ao contraditório, ampla defesa e devido processo em relação à moderação de conteúdos; IV – o fomento à educação para o uso seguro, consciente e responsável da internet como instrumento para o exercício da cidadania; V – proteção integral e prioritária dos direitos fundamentais das crianças e adolescentes; e VI – o incentivo a um ambiente livre de assédio e discriminações."

Este projeto tem sido comparado ao *Digital Services Act* da União Europeia[289], aprovado em 2022, e com aplicação desde fevereiro deste ano, sendo considerada uma das mais avançadas em matéria de regulamentação de serviços digitais. Com base principalmente em questões de transparência dos processos de moderação de conteúdo e dos riscos sistémicos, coloca sobre as plataformas a responsabilidade de definir protocolos de ação para diminuir o risco do serviço que oferecem (cf. PINOTTI, 2023). Em comparação com o projeto lei, ambos prosseguem a mesma responsabilização das plataformas, bem como o compromisso com a transparência (idem). Em escala global, no entanto, os interesses financeiros e as "*big tech*" têm oferecido grande resistência face ao projeto de lei no Brasil, nomeadamente a Alphabet, empresa controlada pela Google, que colocou um anúncio na sua página inicial de busca, no Youtube, e ainda no jornal local "Folha de S. Paulo", de modo a influenciar a opinião pública contra a sua aprovação, sendo acusada pelo governo e pelo judiciário brasileiro de interferência indevida no debate no Congresso (PAUL, 2023). A perspetiva

[289] Cf. https://www.consilium.europa.eu/en/policies/digital-services-act/

das "*big tech*" é a de que o projeto coloca em risco a liberdade de expressão dos utilizadores, temendo igualmente as punições em caso de não cumprimento da lei. A título de exemplo, numa publicação do deputado federal Nikolas Ferreira (PL-MG) nas redes sociais alegando, entre outras coisas, que "a liberdade de expressão está sobre severo ataque", o empresário Elon Musk, respondeu ao deputado com um sinal de exclamação, demonstrando a sua concordância[290].

Ao lado das "*big tech*", estão também os seus opositores políticos, que apelidam o projeto lei de "Projeto Lei da Censura". Os parlamentares mais à direita, opositores do governo do presidente Lula da Silva (PT), são contra a sua aprovação criticando a proposta pelo atentado à liberdade de expressão dos utilizadores nos mídia sociais, pois acreditam que este poderá enquadrar conteúdos como "discurso de ódio" e até excluir as publicações das plataformas (HENRIQUE, 2023). Para além disso, também afirmam que a limitação dos aplicativos de mensagens de distribuição de conteúdos em massa poderá afetar as suas bases de seguidores, dado que, segundo os próprios, os seus conteúdos são frequentemente alvos de investigação de agências de *fact checking* e, por conseguinte, classificados como falsos ou fora de contexto (idem). Por oposição, do lado político mais à esquerda, a visão é a de que o projeto de lei irá criar mecanismos para que as plataformas excluam conteúdos que geram "desinformação" e penalizem o compartilhamento de conteúdos de discursos de ódio. Mais recentemente, e devido a todo este debate, o presidente da Câmara dos Deputados, anunciou a criação de um grupo de trabalho para debater um novo projeto de regulação das redes sociais, deixando incerto o destino do projeto de lei (MARQUES, 2024). Neste contexto, no legislativo brasileiro são dominantes as tensões entre *o efeito do dissenso político* e da mitigação do *efeito da exceção no Estado de direito.*

[290] Aliás, o empresário tem sido um dos grandes opositores ao projeto de lei, estando igualmente envolvido na resposta do judiciário, como veremos mais adiante.

A reação do judiciário: aliança no enfrentamento da desinformação, a defesa do STF e investigação aos atos antidemocráticos

O Tribunal Superior Eleitoral (TSE) pronunciou-se muito rapidamente, em 2018, decidindo pela proibição da divulgação de mensagens políticas de natureza sexual ou sexista. Posteriormente, em 2020, o TSE também instituiu o "Projeto de Enfrentamento à Desinformação" em parceria com 45 instituições, entre partidos políticos, plataformas digitais e servidores de mensagens. O objetivo deste projeto foi compreender o fenômeno das notícias falsas a partir de uma visão global e multissetorial, considerando sua tendência à perpetuação. Entre as entidades associadas a este Projeto, encontraremos o Ministério Público (Ministério Público Federal), o Gabinete de Segurança Institucional da Presidência da República, o Tribunal de Contas, e ainda Google, Facebook, Twitter e WhatsApp. O Tribunal Superior Eleitoral também uniu forças com o Grupo Multissetorial de Controle de Informações e Combate às Notícias Falsas, lançado pelo CNJ e pelo Supremo Tribunal Federal, cujo objetivo é alertar os internautas sobre os perigos do compartilhamento de informações questionáveis, ensinando-os a verificar a veracidade das informações que recebem.

Apesar dessas complexidades e das dificuldades no combate às informações falsas, o sistema judiciário brasileiro tem tomado diversas medidas para controlar esse fenômeno, principalmente a partir de 2019. Todavia, para entender a reação do judiciário brasileiro às *fake news*, é necessário compreender o contexto onde tal se desenvolve.

De modo muito breve, entre 2018 e 2019, o Supremo Tribunal Federal (STF), tomou decisões quanto à operação "Lava Jato" que teve início em 2014 pela Polícia Federal, nomeadamente, contra o entendimento alcançado em 2016 – prisão após condenação em segunda instância, de vários atores políticos– sendo favorável à libertação de alguns presos durante as operações. A operação "Lava Jato" contou com imenso apoio popular, sendo designada como a maior do género no combate à corrupção do país, tendo como alvo, também, grandes empresários do setor das infraestruturas, agentes do mercado financeiro e funcionários públicos brasileiros (LUSA, 2024). No entanto, em 2019, conversas

em aplicativos de mensagens, que se tornaram públicas a partir de reportagens do *site The Intercept Brasil*, indicaram que os procuradores da "Lava Jato" mantiveram diálogos ilegais com o Juiz Sérgio Moro, o qual liderou as investigações em primeira instância e deixou a magistratura para se tornar ministro da Justiça no Governo do ex-presidente Jair Bolsonaro. Essas revelações deram início a uma avalanche de revisões de decisões judiciais, principalmente, no STF, incluindo a libertação e a anulação dos processos contra Lula da Silva (idem). Para além disso, o discurso anti-sistema ganhou relevância com a eleição do novo governo encabeçado por Jair Bolsonaro, que desde a sua posse enfrentou resistência a algumas das suas bandeiras por parte do Congresso Nacional e do STF, os quais se tornaram alvo de manifestações dos seus apoiantes.

O STF ganhou, assim, protagonismo, fazendo com que "fosse chamado a verdadeiramente criar o direito pela via interpretativa-argumentativa, apresentando decisões constitucionais para os mais profundos dissensos políticos (…)" (LORENZETTO e PEREIRA, 2020, p. 182). Tal teve duas consequências principais: o STF tornou-se objeto de interesse social e mediático; e consequentemente, devido a este "escrutínio" das suas decisões, passou a colecionar desafetos (idem: 183). Neste cenário, no dia 13 de Março de 2019, o Procurador da República, Diogo Castor de Matos, ligado à Operação "Lava Jato", publicou um artigo no jornal "O Antagonista" onde abertamente assinala que a ação do STF tem como objetivo tentar transferir investigações de corrupção para a Justiça Eleitoral, afirmando que "*Embora poucos tenham percebido, há algum tempo vem sendo ensaiado na Segunda Turma do STF o mais novo golpe à Lava Jato (…) Agora, como no Brasil todo político corrupto pede propina a pretexto de uso em campanhas políticas, se o entendimento da turma do abafa sobressair, praticamente todas as investigações da Lava Jato sairiam da Justiça Federal e iriam para Justiça Eleitoral* (…)[291]". O artigo despoletou uma tensão entre o Ministério Público e o poder judiciário, e no dia seguinte, a 14 de Março de 2019, o até então Presidente do

[291] Disponível em: https://oantagonista.com.br/brasil/procurador-da-lava-jato-denuncia-o-mais-novo-golpe-stf/

STF, o ministro Dias Toffoli, publicou a portaria GP n.º 69[292], que com base no artigo 43º, do Regimento Interno do STF[293], e instaurou o Inquérito identificado com o n.º 4.781, designado de "Inquérito das *fake news*". Este inquérito teve como objetivo investigar "a existência de notícias fraudulentas (*fake news*), denunciações caluniosas, ameaças e infrações revestidas de *animus caluniandi*, *diffamandi* ou *injuriandi*, que atingem a honorabilidade e a segurança do Supremo Tribunal Federal, de seus membros e familiares. No seguimento, foi nomeado para seu relator o ministro Alexandre de Moraes.

Porém, a forma como foi instaurado o inquérito e a condução da sua investigação tem sido alvo de críticas. As críticas mais recorrentes refletem-se no pedido por ofício da Procuradoria-Geral da República (PGR) de esclarecimentos sobre o mesmo, afirmando que o inquérito carecia de definição dos fatos concretos a serem investigados e também de justificativa da competência do STF para proceder à abertura do inquérito sem participação da PGR ou sequer abertura de vistas ao Ministério Público[294]. Tal encontra fundamento no facto de que, por princípio, a investigação criminal cabe à Polícia Judiciária e ao Ministério Público, na lógica do sistema acusatório. Para além disso, o procedimento não estaria de acordo com o artigo 67º, do regime Interno do STF, sobre o processo de distribuição na Corte depender de sorteio eletrónico a fim de garantir o princípio do juiz natural, tendo sido atribuído diretamente ao ministro Alexandre de Moraes (cf. LORENZETTO e PEREIRA, 2020, p. 187).

No âmbito da investigação, o ministro Alexandre de Moraes decretou medidas para bloquear contas de internet que propagassem discurso de ódio contra a Corte, com base em suspeitas de que essas ações nas redes sociais estariam a ser pagas por grupos que queriam desestabilizar o Judiciário[295]. No mesmo sentido, foram emitidos mandados de busca e apreensão, sendo

[292] Disponível em: https://www.conjur.com.br/dl/co/comunicado-supremo-tribunal-federal1.pdf

[293] Artigo 43º - "Ocorrendo infração à lei penal na sede ou dependência do Tribunal, o Presidente instaurará inquérito, se envolver autoridade ou pessoa sujeita à sua jurisdição, ou delegará esta atribuição a outro Ministro".

[294] Disponível em: https://www.migalhas.com.br/arquivos/2019/3/art20190315-11.pdf

[295] Cf. https://www.conjur.com.br/2019-mar-22/alexandre-moraes-manda-bloquear-perfis-atacaram-stf/

determinado o bloqueio do Twitter (na altura), do Facebook, do Instagram e até do WhatsApp dos investigados[296]. O ministro do STF ordenou, também, que fossem retirados artigos que mencionavam o presidente do STF, ganhando críticas de várias entidades da sociedade civil, como a Ordem dos Advogados do Brasil, e associações representantes de jornalistas, os quais classificaram o ato como uma censura à liberdade de imprensa[297]. Esta acusação foi recusada veementemente por Alexandre de Moraes, revogando a medida (idem).

A questão da sua constitucionalidade ganhou destaque, reunindo argumentos a favor e contra. A título de exemplo, por um lado, Aury Lopes Jr. e Alexandre Morais da Rosa (2019), pugnaram pela inconstitucionalidade do inquérito, argumentando que o "(…) perigo de se atribuir a instituições não previstas expressamente em lei o poder de investigar é o de se dar o fenômeno da cegueira deliberada das provas que não são interessantes à estratégia eleita, por efeito da dissonância cognitiva. É importante certo afastamento objetivo, subjetivo e cognitivo do Estado-investigador, sob pena de sedução pelas hipóteses imaginadas, aplicando-se o que foi dito sobre heurísticas e vieses". A inconstitucionalidade foi afirmada, igualmente, pela procuradora-geral da República, Raquel Dodge, que pediu o seu arquivamento, mas sem sucesso (CRUZ, 2019).

Por outro lado, Lenio Luiz Streck, Marcelo Andrade Cattoni de Oliveira e Diogo Bacha e Silva (2020), defenderam a constitucionalidade da investigação, rebatendo que "(…) em primeiro lugar, há um caso explícito de atentado à própria jurisdição do STF (e isso atinge os princípios da democracia e da República), fazendo com que o próprio STF deva eliminar o contempt of court; em segundo, em um ambiente virtual, a velha noção de um local físico não faz mais sentido, embora o próprio § 1º do art. 43, do RISTF, autorize ao Presidente do Tribunal agir de acordo com o disposto no caput do mesmo artigo, mesmo quando a infração não se dê nas dependências físicas do STF. Ainda há um

[296] Cf. https://olhardigital.com.br/2019/04/16/noticias/alexandre-de-moraes-manda-bloquear-redes-sociais-de-7-suspeitos-de-atacar-o-stf/
[297] Cf. https://www.bbc.com/portuguese/brasil-52824346

terceiro elemento: está-se a tratar de dois órgãos dos quais não cabem recursos: o STF e a PGR. Por isso o RISTF se apresenta como um remédio nas hipóteses nas quais quem deveria defender o STF de um contempt of court não o faz (…)".

O inquérito das *fake news* teve também impacto no Congresso, que instalou uma Comissão Parlamentar de Inquérito (CPMI) sobre o assunto. A CPMI foi dominada pela oposição e ex-aliados que romperam com Bolsonaro, em que parte das investigações chegaram a Moraes, sobretudo a história de que haveria um "gabinete do ódio", composto por assessores de Bolsonaro no Palácio do Planalto, que espalhavam memes e mentiras contra os seus desafetos nas redes sociais[298]. O inquérito das *fake news* teve "ramificações", sendo que, em 2020, e já com um novo procurador-Geral da República, Augusto Aras, e devido a manifestações com a eventual participação de parlamentares contra o STF, o Congresso e em defesa da ditadura militar, foi aberto novo inquérito para investigar "atos antidemocráticos" (Inquérito n.º 4.828). No seguimento, Alexandre de Moraes determinou a quebra dos sigilos bancários de deputados e um senador bolsonaristas, que seriam imprescindíveis "na verificação da existência de organizações e esquemas de financiamento de manifestações contra a Democracia"[299]. Entre vários desenvolvimentos, no final de julho de 2021, a PGR pediu o arquivamento do inquérito dos atos antidemocráticos. O ministro do STF concordou, porém, abrindo um novo inquérito, denominado de "inquérito das milícias digitais" (inquérito n.º 4.874), cujo objeto seria a investigação de uma organização criminosa dividida em núcleos de produção, financiamento, divulgação de "notícias fraudulentas" contra as instituições democráticas, com o foco em militantes e influenciadores de direita. Nesta investigação inclui-se a invasão de 8 de janeiro de 2023, do Palácio do Planalto, o Congresso e o Supremo Tribunal Federal (STF), por parte de apoiantes radicais do ex-presidente Bolsonaro (PL), que insatisfeitos com a eleição e posse do presidente Lula da Silva (PT), afirmaram-se contra a confiabilidade das urnas

[298] Cf. https://www.gazetadopovo.com.br/republica/ha-cinco-anos-inquerito-das-fake-news-persegue-quem-ousa-se-opor-ao-stf/

[299] Cf. https://g1.globo.com/politica/noticia/2020/06/15/entenda-inquerito-do-stf-sobre-manifestacoes-antidemocraticas.ghtml

eletrónicas, questionando a legitimidade da eleição presidencial e pedindo a "intervenção militar" (SCHREIBER, 2024). Os invasores foram denunciados por tentativa de golpe de Estado, tentativa de abolir o Estado Democrático de Direito, associação criminosa, dano ao património tombado e depredação de bens públicos. A investigação assenta também sobre os financiadores e instigadores do ato, estando aqui incluído, Jair Bolsonaro, suspeito de ser o mentor intelectual da manifestação (idem).

Mais recentemente, em abril de 2024, o empresário Elon Musk, detentor da rede "X" (antigo Twitter) foi também incluído no inquérito das milícias digitais, no seguimento de uma série de *posts* com críticas contra o ministro Alexandre de Moraes, acusando o magistrado de atentar contra a liberdade de expressão ao determinar o bloqueio de utilizadores investigados e ameaçando não cumprir ordens do STF quanto à suspensão das contas (RIBEIRO e MENESES, 2024). Segundo a decisão proferida por Moraes: "A conduta do X configura, em tese, não só abuso de poder econômico, por tentar impactar de maneira ilegal a opinião pública mas também flagrante induzimento e instigação à manutenção de diversas condutas criminosas praticadas pelas milícias digitais investigadas no INQ 4.874, com agravamento dos riscos à segurança dos membros do Supremo Tribunal Federal"[300]. Esta polémica, por sua vez, deu novo destaque à temática da regulação das redes sociais, opondo membros do governo do Congresso Nacional que voltaram a defender a necessidade de se aprovar a regulação das plataformas digitais no Brasil, contra os líderes da oposição que saíram em defesa do dono da plataforma X, reforçando a tese de censura e de violação da liberdade de expressão[301].

No seguimento, a 30 de agosto de 2024, o ministro Alexandre Moraes ordenou a retirada imediata da plataforma X no Brasil, por falta de cumprimento das ordens judiciais proferidas pelo ministro, nomeadamente, a recusa em bloquear perfis de pessoas sob investigação, o pagamento das respetivas multas

[300] Disponível em: https://www.conjur.com.br/wp-content/uploads/2024/04/Decisao-4874-Assinada.pdf

[301] Cf. https://agenciabrasil.ebc.com.br/politica/noticia/2024-04/lira-anuncia-grupo-para-propor-nova-versao-do-pl-das-fake-news

e a falta de nomeação de pessoa física ou jurídica representante em território nacional (Prazeres, 2024). Pode ler-se na decisão[302] que "*A flagrante conduta de obstrução à Justiça brasileira, a incitação ao crime, a ameaça pública de desobediência as ordens judiciais e de futura ausência de cooperação da plataforma são fatos que desrespeitaram a soberania do Brasil e reforçam à conexão da DOLOSA INSTRUMENTALIZAÇÃO CRIMINOSA DAS REDES SOCIAIS, (…) as condutas ilícitas foram reiteradas na presente investigação, tornando-se patente o descumprimento de diversas ordens judiciais pela X BRASIL, bem como a dolosa intenção de eximir-se da responsabilidade pelo cumprimento das ordens judiciais expedidas, com o desaparecimento de seus representantes legais no Brasil para fins de intimação (…)*". Denota, ainda, que "*ELON MUSK confunde LIBERDADE DE EXPRESSÃO com uma inexistente LIBERDADE DE AGRESSÃO, confunde deliberadamente CENSURA com PROIBIÇÃO CONSTITUCIONAL AO DISCURSO DE ÓDIO E DE INCITAÇÃO A ATOS ANTIDEMOCRÁTICO*". Em resposta, a rede social afirmou, ainda na noite de quinta (29 de agosto), que não cumpriria ordens de Moraes e dizia esperar o bloqueio no Brasil, recusando acatar as ordens e acusando o judiciário brasileiro de ser uma ameaça à democracia[303].

A decisão viria a ser confirmada pela 1ª Turma do STF, pelos ministros Flávio Dino, Cristiano Zanin, Cármen Lúcia e Luiz Fux, que foi o único que acompanhou o voto do relator com ressalvas (Higídio e Angelo, 2024). Para o ministro Flávio Dino[304], a empresa "despreza a ética" quando "efetua ou protege agressões, recusa-se reiteradamente a cumprir ordens judiciais, foge deliberadamente das suas responsabilidades legais (…)", subinhando que

[302] Disponível em: https://www.conjur.com.br/wp-content/uploads/2024/08/PET-12404-Assinada.pdf

[303] A este propósito, refira-se que em pelo menos dois casos semelhantes, na índia e na Turquia, por exemplo, as autoridades determinaram a retirada de perfis e conteúdo considerado inapropriado e, apesar de uma resistência inicial, o X acabou por cumprir as determinações. Logo, a decisão inversa no Brasil, conduz ao questionamento da resistência por parte da rede X às ordens do STF. Segundo a BBC News Brasil, esta postura baseia-se numa conjunção de fatores, entre eles, o apoio que Musk tem por parte da direita brasileira, o que cria condições para que Musk desafie o STF na medida em que oferece suporte político para essa posição; e o facto de conciliar a bandeira do direito à liberdade de expressão com seus interesses econômicos, como é visível nos seus negócios bilionários com países considerados autoritários, por exemplo, com a China e a Arábia Saudita (Prazeres, 2024a).

[304] Disponível em: https://www.conjur.com.br/wp-content/uploads/2024/09/voto-Dino-bloqueio-X.pdf

"governança digital pública é essencial, num cenário de monopolização e concentração de poder nas mãos de poucas empresas". Por sua vez, Cristiano Zanin[305], afirmou que "O reiterado descumprimento de decisões do Supremo Tribunal Federal é extremamente grave para qualquer cidadão ou pessoa jurídica pública ou privada. Ninguém pode pretender desenvolver suas atividades no Brasil sem observar as leis e a Constituição". Para a ministra Carmen Lúcia[306] "Não se baniu empresa no Brasil na decisão em exame, não se excluiu quem quer que seja de algum serviço que seja legitimamente prestado e usado. Exigiu-se o cumprimento do Direito em benefício de todas as pessoas, por todas as pessoas naturais ou jurídicas, nacionais e não nacionais". Quanto a Luiz Fux[307], realça que acompanha "o Ministro relator com as ressalvas de que a decisão referendada não atinja pessoas naturais e jurídicas indiscriminadas e que não tenham participado do processo, em obediência aos cânones do devido processo legal e do contraditório, salvo se as mesmas utilizarem a plataforma para fraudar a presente decisão, com manifestações vedadas pela ordem constitucional (…)". Também o presidente do STF, o ministro Luís Roberto Barroso, mostrou apoio à decisão dado que "A atitude de retirar a representação para não ter que cumprir ordens judiciais e para não ter que observar a legislação brasileira é um comportamento que não seria aceitável em qualquer lugar do mundo. Portanto, não há nada de excepcional, salvo uma politização indevida" (Richter, 2024).

Contudo, existem também vozes dissonantes que contestam a decisão. A título de exemplo, a Associação Nacional de Jornais (ANJ) do Brasil, com 97 jornais associados, manifestou uma "profunda preocupação com as restrições ao trabalho da imprensa diante da proibição do STF de acesso à rede social X mesmo por meio de VPN [rede privada virtual] e da ameaça de multa a veículos [de imprensa]" (Lusa, 2024). A associação refere que tem recebido várias queixas por falta de acesso "a visões, relatos e pensamentos de diferentes fontes de notícias, dentro e fora do Brasil" (idem). A suspensão da Rede X foi, igualmente, tema da

[305] Disponível em: https://www.conjur.com.br/wp-content/uploads/2024/09/voto-Zanin-bloqueio-X.pdf
[306] Disponível em: https://www.conjur.com.br/wp-content/uploads/2024/09/6264615.pdf
[307] Disponível em: https://www.conjur.com.br/wp-content/uploads/2024/09/6264645.pdf

audiência pública promovida pela Comissão de Assuntos Econômicos (CAE), onde diferentes vozes se pronunciaram sobre as consequências da decisão. Para Sergio Moro (União-PR), as decisões são desproporcionais porque prejudicam mais de 20 milhões de usuários brasileiros do X que não incorreram em ilegalidades; para o economista Paulo Rabello de Castro, o X é crucial na comunicação internacional e no acesso a informações de diversos setores profissionais; para o senador Marcos Rogério (PL-RO), a suspensão da rede provoca um impacto indireto nas decisões de outras empresas, com a potencial consequência de redução de investimentos no país; o especialista em tecnologia Arthur Igreja criticou a falta de critérios objetivos e regras claras nas decisões judiciais que envolvem plataformas de redes sociais; e o representante do instituto Artigo 19 Brasil, André Boselli, afirmou que o Judiciário brasileiro não tem parâmetros muito claros sobre liberdade de expressão em razão de uma omissão legislativa, havendo o risco de os juízes passarem "a decidir sobre algo que não foi objeto de legislação" (Agência Senado, 2024).

A análise acima demonstra a dificuldade, mas também a possibilidade de reagir contra as *fake news* e o seu efeito nas instituições democráticas. No caso brasileiro, a unidade do judiciário na sua defesa institucional consegue reagir por meio do direito e dos procesos judiciais, encontrando uma justificação para regular e limitar a liberdade de expressão. Todavia, face ao impacto das novas tecnologias e o seu rápido e exponencial desenvolvimento, pode afirmar-se que o agir do direito e da justiça, na sua produção e aplicação, em combater as *fake news* estará, por ora limitado, em função dos *efeitos perversos do dissenso político e da exceção no Estado de direito* que, apesar das iniciativas referidas, também se refletem no legislativo e no judiciário brasileiro.

O caso entre a rede X e o Brasil indica a emergência de uma nova problemática da maior importância para a sociologia política do direito: a da questão da soberania digital. Em um contexto global, onde o poder das empresas busca prevalecer sobre o poder dos Estados, batalha que se estabeleceu entre as altas tecnologias e as democracias, está a ameaçar as soberanias estatais (Osava, 2024). Neste sentido, lembramos a recente afirmação de Elon Musk sobre a

Bolívia por causa do lítio, que alimenta as baterias dos veículos Tesla: "vamos dar um golpe em quem quisermos"![308] Neste embate entre democracia e monopólios da rede, torna-se visível que e**ssa** questão é mais política do que jurídica, uma vez que se "a internet está a democratizar-se, o problema não é a internet, mas o sistema de algoritmos das plataformas, que são braços do neoliberalismo e respondem aos interesses dos Estados Unidos" (cf. Lefevre *apud* Osava, 2024).

Em Carta Pública intitulada "*Against Big Tech's Attack on Digital Sovereignties*", várias personalidades de relevo internacional expressaram sua "profunda preocupação com os contínuos ataques de grandes empresas de tecnologia e seus aliados contra a soberania digital do Brasil". Os signatários desta Carta[309] afirmaram que "a disputa do governo brasileiro com Elon Musk é apenas o exemplo mais recente de um esforço mais amplo para "restringir a capacidade de nações soberanas definirem uma agenda de desenvolvimento digital livre do controlo de megacorporações sediadas nos Estados Unidos". Para eles, "todos aqueles que defendem valores democráticos devem ficar ao lado do Brasil em sua busca pela soberania digital. Exigimos que as empresas de Big Tech cessem suas tentativas de sabotar as iniciativas do Brasil voltadas para a construção de capacidades independentes em inteligência artificial, infraestrutura pública digital, gerenciamento de dados e tecnologia de nuvem. Esses ataques minam não apenas os direitos dos cidadãos brasileiros, mas as aspirações mais amplas de cada nação democrática de alcançar a soberania tecnológica" (cf. Pascual, 2024). Ora, os ataques à soberania digital dos Estados traz à luz a importância da reflexão aqui iniciada, sobre o papel essencial do direito e da justiça no controle da esfera digital pública, na medida em que são, por excelência, os dispositivos mais eficazes para minimizar aos abusos do capitalismo digital.

---

308 Cf. https://exame.com/negocios/daremos-golpe-onde-quisermos-diz-musk-apos-insinuacoes-sobre-a-bolivia/

309 Thomas Piketty, Yanis Varoufakis, Shoshana Zuboff, entre muitos outros importantes ensaístas e atores políticos.

Elementos conclusivos

A partir dos *modelos* e *movimentos* que caracterizam a sociedade digital, devemos reter o fato de sua virtualização massificada, através da qual as *fake news*, disseminadas coletivamente, atingem frontalmente o(s) campo(s) político, do direito e da justiça. Nele, as desinformações são intencionalmente fabricadas em massa e para as massas, circulando de maneira rizômica, complexa e *glocal*, com projeções para além da dimensão espaço-temporal, o que caracteriza os sistemas de IA. A *Polis* classicamente concebida como o espaço público da comunicação interpessoal e coletiva, visando o bem comum e a afirmação da democracia, torna-se, sob o impacto das *fake news*, um espaço político desordenado e obscuro. As redes virtuais podem constituir, simultaneamente, lugares abertos para a expressão democrática e, ao mesmo tempo, podem tornar-se uma ferramenta das desordens anti-democráticas, onde a desinformação *das fakes news* cria as condições para a emergência dos neofascismos virtuais. De facto, na sociedade digital, avultam os efeitos de desordem que pervertem a vida política e social, tal como acima verificamos: o *efeito de desordem informativa*, o *efeito de fractura social*, o *efeito de confusão cognitiva*, o *efeito de dissenso político e o efeito da exceção no Estado de Direito*. Em nossa argumentação, ilustrada pelo estudo do caso brasileiro, constatamos as dificuldades encontradas pelo direito e pela justiça em minimizar as consequências políticas das *fake news*. No Brasil, tanto o poder legislativo quanto o poder judiciário encontram-se, eles mesmos submergidos nas teias das redes digitais, atacados por este fenómeno, onde as questões da luta política, do anonimato e a atual fragilidade da regulação e da possibilidade da imputação da responsabilidade penal deixam pouca margem para seu controle efetivo.

A sociologia política do direito também enfrenta esses desafios. O ritmo vertiginoso da evolução da IA, e a revolução silenciosa e de aceleração que promove, obrigam a um permanente movimento de renovação epistemológica dos estudos sociojurídicos, o que facilitará uma melhor apreensão desses factos, neste caso das *fake news*, pelas instituições existentes (ou a criar), que devem tratar da sua regulação e, quando necessário, da sua sanção. Assim, nas sociedades

digitais, o direito e a justiça, nos seus processos de produção e aplicação, são chamados a dar um salto paradigmático que a era da pós-verdade exige para poder resolver a seguinte equação: ação individual > ação coletiva> ação de massa. O reforço da democracia e do Estado de Direito exigem iniciativas nos campos social, económico, político, do direito e da justiça, de educação, de prevenção, de regulação e de sanção, com recurso à aplicação do Direito vigente e ao funcionamento das instituições existentes, bem como a autorregulação, a hetero-regulação, a produção de "novo" direito e de novas instituições promotoras de relações sociojurídicas que anulem, ou mitiguem, as desordens e efeitos supra identificados. Como a IA não é apenas uma questão tecnológica, é preciso ressaltar o facto de que a aceleração tecnológica e a alienação causam mutações, tanto ao nível da racionalidade política, como jurídica, quanto ao nível ontológico. Ou seja, nas maneiras de pensar e sentir os lugares do político e do jurídico nas sociedades contemporâneas. O tema fica em aberto.

Referências bibliográficas

AGAMBEN, Giorgio. **Homo Sacer – Sovereign Power and Bare Life**. Stanford, CA: Stanford University Press, 1998.

AGAMBEN, Giorgio. **Qu'est-ce qu'un dispositif?** Paris: Payot & Rivages, 2007.

AGÊNCIA DO SENADO. CAE: debatedores discordam sobre impacto da suspensão do X no Brasil. **Agência do Senado**, 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/09/10/cae-debatedores-discordam-sobre-impacto-da-suspensao-do-x-no-brasil. Acesso em 12 set 2024.

ALLCOTT, Hunt; GENTZKOW, Matthew. Social Media and Fake News in the 2016 Election. **Journal of Economic Perspectives**, v. 31, n. 2, p. 211–236, 2017.

AMARAL, Inês; SANTOS, Sofia José. Algoritmos e redes sociais: a propagação de fake news na era da pós-verdade. *In:* FIGUEIRA, João e SANTOS, Sílvo (orgs.). **As fake news e a nova ordem (des)informativa na era da pós-verdade:** Manipulação, Polarização, Filter Bubbles. Coimbra: Imprensa da Universidade de Coimbra, 2019, p. 63-86

ARENDT, Hannah. **Crises of the Republic; lying in politics, civil disobedience on violence, thoughts on politics, and revolution**. New York: Harcourt Brace Jovanovich, 1972.

ARENDT, Hannah. **Du mensonge à la violence. Essais de politique contemporaine**, Paris: Calmann-Lévy, 1972.

ARENDT, Hannah. **Le système totalitaire. Les origines du totalitarisme**. Paris: Gallimard, 2002.

ARENDT, Hannah. Mentira na política: reflexões sobre os Documentos do Pentágono. *In:* **Crises da República**. Trad. J. Volkmann. São Paulo: Editora Perspectiva, 2ª edição (3ª reimpressão), 2004.

ARENDT, Hannah. **La politique a-t-elle encore un sens ?** Paris : Editions de l'Herne, 2017.

BARBOSA, Beatriz.; MARTINS, Helena; VALENTE, Jonas. **Fake News: como as plataformas enfrentam a desinformação**. Rio de Janeiro: Grupo Multifoco, 2021.

BBC NEWS (2016). The saga of 'Pizzagate': The fake story that shows how conspiracy theories spread. **BBC online**, 2016. Disponível em: http://www.bbc.com/news/blogs-trending-38156985. Acesso em: 30 jul. 2024

BERNAYS, Edward. **Propaganda. Comment manipuler l'opinion en démocratie**, Paris : La Découverte, 2007.

BEZERRA, Sabrina. O que faz o Brasil ser o segundo maior mercado do WhatsApp no mundo? **Startse online**. Disponível em: https://startups.com.br/whatsapp-summit-brasil/o-que-faz-o-brasil-ser-o-segundo-maior-mercado-do-whatsapp-no-mundo/. Acesso em: 30 jul. 2024

BLOCH, Marc. **Reflexões de um historiador sobre as notícias falsas da guerra**. Disponível em: https://fr.scribd.com/document/453364001/BLOCH-M-Reflexoes-de-um-historiador-sobre-as-noticias-falsas-da-guerra-pdf. Acesso em: 30 jul. 2024

BLOCH, Marc. **Réflexions d'un historien sur les fausses nouvelles de la guerre**. Paris: Allia, 2019.

BRKAN, Maja. Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting**. Delphi**, 2, p.66-71, 2019.

CAMPBELL, Alex. How Data Privacy Laws Can Fight Fake News?. **Just Security online**, 2019. Disponível em: https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/. Acesso em 30 jul. 2024

CAPELLER, Wanda. A emergência do campo penal global: desconstrução do direito penal moderno. **Revista Internacional de História Política e Cultura Jurídica**, v. 12, n. 2, p. 180-196, 2020.

COMISSÃO PARLAMENTAR MISTA DE INQUERITO, **Congresso Nacional**, 2019.

COMMAILLE, Jacques. **L'esprit sociologique des lois**. Essai de sociologie politique du droit, Paris, Presses Universitaires de France, 1994.

CONSELHO NACIONAL DE JUSTICE (CNJ). Projeto é reconhecido por combate a fake news. Disponível em : https://www.cnj.jus.br/projeto-e-reconhecido-por-combate-a-fake-news/. Acesso em: 30 jul. 2024

CRUZ, José. PGR pede esclarecimento ao STF sobre investigação de fake news". **AgênciaBrasil online**, 2019. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2019-03/pgr-pede-esclarecimento-ao-stf-sobre-investigacao-de-fake-news. Acesso em 30 jul. 2024

CRUZ, Manuel. **Fake News & Desinformação:** Estudo de caso numa instituição de ensino superior em Portugal. Mestrado em Comunicação Aplicada – Ramo Comunicação Estratégica. Instituto Politécnico de Viseu, 2020.

D' ANCONA, M. **Post-truth:** The new war on truth and how to fight back. Random House, 2017.

DELEUZE, Gilles; GUATTARI, Félix. **Mille Plateaux**. Paris : Les Éditions de minuit, 1980.

DELMAZO, C.; VALENTE, J. C. L. Fake news nas redes sociais online: propagação e reações à desinformação em busca de cliques. **Media & Jornalismo**, v. 18, n. 32, p. 155-169, 2018.

FARIA, Luís M. Porque acreditamos em teorias da conspiração ou em 'fake news'?. **Expresso online**, 2021. Disponível em: https://expresso.pt/sociedade/2021-04-22-Porque-acreditamos-em-teorias-da-conspiracao-ou-em-fake-news-865f4928. Acesso em: 30 jul. 2024

FATHAIGH, Ronan Ó; HELBERGER, Natali; APPELMAN, Naomi. The perils of legally defining disinformation. **Internet Policy Review**, v.10, n. 4, 2021.

FERREIRA, António Casimiro. **Política e sociedade:** teoria social em tempo de austeridade. Porto: Vida Económica, 2014.

FERREIRA, António Casimiro. **Sociologia do Direito:** uma abordagem sociopolítica. Porto: Vida Económica, 2019.

FILHO, M. Cunha; CARVALHO, P. Feitosa Araújo de; CARVALHO, S. Fake News: Definições, tipologias e a insuficiência das respostas estatais. **Revista De Estudos Empíricos Em Direito**, v. *9*, p. 1–35, 2022.

FOUCAULT, Michel. **Naissance de la biopolitique,** Cours au Collège de France (1978-1979). Paris : Gallimard/Seuil, 2004.

FRANCE 24. La présidentielle au Brésil et le vrai fléau des fake news. Disponível em: https://www.france24.com/fr/amériques. Acesso em: 30 jul. 2024

FUKUYAMA, Francis. **La Fin de l'histoire et le Dernier Homme**. Paris: Flammarion, coll. Histoire, 1992.

HENRIQUE, Layane. PL das Fake News: os 10 pontos principais para entender o projeto de lei. **POLITIZE! Online**, 2023. Disponível em: https://www.politize.com.br/pl-das-fake-news/. Acesso em 30 jul. 2024

HILEG. **A multi-dimensional approach to disinformation -** Report of the independent High-level Group on fake news and online disinformation. Luxembourg: Publications Office of the European Union, 2018.

HIGÍDIO, José; ANGELO, Tiago. Por unanimidade, 1ª Turma do Supremo confirma bloqueio do X no Brasil. **Consultor Jurídico**, 2024. Disponível em: https://www.conjur.com.br/2024-set-02/1a-turma-do-supremo-confirma-bloqueio-do-x-no-brasil/. Acesso em 12 set 2024.

KOYRE, Alexandre. **Réflexions sur le mensonge**. Paris: Ed Allia, 2004.

LAW LIBRARY. Initiatives to Counter Fake News in Selected Countries. **The Law Library of Congress, Global Legal Research Directorate**, 2019. Disponível em: https://www.loc.gov/item/2019668145/. Acesso em 30 jul. 2024

LAZER, D. M. J. *et al*. The science of fake news. **Science**, v. 359, n. 6380, p. 1094–1096, 2018.

LEWANDOWSKY, Stephan; ECKER, Ullrich K.H.; COOK, John. Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. **Journal of Applied Research in Memory and Cognition**, v. 6, n. 4, p. 353-369, 2017.

LI, J.; SU, M.-H. Real Talk About Fake News: Identity Language and Disconnected Networks of the US Public's "Fake News" Discourse on Twitter. **Social Media + Society**, v. 6, n. 2, 2020.

LOPES JR., Aury; ROSA, Alexandre Morais da. Entenda a semana do Supremo e sua investigação de ofício. **Consultor Jurídico (conjur) online**, 2019. Disponível em: https://www.conjur.com.br/2019-abr-19/entenda-semana-supremo-investigacao-oficio/. Acesso em 30 jul. 2024

LORENZETTO, Bruno Meneses; PEREIRA, Ricardo dos Reis. O supremo soberano no Estado de exceção: a (des)aplicação do direito pelo STF no âmbito do inquérito das "Fake News" (Inquérito n. 4.781). **Sequência - Estudos Jurídicos e Políticos**, v. 41, n. 85, p. 173–203, 2020.

LUSA. Brasil: Lava Jato completa dez anos com acordos de grandes empresas investigadas para redução de coimas". **Expresso online**, 2024. Disponível em: https://expresso.pt/economia/2024-03-16-Brasil-Lava-Jato-completa-dez-anos-com-acordos-de-grandes-empresas-investigadas-para-reducao-de-coimas-ea8805a9. Acesso em 30 jul. 2024

LUSA. **Associação de Jornais do Brasil pede revisão da suspensão da rede social X.** Jornal de Negócios, 2024. Disponível em: https://www.jornaldenegocios.pt/empresas/detalhe/associacao-de-jornais-do-brasil-pede-revisao-da-suspensao-da-rede-social-x. Acesso em 12 set. 2024

MARQUES, Lula. Lira anuncia grupo para propor nova versão do PL das Fake News. **AgênciaBrasil online**, 2024. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2024-04/lira-anuncia-grupo-para-propor-nova-versao-do-pl-das-fake-news. Acesso em 30 jul. 2024

MARTINS, Sandro; NAIFF, Denis. As representações sociais das fake news: perspectivas atuais das notícias falsas. *In:* KNOLL, Alessandra (org.). **Fake news: objetividade e subjetividade na era da pós-verdade**. Ebook, 2023, p. 27-41. Disponível em:

https://www.editoracientifica.com.br/books/chapter/230513090. Acesso em: 30 jul. 2024

MELKEVIK, Bjarne. Wolfgang Langhoff : un des premiers témoignages sur l'Allemagne nazie. *In* : La Chronique de Bjarne Melkevik, 2024. Tolerance. ca. Disponível em: https://www.tolerance.ca/Rubrique.aspx?ID=239&L=fr. Acesso em 14 agosto, 2024

MENESES, João Paulo (2019) "Como as leis estão a definir (e a criminalizar) as fake news. **Comunicação Pública [Online]**, v. 14, n. 7, 2019. Disponível em: http://journals.openedition.org/cp/5423. Acesso em 30 jul. 2024

MILLS, Wright. **The Sociological Imagination**. Oxford: Oxford University Press, 1959

MOREIRA, N. C.; MOREIRA JÚNIOR, R. F. A disseminação de desinformação como instrumento potencializador do estado de exceção permanente. **OBSERVATÓRIO DE LA ECONOMÍA LATINOAMERICANA**, v. 21, n. 11, p. 20597–20615, 2023.

NOBRE GAMA, Bruna M. **Sobre a Mentira na Política:** Uma análise da visão de Maquiavel e Hannah Arendt. Instituto de Ciência Política: Universidade de Brasilia, 2019.

NORMANDIN, Audrey C. Redefining "Misinformation," "Disinformation," and "Fake News": Using Social Science Research to Form an Interdisciplinary Model of Online Limited Forums on Social Media Platforms. **CAMPBELL Law Review**, v. 44, n. 2, p. 289-333, 2022.

OSAVA, Mario. Altas tecnologías y democracia en la batalla entre X y Brasil, OtherNews [Online], Disponível em : https://www.other-news.info/noticias/altas-tecnologias-y-democracia-en-la-batalla-entre-x-y-brasil. Acesso em 6 setembro 2024.

OST, François ; VAN DE KERCHOVE, Michel. **De la pyramide au réseau ? Pour une théorie dialectique du droit**. Facultés Universitaires Saint-Louis Bruxelles, 2010.

PAIVA, Felipe. Direito e fake news - A imposição da verdade e a supressão da liberdade de expressão na defesa de interesses. **JusBrasil online**, 2023.

Disponível em: https://www.jusbrasil.com.br/artigos/direito-e-fake-news/1824811637. Acesso em 30 jul. 2024

PASCOAL, Valdirene; POLONINI, Janaína; e OLIVEIRA, Carla. Serão As Fake News informações? Uma Análise a Partir Dos Planos Teóricos Da Informação. **Logeion: Filosofia Da Informação,** v. 10, n. 1, p. 21-43, 2023

PASCUAL, Manuel G. Tecnologia, EL PAIS [Online]. Disponível em: https://elpais.com/autor/manuel-gonzalez-pascual/. Acesso em 17 set. 2024.

PAUL, Kari. Brazil receives pushback from tech companies on 'fake news' bill. **The Guardian online**, 2023. Disponível em: https://www.theguardian.com/world/2023/may/03/alphabet-google-fake-news-law. Acesso em 30 jul. 2024

PEDROSO, João; CAPELLER, Wanda; SANTOS, Andreia. Os efeitos perversos da inteligência artificial: A democracia, o estado de direito e a distribuição de desigualdades e poder no mundo. **Confluências - Revista Interdisciplinar de Sociologia e Direito**, v. 25, n. 3, p. 230-253, 2023.

PINOTTI, Fernanda. Lei europeia que inspira PL das Fake News foca na transparência, não no conteúdo; entenda". **CNN Brasil online**, 2023. Disponível em: https://www.cnnbrasil.com.br/politica/lei-europeia-que-inspira-pl-das-fake-news-foca-na-transparencia-nao-no-conteudo-entenda/. Acesso em 30 jul. 2024

PIOTTE, Jean-Marc. **Les grands penseurs du monde occidental:** l'éthique et la politique de Platon à nos jours. Québec: Fides, 1997.

PIRES, Arthur. Notícias falsas e teorias da conspiração face ao absurdo. **PPGCOM – UFJF**, v. 16, n. 3, p. 112-126, 2022.

PRADEAU, Jean-François. **Les mythes de Platon**. Paris : Flammarion, 2004.

PRAZERES, Leandro. As razões de Moraes para decretar bloqueio do X no Brasil após embates com Elon Musk. **BBC News Brasil**. Disponível em: https://www.bbc.com/portuguese/articles/cx2gdx2ezz2o. Acesso em 11 set. 2024

PRAZERES, Leandro. Musk aceitou bloquear contas no X na Turquia e na Índia: por que no Brasil foi diferente? **BBC News Brasil**. Disponível em:

https://www.bbc.com/portuguese/articles/cgjv0j0p1jpo Acesso em 11 set. 2024

RENDA, Andrea. **The legal framework to address "fake news":** possible policy actions at the EU level. Brussels: European Parliament, 2018.

RIBEIRO, Amanda; MENEZES, Luiz Fernando. Entenda o embate entre Elon Musk e Alexandre de Moraes e suas possíveis consequências". **Aos fatos online**, 2024. Disponível em: https://www.aosfatos.org/noticias/elon-musk-alexandre-de-moraes-entenda/. Acesso em 30 jul. 2024

RIBEIRO, Marta. Desinformação sobre esfaqueamento provoca ataques islamofóbicos no Reino Unido. **Público online**, 2024. Disponível em: https://www.publico.pt/2024/07/31/mundo/noticia/desinformacao-esfaqueamento-provoca-ataques-islamofobicos-reino-unido-2099371. Acesso em: 31 jul. 2024

RICHTER, André. Barroso diz que há politização indevida sobre suspensão do X - Mais cedo, Primeira Turma manteve suspensão da plataforma no país. **Agência Brasil**, 2024. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2024-09/barroso-diz-que-ha-politizacao-indevida-sobre-suspensao-do-x. Acesso em 12 set. 2024

ROBERTSON, Roland. "Glocalization: Time-Space and Homogeneity-Heterogeneity". In: FEATHERSTONE, Mike; LASH, Scott and ROBERTSON Roland (eds.), **Global Modernities**, SAGE Publications, 1995, p. 25-44.

ROSA, Hartmut. A**liénation et accélération.** Vers une théorie critique de la modernité tardive. Paris : La Découverte, 2014.

SANTOS, Amanda; VAZ, Paulo. Sobre fake news e teorias da conspiração: Populismo conservador e desinformação na cultura contemporânea. **Revista Culturas Midiáticas**, João Pessoa, v. 18, p. 22-42, 2023.

SCHREIBER, Mariana. 8 de janeiro: as perguntas sem respostas um ano após ataques. **BBC News Brasil online**, 2024. Disponível em: https://www.bbc.com/portuguese/articles/c06y1vekdgeo. Acesso em 30 jul. 2024

SILBEY, Susan. Legal Culture and Consciousness. In: SMELSR, N.J; BALTES, P.B (eds.). **International Encyclopedia of the Social and Behavioral Sciences.** Amsterdam: Elsevier Sci., 2001, p. 8623-8629.

SOARES, H. Combate penal às fake news? Sobre a relação da teoria da criminalização com a verdade. **Revista do Instituto de Ciências Penais**, v. 8, n. 2, p. 299–324, 2023.

STRECK, Lenio Luiz; OLIVEIRA, Marcelo Andrade Cattoni de; BACHA E SILVA, Diogo. Inquérito judicial do STF: o MP como parte ou "juiz das garantias"?. **Consultor Jurídico (conjur) online**, 2020 Disponível em: https://www.conjur.com.br/2020-mai-28/opiniao-inquerito-stf-mp-parte-ou-juiz-garantias/. Acesso em 30 jul. 2024

THIEL, Thorsten. **Artificial Intelligence and Democracy**. Berlin: Heinrich Böll Stiftung Tel Aviv, 2022.

TIERCELIN, Claudine. **La Post-vérité ou le dégout du vrai**. Paris : Editions Intervalles, 2023.

VERSTRAETE, Mark; BAMBAUER, Jane R; BAMBAUER, Derek E. Identifying and Countering Fake News. **Hastings Law Journal**, v. 73, n. 3, p. 821-860, 2022.

VIRILIO, Paul. **Cybermonde. Les politique du pire**. Paris, Editions Textuel, 1996.

VIRILIO, Paul. **Vitesse et Politique :** essai de dromologie. Paris, Ed. Galilée, 1977.

WARDLE, Claire; DERAKHSHAN, Hossein. **Desordem Informacional:** Para um quadro interdisciplinar de investigação e elaboração de políticas públicas. Tradução: Pedro Caetano Filho e Abilio Rodrigues. Strasbourg: Council of Europe, 2023 [2017]

WECKER, Katharina. Inteligência artificial e democracia direta podem conviver?". *SWISSInfo.* **Ch online**, 2022. Disponível em: https://www.swissinfo.ch/por/intelig%C3%AAncia-artificial-e-democracia-direta-podem-conviver-/47577828. Acesso em: 30 jul. 2024

ZIZEK, Slavoj. **Violência**. São Paulo: Boitempo Editorial, 2014.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism.** The fight for a Human Future at the New Frontier of Power. Great Britain: Profile Books, 2019.

12. Do trilema regulatório à metarregulação: o caso das *fake news*

Leonardo Koyama[310]

Lucas Fucci Amato[311]

Introdução

Estamos caminhando para um cenário em que a mídia digital irá abranger todos os aspectos da vida contemporânea, seja no ambiente de trabalho, nas instituições educacionais ou nas casas. Termos como "*smart city*", "metaverso", "*machine learning*", "base de dados", "proteção de dados" e outros se incorporaram ao vocabulário cotidiano. Há alguns anos, os efeitos desse processo começaram a se manifestar. Inicialmente, com o caso Snowden, quando se descobriu, pela primeira vez na história, o alcance da tecnologia de vigilância. Posteriormente, os casos de manipulação eleitoral pela empresa Cambridge Analytica, assim como as eleições brasileiras de 2018, revelaram o potencial da ciência de dados e do direcionamento de notícias falsas, abalando nossas estruturas e instituições democráticas.

O avanço tecnológico cresce em um sistema de *looping*, na medida em que novas ferramentas possibilitam a criação de outras ferramentas ainda mais inovadoras e de maneira mais rápida e eficiente, resultando em um desenvolvimento tecnológico que segue um ritmo exponencial, o que contrasta com a rigidez do sistema jurídico e da estrutura do Estado democrático. Neste contexto, o que vêm sendo observado é uma crise regulatória no Estado e nas suas instituições, refletindo uma dificuldade por parte do direito em se adequar

[310] Bacharel pela Faculdade de Direito da Universidade de São Paulo – USP. Advogado na área de Direito Digital.

[311] Professor Associado do Departamento de Filosofia e Teoria Geral do Direito da Faculdade de Direito da Universidade de São Paulo – USP. Pesquisador visitante nas Universidades de Cambridge, Oxford e Harvard. Livre-docente, pós-doutor, doutor e bacharel em Direito pela USP. Vice-Presidente da Associação Brasileira de Pesquisadores em Sociologia do Direito – ABraSD.

à dinâmica dessas novas tecnologias emergentes. Frente a isso, cabe a nós, juristas, o exercício de pensar alternativas jurídicas criativas e experimentais, na tentativa de adequar as rígidas estruturas do direito à realidade contemporânea da sociedade da informação.

É diante desse movimento que o presente capítulo procura analisar um dos inúmeros desdobramentos que surgem desse fenômeno: a questão envolvendo a disseminação em massa das *fake news*.

A ascensão de *fake news* representou um desafio significativo no cenário contemporâneo, impactando não apenas a esfera da informação, mas também reverberando nas bases fundamentais da sociedade, como a liberdade de expressão e a integridade das democracias representativas e de seus processos democráticos. Este capítulo, assim, propõe-se a investigar a interseção entre a disseminação de *fake news*, a regulamentação da internet no contexto brasileiro e a viabilidade da proposta de autorregulação regulada como uma abordagem eficaz a solucionar o problema.

O texto busca aprofundar a discussão sobre "metarregulação" (AMATO, 2021) no campo da disseminação massiva de notícias falsas pelas plataformas digitais (redes sociais e serviços de mensageria privada). No primeiro tópico, de natureza mais teórica, estabelecemos uma base conceitual para contextualizar o problema das *fake news*. Inspirado nas contribuições de teóricos sistêmicos como Niklas Luhmann e Gunther Teubner (particularmente com seu conceito de "trilema regulatório"), o estudo busca oferecer *insights* sobre como a interação entre a regulação estatal e a autorregulação pode proporcionar soluções mais flexíveis e eficazes para o desafio da disseminação de informações falsas.

O segundo tópico assume uma abordagem mais prática, observando a aplicação e implementação dos conceitos. O instituto da "autorregulação regulada" foi previsto no art. 30 da versão anterior do Projeto de Lei das *Fake News* (Projeto de Lei nº 2.630/20) em curso no Congresso Nacional brasileiro, mas foi retirado na última versão desse projeto, que ainda não foi transformado em lei. Assim, o trabalho procura analisar as principais controvérsias envolvendo o Projeto de Lei no ano de 2023 e o que esteve por trás das dificuldades em sua

aprovação. A análise deste fenômeno proporciona uma compreensão mais profunda das possíveis vantagens e desafios associados à "metarregulação" no contexto da regulação da internet, contribuindo para o entendimento crítico desse complexo cenário regulatório.

1. *Fake News*

No Brasil, a problemática das *fake news* se insere em um contexto legislativo e político marcado por eventos que escancararam o mau uso dos meios digitais e a manipulação de informações. Um marco relevante foi o ano de 2013, quando Edward Snowden expôs práticas de espionagem conduzidas pelo governo dos Estados Unidos, justamente durante a tramitação do Marco Civil da Internet no Brasil, que se tornou lei em 2014. Alguns anos mais tarde, a discussão sobre a proteção de dados pessoais ganhava força, agravada pelo escândalo da Cambridge Analytica, que utilizou dados de maneira irregular nas eleições nos Estados Unidos e no caso do Brexit do Reino Unido. Este cenário internacional culminou com a implementação do *General Data Protection Regulation* (GDPR) na União Europeia, impactando diretamente as discussões sobre privacidade e regulação no Brasil, culminando mais tarde com a Lei Geral de Proteção de Dados (LGPD), aprovada em 2018, às vésperas das eleições nacionais (marcadas por amplas estratégias de desinformação, sobretudo da parte do presidenciável vencedor, Jair Bolsonaro). Entretanto, a lei teve sucessivas postergações do início da vigência – entrou em vigor apenas em setembro de 2020, com sanções imponíveis a partir de agosto de 2021.

Essa conjuntura, permeada por avanços tecnológicos e crises de desinformação, amplificou-se com as eleições brasileiras de 2018 e 2020, nas quais o disparo massivo de desinformação se revelou uma estratégia eleitoral preocupante. Diante desse cenário, o Legislativo brasileiro se viu pressionado a agir, dando origem ao Projeto de Lei das *Fake News* (PL 2.630/2020). Além disso, o tema das *fake news* mobilizou não apenas o Legislativo, mas também o Judiciário, o que se evidencia, por exemplo, na Comissão Parlamentar Mista de

Inquérito das *Fake News* e no Inquérito das *Fake News* instaurado pelo Supremo Tribunal Federal.

A questão das *fake news* certamente não é o único problema que emerge da dominação do espaço público pelas plataformas digitais, mas nos últimos anos, evidentemente, tornou-se um dos assuntos mais discutidos pelo impacto produzido. Além disso, a discussão envolve outros temas centrais, como dados pessoais, privacidade, liberdade de expressão e discurso de ódio.

Fake news, no contexto das mídias sociais, não podem ser interpretadas simplesmente como "notícia falsa" ou o que antigamente se consideraria um boato. São notícias intencionalmente falsas, veiculadas com o objetivo de confundir seus leitores. No contexto das eleições, esse objetivo se traduz na intenção de beneficiar determinado candidato, podendo-se difamar um candidato adversário. Ademais, isso se intensifica ainda mais pelo alcance permitido pelas novas tecnologias de comunicação e disseminação da informação.

> Não se trata meramente do uso da mentira e de boatos no processo eleitoral, mas de uma nova estrutura social configurada pela emergência de tecnologias que permitem a produção e a disseminação descentralizada e massiva de desinformação, sem os controles comuns aos meios de comunicação de massa tradicionais do século XX (como empresas de rádio e televisão, objeto de concessão estatal) e, igualmente, sem fácil identificação e responsabilização individualizada de uma multidão de envolvidos no impulsionamento dessas notícias. (AMATO; SABA; BARROS, 2021, p. 541).

A interseção complexa entre a legislação, os eventos políticos marcantes e a ascensão das *fake news* no cenário brasileiro reflete um desafio multifacetado. A resposta legislativa, exemplificada pelo Projeto de Lei das *Fake News*, e as iniciativas do Judiciário, como a Comissão Parlamentar Mista de Inquérito e o Inquérito das *Fake News*, destacam a necessidade urgente de abordar o impacto eleitoral e social dessas práticas prejudiciais.

A conjuntura regulatória, marcada por avanços tecnológicos e crises de desinformação, ressalta não apenas a complexidade das *fake news*, mas também a necessidade de um equilíbrio cuidadoso entre a proteção da liberdade de

expressão, a salvaguarda da privacidade e a preservação da integridade democrática.

1.1. Tipos de sociedade e tecnologias comunicacionais

A relação entre diferentes tipos de sociedade e as tecnologias comunicacionais que os suportam pode ser considerada à luz da sociologia sistêmica de Niklas Luhmann. Isso ajuda a compreender que a mentira, o boato ou a notícia falsa são fenômenos não exclusivos da sociedade da informação, mas sim presentes em todos os tipos de sociedade; o efeito causado atualmente se dá pelo avanço dos meios de disseminação. Os meios digitais de disseminação da comunicação são a estrutura marcada por trás da semântica das "*fake news*".

Podemos correlacionar as formas de diferenciação social apontadas por Luhmann (2013) com os respectivos "meios de disseminação" da comunicação predominantes. Em sociedades baseadas em sistemas de interação – encontros pessoais, face-a-face, a diferenciação é segmentária; os grupos são ligados principalmente pelo parentesco, havendo uma profunda distinção entre os membros e os estranhos. Nessa forma de diferenciação "tribal", a comunicação presencial e oral implicava restringir a variabilidade da comunicação, ou seja, seu uso, sua mensagem e compreensão supunham a adesão à mesma comunidade de vida e valores. A interação e a comunicação entre os presentes eram então estritamente limitadas pelas estruturas; a disseminação era restrita, baixa e lenta, constrangida pelo estreito repertório de expectativas profundamente compartilhadas dentro do mesmo grupo.

Em uma transição de sociedades baseadas em interações pessoais comunitárias para sociedades fundadas em hierarquias abrangentes, surgem distinções entre centros (já hierarquizados, baseados na escrita e no direito imposto por governos centralizados) e periferias (comunidades interacionais, baseadas na comunicação oral e no costume). Nessa forma de sociedade, os meios de comunicação ficam concentrados naqueles grupos em que a escrita é difundida, na medida em que a técnica é dominada por uma elite letrada.

As sociedades estratificadas, fundadas em uma ampla hierarquia

polarizada entre nobres e povo (como nos grandes impérios da antiguidade e no Estado absolutista europeu do início da modernidade), têm justamente este último perfil. Pode-se pensar, por exemplo, na igreja católica, que controlou por muito tempo os meios de preservação e difusão escrita da informação. A sociedade estratificada caracteriza-se pela concentração da comunicação escrita entre as elites, com um predomínio da oralidade na comunicação popular.

O surgimento da imprensa desestabiliza a estratificação social, colocando em xeque o monopólio informacional da elite letrada, difundindo a informação e tornando possível a crítica pública das ações do poder estatal. Nesse contexto, nasce a "opinião pública", refletindo e julgando as decisões do Estado e criando uma arena de cidadãos que disputam o sentido da imprensa. Das revoluções liberais dos séculos XVII, XVIII e XIX, chegamos no século XX à difusão da imprensa operária, dos sindicados e dos partidos de massa. A partir desse momento, tem-se uma disputa mais organizada pelo controle da comunicação política.

Em 1995, Niklas Luhmann, em seu livro sobre a realidade da comunicação de massa, cravou: "Aquilo que sabemos sobre nossa sociedade, ou mesmo sobre o mundo no qual vivemos, o sabemos pelos meios de comunicação" (LUHMANN, 2005, p. 15). Na ocasião, Luhmann estava revelando a centralidade dos meios de comunicação de massa na nossa sociedade, especialmente enfatizando, para a década de noventa, o papel central desempenhado por organizações ou empresas na produção de informações, tais como jornais impressos, rádio e televisão. A "veracidade" ou, mais precisamente, a qualidade da informação estava associada, por um lado, aos padrões jornalísticos decorrentes da formação profissional dos jornalistas, com suas técnicas de verificação e princípios éticos, e, por outro lado, à responsabilidade civil e penal do editor-chefe do jornal.

Com a popularização do mundo digital, os usuários começaram a se tornar cada vez mais relevantes, na medida em que estão no centro da operação das plataformas digitais. São não apenas consumidores massivos, mas também produtores dispersos e massivos de informação. São "produmidores". Com as

redes sociais, as organizações profissionais de comunicação passam a perder um pouco do seu valor e se desvinculam cada vez mais da produção de informação, tornando-a mais direta, ao mesmo tempo em que é reintermediada pelas plataformas digitais, por exemplo, em posts no Facebook ou Instagram, na interação entre leitores em *blogs* ou no compartilhamento em grupos do WhatsApp.

Quando os indivíduos têm a capacidade de expressar suas opiniões e pontos de vista a audiências cada vez mais amplas e interconectadas, a comunicação individualmente impulsionada adquire importância equivalente ao sistema funcional da mídia. Isso implica que tanto a informação global quanto as mensagens – incluindo aquelas que possam ser falsas – perdem sua ligação com seus emissores originais, passando a fazer parte do sistema de comunicação digital autorreferente, que não possui identidade específica. Ao lado da informação e da mensagem, a compreensão da comunicação é hipersimplificada, na forma de memes e tweets.

1.2. Redes sociais, fake news e liberdade de expressão: cenários regulatórios

As características da internet a princípio se harmonizariam perfeitamente com o direito fundamental da liberdade de expressão. Através da internet, a liberdade de expressão pode ser exercida instantaneamente por meio de diversas ferramentas disponibilizadas pela própria plataforma, tais como realizar uma publicação, comentar em uma foto ou compartilhar um conteúdo.

No contexto brasileiro, essa dinâmica torna-se ainda mais evidente. O direito à liberdade de expressão foi incorporado ao ordenamento jurídico do Brasil pela Constituição Federal de 1988, marcando o fim da ditadura militar após duas décadas de censura, proibição da manifestação do pensamento e repressão a diversos direitos. Nesse cenário, com a tutela do Estado e o avanço da internet, as redes sociais emergiram como um ambiente propício para a fusão entre a liberdade de expressão e a possibilidade de gerar conteúdo ou informação, mesmo que não houvesse compromisso com a veracidade da informação.

Dessa forma, o fenômeno das *fake news* pode ser observado seguindo três cenários regulatórios:

(i) Liberdade de Expressão Plena: assegurar uma liberdade de expressão irrestrita nas redes sociais, permitindo que os usuários compartilhem livremente suas opiniões, independentemente de sua veracidade ou impacto na sociedade;

(ii) Liberdade de Expressão Restrita: implementar um controle estrito sobre as redes sociais, monitorando e regulamentando as informações compartilhadas para combater a propagação de *fake news*, desinformação e discursos de ódio;

(iii) Liberdade de Expressão Moderada: buscar um equilíbrio entre a liberdade de expressão e a necessidade de controlar informações falsas, com intervenções seletivas para eliminar *fake news* e desinformação, preservando a veracidade dos dados compartilhados, mas com um risco de censura ou viés na moderação.

Sobre o primeiro cenário: a noção de uma liberdade de expressão irrestrita é extremamente sedutora (FAUSTINO, 2019), especialmente quando se leva em conta que existe uma possibilidade de não responsabilização pela manifestação dessas ideias, deixando a opção ainda mais atraente. É essa a impressão que a internet transmite ao evidenciar sua dinâmica de interação: um ambiente universal e difuso que permite facilmente a anonimização, o que gera um descolamento entre o mundo real e o virtual e faz com que as pessoas se sintam encorajadas a publicar ou expressar pensamentos sem se preocupar com as consequências desses atos. Isso resulta numa exacerbação no exercício da liberdade de expressão, criando um ambiente propício para a disseminação de conteúdos que podem violar diversos direitos, como os discursos de ódio e as *fake news*. A internet potencializa "movimentos de integração social" (CAMPILONGO, 2012; CARROZZA, 2023), que, em nome de uma purgação moral redentora, promovem cancelamentos e linchamentos virtuais, a fim de reforçar sua unidade moral, estigmatizar e ostracizar dissidentes. O pluralismo valorativo da sociedade liberal e funcionalmente diferenciada se vê

comprometido pela própria descentralização do potencial comunicativo que essa mesma sociedade exponenciou por meio das tecnologias digitais.

Na mídia digital, a monetização derrota a veracidade, associada a padrões jornalísticos e à responsabilidade civil e penal do editor-chefe de um jornal. A liberdade de expressão como fundamento do uso da internet criou uma falsa percepção de liberdade plena como um "supraprincípio" no ciberespaço. Essa crença, quando levada em conta a universalidade da internet, permite que qualquer pessoa possa se tornar um provedor de informação e conteúdo, quebrando com a antiga lógica da sociedade estratificada e mesmo dos meios de comunicação de massa típicos da sociedade funcionalmente diferenciada na era industrial, quando os meios de comunicação pertenciam a ou eram controlados por um determinado grupo. Hoje, por contraste, inexiste, cada vez mais, uma diferenciação entre o conteúdo gerado por canais oficiais de imprensa e aqueles gerados por terceiros. Esse fato se relaciona com a característica de ineditismo da sociedade da informação, na qual é preciso produzir mais informação para atender à demanda insaciável por novidades, gerando essa despreocupação com a fonte da informação e do conteúdo, pois a velocidade é mais importante do que o conteúdo. O ineditismo está relacionado com a celeridade na circulação da informação, e não necessariamente com a sua qualidade.

Por outro lado, um (segundo) cenário onde a liberdade de expressão é restrita também traz consequências negativas. O Brasil, assim como outros países em que a memória de uma ditadura permanece recente, não precisa recapitular tanto a história para concluir que o direito de liberdade de expressão é, de fato, imprescindível. Em um Estado autoritário, opiniões contrárias ao sistema são reprimidas através do medo e da violência, limitando o que os indivíduos podem pensar, agir e falar publicamente. A opinião pública se torna completamente manipulada a favor do Estado por meio do aparelhamento dos meios de comunicação.

Brendan O'Neill (2015) defende a ideia de que a restrição do direito de se expressar livremente faz com que os indivíduos percam um outro direito: o direito de ofensa. Este direito adviria da liberdade de poder expressar opiniões

que são contrassistêmicas, que seriam reprimidas por algum grupo específico ou que são consideradas inapropriadas. Na atual cultura do cancelamento, tão presente nas escolas e universidades, estudantes reprimem estudantes em razão de comentários, publicações ou ações consideradas incorretas. Para o pensador, entretanto, o progresso da sociedade se deu, em parte, pelo direito de ofender, de expressar opiniões contrárias ao sistema. Diversas personalidades que exerceram seu "direito de ofensa", como Galileu Galilei e Martin Lutero, em situações em que suas opiniões eram consideradas impróprias, acabando por ser importantes para moldar o futuro da humanidade.

O termo "cancelamento" pode ser definido como a prática de promover um boicote em larga escala contra um indivíduo – frequentemente uma figura pública – em resposta a comportamentos ou declarações considerados ofensivos, injustificáveis ou moralmente condenáveis. Nesse sentido (CAMILLOTO; URASHIMA, 2021, citando RODRIGUES), a prática do cancelamento pode ser interpretada como uma prestação pública de contas e uma solicitação de correção de comportamentos em resposta a uma transgressão social que não foi devidamente controlada pelos meios convencionais. Essa prestação de contas surge da crise regulatória do Estado em estabelecer parâmetros adequados para o ambiente digital. Antigamente, se alguém fosse ofendido na rua mediante o uso de um termo pejorativo, essa pessoa poderia, caso desejasse tomar providências concretas, dirigir-se a uma delegacia e fazer uma denúncia formal. Contudo, com o advento da internet, tudo se transformou. Qualquer usuário passou a ter a capacidade de postar o que quiser sobre determinada pessoa. Subitamente, as autoridades se viram diante de um grande desafio. Como aplicar regras e sanções em um ambiente que o próprio ordenamento jurídico desconhece? Como penalizar um usuário cujo perfil não corresponde à sua identidade verdadeira? E como impor regras a uma plataforma cuja sede está localizada em outro país?

Após o período da ditadura militar e com o surgimento da internet, as pessoas estavam entusiasmadas com a oportunidade de se expressarem livremente em um ambiente que permitiria uma clara separação entre o mundo real e o virtual, tornando menos provável qualquer responsabilização. Nessa

fase, tudo era permitido, possibilitando a publicação de praticamente qualquer conteúdo desejado.

Entretanto, ao longo dos anos, o crescimento e desenvolvimento da internet acompanharam o fortalecimento dos movimentos sociais das minorias (como os movimentos de gênero, negro, feminista etc.), iniciando uma tendência de estabelecer padrões morais e éticos sobre o que poderia ou não ser divulgado nas redes sociais. Desse modo, a cultura do cancelamento surgiu como uma resposta dos próprios indivíduos à dificuldade do Estado em regular, responsabilizar e punir os conteúdos considerados inadequados. Surge, assim, uma espécie de autorregulação por parte dos próprios cidadãos, enquanto estes esperam que o Estado se adeque à dinâmica das plataformas digitais.

Por fim, partindo para o último cenário regulatório, no qual se tem uma liberdade de expressão moderada, trata-se de um delicado equilíbrio entre garantir a livre manifestação de ideias e combater a disseminação de informações falsas por meio da regulação do ambiente digital. Um caminho para atingir essa moderação pode ser o da "metarregulação" ou autorregulação regulada. Nesse cenário, será essencial estabelecer diretrizes transparentes para a moderação das redes sociais, com intervenções seletivas visando eliminar especificamente as *fake news*, a desinformação e conteúdos ofensivos (como o discurso de ódio). No entanto, esse caminho não está isento de desafios: como visto, inclui os riscos de censura seletiva e de viés nas decisões de moderação. Portanto, a implementação bem-sucedida dessa estratégia requer um constante debate sobre a regulamentação das plataformas, com a participação de diversos atores, a fim de assegurar a justiça e a eficácia no tratamento das informações enganosas e evitar os efeitos nocivos do chamado trilema regulatório. Mas o que é, teoricamente, o "trilema regulatório"?

1.3. Direito reflexivo e o trilema regulatório

Desde as eleições brasileiras de 2018, revelou-se uma grande dificuldade por parte do Estado em lidar com uma sociedade complexa e diferenciada em várias arenas comunicativas, especialmente quando considerada sob a

perspectiva do pluralismo jurídico. Nesse sentido, a legislação, a jurisprudência e o regramento administrativo podem ser instrumentos excessivamente rígidos, lentos ou insensíveis para enquadrar juridicamente fenômenos emergentes, resultando em uma sobrecarga para o poder público.

Nesse contexto, ganha destaque a estratégia da procedimentalização ou de um "direito reflexivo" (TEUBNER, 1983). Essa abordagem visa a oferecer maior flexibilidade e adaptabilidade às transformações sociais, reconhecendo a necessidade de um enfoque mais dinâmico e responsivo por parte do sistema jurídico diante de fenômenos em constante evolução.

A autorregulação privada, conforme propunha o antigo art. 30 do PL nº 2.630, é um instituto de direito reflexivo, o qual se baseia na ideia fundamental de adaptação e reflexividade do sistema jurídico em resposta às mudanças em seu ambiente. Por sua vez, a perspectiva da reflexividade considera que o sistema jurídico se vê a si próprio como um sistema dentro de um ambiente multissistêmico, reconhecendo os limites da sua capacidade de regular os outros sistemas sociais. Essa abordagem deriva da teoria do direito de Gunther Teubner e foi uma contribuição significativa à teoria sistêmica, enfatizando a habilidade do sistema jurídico de se adaptar e reconhecer e reagir às mudanças em seu contexto por meio de processos de comunicação e autopoiese (MELLO, 2006).

Segundo Teubner (1986), a regulação enfrenta um risco de fracasso se não estiver alinhada às condições de "acoplamento estrutural" do direito, da política e de outros subsistemas da sociedade. Esse acoplamento refere-se ao mecanismo em que um sistema se utiliza das estruturas de funcionamento de outro para operar seus próprios processos comunicativos (NEVES, 2005). Trata-se da interdependência entre os sistemas sociais e seu ambiente, mediada por processos de comunicação e diferenciação funcional. Teubner (1986) identifica três cenários possíveis para o fracasso regulatório denominado "trilema regulatório" (*regulatory trilemma*): (i) simbolismo; (ii) instrumentalismo e (iii) juridificação.

O simbolismo refere-se a um cenário no qual há uma incongruência entre os sistemas jurídico, político e outros sistemas sociais. A ação regulatória torna-

se incompatível com as interações autopoiéticas do sistema regulado, levando-o a reagir por meio de uma não reação. Nesse contexto, a ação regulatória não atende aos critérios de relevância do sistema regulado, tornando-se simplesmente irrelevante – simbólica – para as interações dos elementos.

No âmbito do problema das *fake news*, o simbolismo pode ser associado ao uso excessivo de princípios, como evidenciado nos casos do Marco Civil da Internet, da LGPD e, mais recentemente, do PL das *Fake News*. Essa abordagem pode resultar em uma ineficácia do direito, de forma que o sistema prolifera proclamações vagas e ambíguas de valores e não estimula mudanças de comportamento no sistema regulado, mas simplesmente confirma moralmente certos valores, sem dar instrumentos para a implementação de medidas concretas e eficazes.

Por sua vez, o instrumentalismo se refere a outro cenário em que ocorre uma falha regulatória, mas a diferença reside no fato de que a organização autorreferencial da área regulada permanece intacta, enquanto a organização autorreferencial do direito é ameaçada. O direito é "capturado" pela política ou pelo subsistema regulado, sendo "politizado", "economicizado", "tecnificado", "mediatizado" etc. Assim, o sistema jurídico torna-se um mero instrumento dos outros sistemas e subsistemas.

No contexto brasileiro, essa realidade se mostra evidente diariamente, com os noticiários frequentemente destacando interferências de outros sistemas no direito. Isso é particularmente perceptível no caso do Projeto de Lei das *Fake News*, que teve sua aprovação adiada devido a influências políticas e econômicas da bancada das *big techs*. Assim, podemos afirmar que o risco do instrumentalismo, no âmbito da regulação das *fake news*, pode resultar em diferentes cenários.

Por um lado, há o perigo de um uso da legislação para promover a vigilância estatal de conteúdo nas redes, o que representaria uma violação da liberdade de expressão, transformando o direito em um instrumento politizado.

Por outro lado, surge a possibilidade de uma instrumentalização do direito por parte das *big techs*, "economicizando" o direito através do uso

estratégico das redes sociais com o principal objetivo de gerar lucro. Isso porque a disseminação de *fake news* tem se mostrado um negócio extremamente rentável, na medida em que faz uso de algoritmos que asseguram o financiamento das plataformas ao selecionar propagandas que possibilitam manter os usuários envolvidos com o conteúdo o maior tempo possível. Assim, quanto maior o tempo passado nas plataformas, mais dados são coletados dos usuários, mais anúncios são exibidos e mais dinheiro é gerado.

Por fim, a juridificação diz respeito a um cenário no qual a ação regulatória influencia as interações internas dos elementos no campo do sistema regulado de uma forma tão intensa que sua autoprodução fica ameaçada. Neste caso, o direito regulatório ultrapassa a linha da mútua indiferença, assim como aquela em que é ameaçado, de forma que o estímulo do seu conteúdo normativo gera efeitos nocivos aos mecanismos internos de operação do sistema regulado, destruindo suas estruturas próprias (AMATO; MISSAGIA, 2023). Isso leva a efeitos desintegradores, gerando uma "colonização" do campo regulado. Seria o caso de uma regulação tão hierárquica, centralizada, minudente e coercitiva do uso das redes digitais que acabaria por impor custos que desmotivariam a inovação tecnológica, a oferta dos serviços e/ou a adesão dos usuários. No limite, voltaríamos simplesmente à era analógica, abrindo mão dos benefícios das plataformas digitais para nos preservarmos de seus custos. No caso da regulação das plataformas digitais, a legislação corre o risco de se tornar abrangente e detalhada a ponto de inviabilizar a própria operacionalidade das plataformas digitais, que funcionam num âmbito mundial e com uma operacionalidade complexa e especializada.

Positivamente, para a superação do trilema regulatório, ganham destaque abordagens que enfatizem a coordenação entre os sistemas sociais, surgindo como uma alternativa valiosa em oposição à mera imposição de legislação ou à regulação "simbólica". Em vez de depender exclusivamente de instrumentos principiológicos, a abordagem coordenativa destaca a necessidade de se estabelecerem mecanismos eficazes de colaboração entre os diversos sistemas,

reconhecendo as peculiaridades e os mecanismos autorreferenciais inerentes ao sistema regulado.

Além disso, a saída do trilema também sublinha a importância da externalização através da concepção de mecanismos de autorregulação. Esse enfoque contrasta com a "juridificação", indicando que a imposição excessiva de regulamentações legais pode não ser a resposta mais eficaz para lidar com as dinâmicas complexas da sociedade atual. A externalização, ao favorecer mecanismos que permitem a autorregulação dentro dos próprios sistemas, reconhece a capacidade dos sistemas sociais de se adaptarem e evoluírem de maneira autônoma, incentivando a autorreferência e autopoiese do sistema regulado.

Por fim, destaca-se a importância de se preservar a autonomia do sistema jurídico e resistir ao "instrumentalismo". Em vez de tratar o direito como um mero instrumento para alcançar objetivos externos, a abordagem autônoma enfoca na autorreferência e autopoiese do sistema jurídico. Impede a instrumentalização excessiva do direito em função de interesses políticos ou econômicos, garantindo que o sistema jurídico mantenha sua capacidade de autodeterminação.

2. Regulação da internet no Brasil: pluralismo jurídico, déficit regulatório e metarregulação

O problema das *fake news* gera um conflito entre pelo menos três sistemas sociais: o sistema político, o sistema jurídico e o dos meios de comunicação de massa. Esse conflito emerge devido ao fato de que o direito estatal – acoplamento entre o sistema político nacional e o sistema jurídico – é pressionado a apresentar respostas regulatórias rápidas e efetivas aos problemas advindos do sistema de comunicação de massa, um sistema cuja dinâmica lhe é estranha, mas cujos impactos transbordam para questões de legitimidade e justiça.

Nesse sentido, há enorme dificuldade do direito estatal em oferecer respostas *democraticamente legítimas, tecnicamente adequadas* e *juridicamente precisas* para o problema da disseminação massiva de *fake news*. As dificuldades de

regular, no caso do Legislativo, e de decidir, no caso do Judiciário, podem ser compreendidas, respectivamente, por referência a dois grandes problemas: (i) o pluralismo jurídico da sociedade mundial, gerando uma incapacidade do direito estatal de regular sozinho; e (ii) a falta de regulações bem definidas, que impede os tribunais de emitirem decisões efetivas, promovendo um déficit de programação.

O pluralismo jurídico na sociedade mundial constitui-se pela emergência de ordens jurídicas transnacionais, setoriais, não estatais, as quais acabam criando uma normatividade própria para lidar com problemas comuns a toda a sociedade mundial. Reflete a coexistência de múltiplos sistemas legais, transformando o sistema jurídico em uma arena na qual disputam esses ordenamentos conflitantes, fazendo com que a autoridade e a justificação do Direito repousem sobre uma racionalidade difusa, sem centro (VESTING, 2018). Nesse sentido, o pluralismo desafia a noção de que o sistema jurídico de um Estado é a única fonte de normas e regulamentações, passando de uma ideia antiga de hierarquia unitária para uma heterárquica.

A questão do pluralismo jurídico também pode ser compreendida como sendo um reflexo da sociedade da informação e da chamada "Era da Informação". Com o advento da internet, presenciamos um crescimento exponencial na quantidade de informação disponibilizada na rede, bem como na capacidade de conectividade que, por sua vez, tornou o mundo um lugar bem "menor". Nesse contexto, o pluralismo no sistema jurídico não é senão um dos múltiplos desdobramentos do mundo digital. Além dele, emergem outras formas de pluralismo, tais como o pluralismo de plataformas digitais, pluralismo cultural, pluralismo de mídia, pluralismo econômico e diversos outros, todos interligados e moldados pela revolução tecnológica e informacional.

Como consequência, o pluralismo jurídico gera uma incapacidade do direito estatal de regular sozinho, uma vez que não dispõe de critérios suficientes para mensurar o risco que as novas tecnologias trazem para a sociedade, podendo provocar disfuncionalidades no sistema jurídico e retardando respostas

adequadas. A questão torna-se, então, um problema de regulação dentro do pluralismo jurídico da sociedade mundial.

Em face do desafio inerente do pluralismo jurídico em lidar com a complexidade das *fake news*, surge o segundo problema, dessa vez relacionado ao Poder Judiciário: o déficit de programação. Esta questão emerge da dificuldade do sistema legal em desenvolver e aplicar eficazmente regras e princípios específicos para abordar de maneira abrangente e oportuna a problemática das *fake news*. O conceito de déficit de programação destaca o papel central do Judiciário, especificamente dos tribunais, no centro do sistema jurídico, a sua relação com a periferia do sistema e as suas decisões programantes. Consequentemente, o déficit decorre da situação em que os tribunais (centro do direito) se veem obrigados a tomar decisões, por conta do princípio da proibição da denegação da justiça (*non liquet*), sem a posse de critérios firmemente estabelecidos pela legislação, consolidados pela jurisprudência ou estipulados pela doutrina (isto é, decide-se sem os filtros e estruturações prévios dados pela "periferia" do sistema jurídico). O fortalecimento dessa periferia implica o desenvolvimento de critérios e estruturas para antecipar e abordar os potenciais conflitos, sem os quais os tribunais se deparam com uma sobrecarga de casos e uma falta de fundamentos legais sólidos para embasar suas decisões.

2.1. Estratégias regulatórias

Após ressaltar a dificuldade dos tribunais em lidar com o desafio das *fake news* devido à ausência de critérios claros, surge a indagação sobre as soluções que o Legislativo, figura central do sistema político incumbida das decisões programadas, tem apresentado até o momento. Nesse sentido, podemos dividir as propostas regulatórias em três iniciativas principais: o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e o PL das Fake News.

O Marco Civil da Internet foi a primeira iniciativa brasileira sobre regulação da internet. Oficialmente denominado Lei nº 12.965, foi aprovado em 2014 e estabeleceu princípios, direitos e deveres para o uso da internet no Brasil. Essa lei foi criada para regulamentar questões como a privacidade dos usuários,

a neutralidade da rede, a responsabilidade de provedores de serviços *online*, e a liberdade de expressão na internet, entre outros aspectos.

Em seguida, a Lei Geral de Proteção de Dados (LGDP) focou especialmente a questão da proteção de dados pessoais e da privacidade dos cidadãos, tendo em vista os diversos escândalos de vazamento de dados e vigilância em massa que vinham acontecendo. Aprovada em 2018 e entrando em vigor, em etapas, a partir de 2020, a LGPD foi fortemente influenciada pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, destinando-se a estabelecer diretrizes e regras claras para o tratamento de dados pessoais no Brasil. O trâmite legislativo da LGPD foi conturbado. Foi alvo de disputa política desde o início: aprovada em agosto de 2018, a fim de surtir seus efeitos já nas eleições presidenciais que ocorreriam em outubro, acabou tendo o início da sua vigência postergada para setembro de 2020. Além disso, as sanções administrativas previstas só se tornaram oponíveis a partir de agosto de 2021.

Por fim, tem-se o PL das Fake News, projeto de Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet ou oficialmente denominado Projeto de Lei n° 2.630, de 2020. Assim como a LGPD, o PL das Fake News segue o mesmo curso turbulento: teve sua tramitação iniciada depois das eleições de 2018 e foi aprovado em 2020 pelo Senado. Entretanto, até o momento não foi aprovado pela Câmara dos Deputados, frustrando a expectativa de tê-lo aprovado a tempo das eleições municipais de 2020, das eleições nacionais de 2022 ou mesmo das eleições municipais de outubro de 2024. A cada ciclo eleitoral, permanecemos sem uma lei das *fake news*, dependendo de resoluções da Justiça Eleitoral.

Cada uma dessas propostas apresenta peculiaridades e objetivos distintos. Entretanto, podemos traçar um paralelo entre as estratégias regulatórias utilizadas na sua composição. Assim sendo, de acordo com o mapeamento de 2018 (AMATO; SABA; BARROS, 2021; SABA *et al.*, 2021), esse pacote regulatório revela o uso de quatro estratégias regulatórias por parte do legislador: (i) principialização; (ii) cognitivização; (iii) periferização e (iv) procedimentalização.

A principialização é o foco em normas principiológicas em vez de definir regras com hipóteses claras de incidência e consequências devidas. Por um lado, permite maior adaptabilidade e a criação de microssistemas legais. Mas, por outro, a falta de determinação também gera incerteza quanto às condutas consideradas ilícitas, às sanções aplicáveis e ao momento em que essas definições serão estabelecidas, seja legislativamente ou através da jurisprudência.

Essa incerteza faz com que o Judiciário – centro do sistema jurídico – busque definições normativas em matéria de direito digital no Legislativo – periferia do sistema jurídico, mas centro do sistema político –, que, por sua vez, tem buscado direcionamentos na sociedade civil – periferia do sistema político – , como partidos, acadêmicos, *experts*, movimentos sociais e grupo de interesses, como as plataformas digitais. A esta estratégia se dá o nome de periferização.

A cognitivização diz respeito à dependência da assessoria de experts em tecnologia da informação (e das próprias plataformas digitais) na criação e aplicação de normas com alto conteúdo técnico especializado; tem-se *standards* com termos de tecnologia da informação que são altamente mutáveis.

Por fim, a procedimentalização refere-se à tendência do direito estatal de estabelecer normas que promovam a abertura a outras fontes de direito que não provenham exclusivamente do Estado, incluindo as instâncias autorregulatórias. Isso implica a própria metarregulação ou autorregulação regulada.

O foco na definição principiológica, o apelo aos *experts* e a participação pública foram amplamente observados, nos casos do Marco Civil da Internet e da LGPD. Da mesma forma, tais aspectos estão sendo observados no PL das Fake News. Entretanto, o que interessa, ou, no caso, *interessava*, é que o PL das Fake News incorporava na sua versão anterior, em seu art. 30, a consagração explícita da procedimentalização, consolidando a abertura do direito estatal à autorregulação privada.

Leia-se o antigo art. 30 do PL nº 2.630 na íntegra:

> Art. 30. Os provedores de redes sociais e de serviços de mensageria privada poderão criar instituição de autorregulação voltada à transparência e à responsabilidade no uso da internet, com as seguintes atribuições:

> I – criar e administrar plataforma digital voltada à transparência e à responsabilidade no uso da internet, que contenha regras e procedimentos para decidir sobre a adoção de medida informativa, atendendo ao disposto nesta Lei;
> II – assegurar a independência e a especialidade de seus analistas;
> III – disponibilizar serviço eficiente de atendimento e encaminhamento de reclamações;
> IV – estabelecer requisitos claros, objetivos e acessíveis para a participação dos provedores de redes sociais e serviços de mensageria privada;
> V – incluir em seu quadro uma ouvidoria independente com a finalidade de receber
> VI – desenvolver, em articulação com as empresas de telefonia móvel, boas práticas para suspensão das contas de usuários cuja autenticidade for questionada ou cuja inautenticidade for estabelecida.
> § 1º A instituição de autorregulação deverá ser certificada pelo Conselho de Transparência e Responsabilidade na Internet.
> § 2º A instituição de autorregulação poderá elaborar e encaminhar ao Conselho de Transparência e Responsabilidade na Internet relatórios trimestrais em atendimento ao disposto nesta Lei, bem como informações acerca das políticas de uso e de monitoramento de volume de conteúdo compartilhado pelos usuários dos serviços de mensageria privada.
> § 3º A instituição de autorregulação aprovará resoluções e súmulas de modo a regular seus procedimentos de análise.

Interessava, pois a versão do PL nº 2.630 que estava pronta para votação em maio de 2023 retirava a previsão de se instituir uma entidade reguladora independente. A ideia inicial era criar um órgão misto que fosse independente para exercer a regulação das comunicações digitais, composto por representantes estatais, das plataformas digitais, dos movimentos sociais e de direitos digitais e da academia. Assim, cria-se um importante mecanismo de aprendizagem mútua, conciliando a evolução tecnológica com a evolução regulatória.

2.2. PL das Fake News, 8 de janeiro de 2023 e bancada das *big techs*

O PL nº 2.630, que tramita na Câmara desde 2020, voltou a ganhar fôlego em 2023 depois dos inúmeros ataques violentos em escolas (CNN BRASIL, 2023) e, principalmente, depois dos atos antidemocráticos de 8 de janeiro de 2023 (TV SENADO, 2023), quando apoiadores radicais do candidato à reeleição para a presidência Jair Messias Bolsonaro invadiram, depredaram e vandalizaram as sedes dos Três Poderes, em Brasília.

Tanto no caso dos ataques às escolas quanto no caso dos atos de 8 de janeiro, surge um questionamento relevante: qual é a responsabilidade dos provedores em relação ao conteúdo disponibilizado em suas plataformas? Em ambos os casos, a controvérsia está centrada na omissão e negligência das plataformas digitais em remover conteúdos explicitamente ilícitos, incitadores de violência e violadores das políticas internas das plataformas.

No quesito regulação, os atos antidemocráticos de 8 de janeiro podem ser considerados um marco histórico. Tal relevância se evidencia não apenas pelo fato de que os atos reacenderam o debate sobre a regulação das plataformas, mas também por representarem o clímax de uma trama que se desenrola desde 2015. Na época, o Brasil começou a notar a presença de uma onda crescente da extrema direita nas ruas e no ambiente digital, como resposta aos inúmeros casos de corrupção do governo petista que foram expostos pelas mídias. Naquela ocasião, tornou-se perceptível a emergência de um fenômeno inédito, à medida que os grupos de direita começavam a ganhar um apoio expressivo da juventude.

Essa base é importantíssima para compreender como o movimento de direita ganhou força e espaço nas plataformas digitais, pois esses jovens – ágeis no uso das redes sociais – foram responsáveis pela proliferação de grupos e páginas de direita que visavam demonstrar uma grande insatisfação com um governo de esquerda através da exposição de discursos conservadores. João Cezar de Castro Rocha (2021) faz uma análise minuciosa da ascensão dessa direita e como isso culminou na eleição do candidato Jair Messias Bolsonaro nas eleições de 2018. O autor parte de uma hipótese interessante:

> [...] a guerra cultural bolsonarista, que se beneficia de uma técnica discursiva, a retórica do ódio, ensinada nas últimas décadas por Olavo de Carvalho, conduzirá o país ao caos social, à paralisia da administração pública e ao déficit cognitivo definidor do analfabetismo ideológico, outro conceito novo que apresento, e com o qual descrevo a negação da realidade e o desprezo pela ciência que estruturam o bolsonarismo. (ROCHA, 2021, p. 23)

Essa premissa é interessante para o presente trabalho, na medida que termos como "guerra cultural" e "retórica do ódio" são conceitos importantes na

compreensão do fenômeno das *fake news* e de sua aparição no contexto brasileiro. Nesse contexto, é possível fazer uma analogia: as *fake news* atuaram como combustível da guerra cultural bolsonarista, cuja fórmula tem raízes na retórica do ódio presente no sistema de crenças do astrólogo Olavo de Carvalho. A guerra cultural é um fenômeno muito anterior ao bolsonarismo, merecendo aprofundamento teórico para ser compreendido por completo. Para fins deste capítulo, basta compreender que a guerra cultural, no contexto brasileiro dos últimos anos, significou uma estratégia política de mobilização permanente das massas digitais para buscar constantemente um inimigo político.

Essa estratégia parte do pressuposto de que existe um inimigo político que deve ser eliminado, tanto no campo ideológico e cultural, quanto no físico. E esse tipo de retórica depende da crença de que exista uma essência, uma identidade profunda e inalterável da nação ou da sociedade, e de que ela está sob ataque.

Por sua vez, a retórica do ódio é a linguagem da guerra cultural bolsonarista, que emergiu do efeito Olavo de Carvalho e se manifestou como uma forma de discurso cujo propósito é a eliminação simbólica do outro, por meio do uso constante e monótono de palavrões, visando desqualificar integralmente o adversário. Além disso, faz parte de um sistema de crenças fundamentado em elaboradas teorias conspiratórias de dominação estrutural, as quais se materializam na concepção de doutrinação. Conforme Rocha (2021, p. 60), essa perspectiva representa o eixo central da mentalidade bolsonarista, levando à conclusão de que todas as instituições foram destruídas com o intuito de levar adiante a doutrinação. A prova disso é o "óbvio" aparelhamento das instituições. Aqui, a conclusão sustenta as premissas, e não o contrário.

Essa inversão da lógica é crucial para a compreensão do fenômeno das *fake news*. Basta que os receptores de uma determinada notícia detenham (pré)conclusões incontestáveis sobre um assunto específico; nesse caso, qualquer informação nova que reforce essa (pré)conclusão passa a ser considerada verdadeira.

Nesse sentido, as *fake news* foram essenciais para que a estratégia bolsonarista funcionasse, na medida em que mantinha o eleitorado bombardeado

de informações que retroalimentavam a ideia de que o perigo estava iminente, reforçando o sentimento de polarização e marginalização política.

Joaquim Falcão (2022) sugere uma diferença entre narrativa *fake* e as *fake news*. Enquanto as *fake news* têm como objetivo ressignificar a informação individualizável, deturpando ou falsificando um fato, notícia, pessoa ou acontecimento, a narrativa *fake* é um conjunto de informações interligadas que tem como objetivo implantar uma determinada compreensão coletiva, podendo incluir notícias verdadeiras dentro de uma lógica própria, em geral oculta. Ou seja, enquanto as *fake news* são unidades isoladas da mentira informacional, a narrativa *fake* é um conjunto de informações interligadas que busca influenciar a compreensão das pessoas sobre determinado assunto.

A narrativa *fake* não se revela de forma explícita, mas permanece oculta, causando danos estratégicos coletivos, sendo muito difícil de identificar e tipificar autor ou vítima. Nas últimas duas décadas, um fator significativo nesse crescimento de grupos que adotam narrativas falsas, como os negacionistas – antivacinas (SALAS, 2020), neonazistas (G1, 2022), terraplanistas (GARCIA, 2019), entre outros –, é a ampla disseminação dessas ideias através das plataformas digitais. A responsabilidade dessas plataformas não pode ser negligenciada, uma vez que seus algoritmos não apenas permitem, mas muitas vezes favorecem discursos negacionistas ao criarem ambientes propícios para a propagação de desinformação.

Assim, de acordo com um estudo produzido pelo próprio Twitter (atualmente denominado "X"), ficou demonstrado que os algoritmos da plataforma, a partir do aprendizado construído com as interações dos usuários, prioriza o impulsionamento de conteúdos publicados por políticos e veículos de comunicação de direita e centro-direita na maioria dos países examinados (NEXO, 2021).

Na mesma linha, o Netlab (2023)[312] fez um mapeamento durante o período de 23 a 30 de agosto de 2022 para identificar quais os principais canais e

[312] Recomendação no Youtube: o caso Jovem Pan. 5 de Setembro de 2022, Escola de Comunicação da Universidade Federal do Rio de Janeiro, Brasil, citado por NetLab (2023).

conteúdos informativos que tiveram visibilidade destacada pelo algoritmo de recomendação do YouTube. Segundo o estudo, durante o período analisado os resultados constataram que o Google privilegiou conteúdos da emissora Jovem Pan e Pró-Bolsonaro[313].

Além disso, outros dois resultados foram bem interessantes. O primeiro é que o sistema de recomendação da plataforma tem um efeito de publicidade. Isso impacta fortemente as escolhas dos usuários, criando a ilusão de que o vídeo sugerido segue critérios de relevância e não influenciados por acordos comerciais ou outros interesses. O outro resultado diz respeito ao ciclo de *feedback loop*. O mapeamento observou que o favorecimento da Jovem Pan pelo sistema de recomendação do YouTube opera em dois níveis: primeiro, ao posicionar vídeos da emissora como a primeira sugestão na *homepage*, e segundo, ao recomendar vídeos relacionados ao primeiro clique. Esse fenômeno, chamado de "propaganda *feedback loop*", conduz os usuários a um ciclo autorreferenciado ao consumir o conteúdo sugerido, exacerbando seu impacto, considerando que 70% do conteúdo assistido pelos usuários é fornecido por meio dessas recomendações.

No caso dos eventos de 8 de janeiro, de acordo com relatório da ONG SumOfUs (URGENT REPORT, 2023), as plataformas de redes sociais permitiram o compartilhamento de conteúdo relacionado aos ataques em Brasília. Inclusive, foi possível observar inúmeras transmissões ao vivo dos eventos que chegaram a atingir milhões de visualizações e foram monetizadas, gerando lucro tanto para os donos das páginas quanto para as plataformas.

Esses relatórios, estudos e mapeamentos são apenas exemplos de inúmeros outros que revelam que há um interesse comercial e político por parte das empresas de tecnologia fornecedoras das principais plataformas digitais.

[313]"Nas 18 visitas-teste, os canais do grupo Jovem Pan foram identificados 14 vezes na primeira página, com um ou mais vídeos. Os vídeos dos canais Jovem Pan aparecem como primeira sugestão em 55% dos testes. [...] Em nossa análise, o vídeo mais recomendado foi da entrevista concedida por Jair Bolsonaro ao Programa Pânico na sexta-feira (26/08). O programa deu espaço ao presidente para exaltar seu atual governo e atacar a candidatura de Luiz Inácio Lula da Silva, rebatendo a sabatina do ex-presidente no Jornal Nacional, realizada na noite anterior" (NetLab-UFRJ, 2023).

Esse fato é relevante para entender o que está por trás da aprovação do PL das Fake News. Em abril de 2023, na véspera da votação do PL, plataformas como Google, Spotify e Meta começaram a veicular anúncios contra o projeto de lei. As estratégias foram diversas. No caso do Google, foram inúmeras, desde o favorecimento de links de conteúdo de oposição ao PL nos resultados das buscas sobre o projeto de lei até a distribuição de alertas internos para pressionar os criadores de conteúdo da plataforma YouTube sobre o projeto.

A plataforma chegou, inclusive, a divulgar um *link* com mensagens explícitas como "O PL das Fake News pode piorar a sua internet" e "O PL das *Fake News* pode aumentar a confusão entre o que é verdade ou mentira no Brasil", bem abaixo da caixa de busca da página inicial do Google. O link direcionava para um post do blog do Google com inúmeras críticas ao projeto (PINOTTI, 2023). Além do Google, a Meta e o Spotify também se mobilizaram. Todas essas ofensivas foram registradas no levantamento feito pelo NetLab (2023).

A chamada "bancada das *big techs*", representa apenas uma das inúmeras bancadas existentes no país, as quais se referem a grupos de parlamentares que compartilham interesses ou afinidades em questões específicas. Esses grupos são formados por membros de um mesmo partido ou coligação, que trabalham em conjunto para promover determinadas políticas, leis ou representar os interesses de um setor específico da sociedade. No caso do PL das Fake News, a bancada das *big techs* esteve muito presente durante a votação em maio de 2023. Fez forte oposição ao projeto, culminando no adiamento da votação, sem data marcada para revisitar a matéria.

No entanto, antes da decisão de adiar a votação, cabe ressaltar que mais de 90 emendas foram enviadas ao relator do projeto. Dentre as sugestões de alterações, algumas foram incorporadas pelo relator, com o intuito de conciliar os interesses da Câmara com os principais pontos polêmicos.

O primeiro ponto se refere à pressão exercida pela bancada evangélica para a inclusão de um dispositivo que garantisse que conteúdos postados por líderes religiosos e seus seguidores não fossem removidos por plataformas sob a

alegação de serem considerados ofensivos à população LGBTQIA+ – muito embora a homofobia seja considerada crime desde 2019 (BRAGON *et al.*, 2023).

Outro ponto incluído foi a questão da imunidade parlamentar material prevista na Constituição Federal. Segundo o relatório, essa imunidade deve ser estendida aos parlamentares pelos conteúdos compartilhados em suas redes sociais. Além disso, também consta que contas de presidentes, governadores, prefeitos, ministros, secretários e outros cargos são consideradas de interesse público, proibindo-se que os detentores restrinjam a visualização de suas publicações por outros usuários.

Outro ponto polêmico diz respeito à remuneração por conteúdo jornalístico e à remuneração de direitos autorais. Estas sugestões, assim como outras, revelam que o texto em discussão traz, entre outros pontos, uma série de obrigações às plataformas digitais.

Por fim, o relator também retirou a previsão de uma agência reguladora, o que os opositores vinham apelidando de Ministério da Verdade, fazendo uma analogia com a instituição descrita no livro *1984*, de George Orwell, que controlava de forma autoritária a circulação de informação.

Todos esses apontamentos revelam de maneira explícita que, por trás da aprovação do projeto de lei, há inúmeros interesses políticos e econômicos. Como consequência, o sistema jurídico se vê em um emaranhado de disputas políticas entre os diferentes sistemas envolvidos no jogo político, resultando em uma incapacidade de regular adequadamente as redes sociais e lidar com o problema das *fake news*.

A aprovação de leis relacionadas às redes sociais não ocorre em um vácuo isolado; ao contrário, reflete as dinâmicas intrincadas de interesses diversos que permeiam a esfera política e econômica. Por trás da aparência de uma legislação destinada a abordar questões cruciais, como o problema das *fake news*, está uma série de motivações que transcendem os objetivos aparentes do projeto de lei.

Os interesses políticos, muitas vezes, buscam moldar a legislação de acordo com agendas específicas, influenciando a redação das leis de maneira a favorecer certos grupos ou partidos. Por outro lado, os interesses econômicos

podem almejar a regulamentação de determinados aspectos das redes sociais para atender a objetivos financeiros e comerciais, muitas vezes à custa da integridade do debate público. Daí o cuidado da regulação em não cair no instrumentalismo jurídico.

Essa complexa interconexão de interesses cria um ambiente propício para disputas políticas, nas quais diferentes sistemas competem por influência na moldagem da legislação. Nesse contexto, a capacidade do sistema jurídico de regular adequadamente as redes sociais e enfrentar o desafio das *fake news* se vê comprometida, pois a legislação resultante pode ser moldada mais pelos interesses políticos e econômicos dominantes do que por uma abordagem objetiva e eficaz na promoção do bem público. Esses interesses são vistos nas inúmeras sugestões de alterações que foram feitas ao projeto desde o início da sua tramitação.

A incapacidade do sistema jurídico de atuar com eficácia nesse cenário cria um vácuo regulatório, permitindo que as lacunas na legislação sejam exploradas por atores mal-intencionados, exacerbando os desafios associados às *fake news* e à desinformação.

Nesse contexto, observamos que os provedores das plataformas digitais estão se aproveitando desse vácuo regulatório, pois é apenas em um cenário onde não existem limites claros de responsabilização e sanções que situações como as ofensivas contra a votação do projeto em abril de 2023 podem ocorrer. Na mesma linha, vemos agentes políticos fazendo amplo uso das redes sociais para se beneficiarem ao promoverem a desinformação e a manipulação de apoiadores. Como explorado nos parágrafos acima, as redes sociais alteraram o jogo político nos últimos anos. Assim, as consequências desse vácuo regulatório são incalculáveis, mas até o momento já foram suficientes para mostrar a urgência do assunto. Os atos antidemocráticos de 8 de janeiro de 2023, assim como os inúmeros ataques às escolas, são apenas exemplos do poder e influência das redes sociais na sociedade.

2.3. De volta à metarregulação como resposta ao trilema regulatório

Como discutido, o direito estatal, imerso em seu próprio arcabouço normativo, mostra-se limitado na capacidade de oferecer respostas regulatórias rápidas e efetivas ao problema das *fake news*. Isso ocorre, em parte, devido à dinâmica singular do sistema de comunicação de massa digital, cujas nuances e complexidades escapam ao escopo tradicional do direito estatal. Além disso, a regulação das *fake news* deve ser considerada em face do pluralismo jurídico da sociedade mundial, evidenciando-se que as respostas eficazes demandam não apenas a ação do direito estatal, mas também a consideração e interação com normas e sistemas jurídicos variados que coexistem na sociedade.

A incapacidade do direito estatal em oferecer respostas regulatórias ágeis e efetivas é, em grande parte, uma consequência da dinâmica autorreferente singular do sistema de comunicação de massa. Uma dinâmica acelerada que advém do dinamismo do mundo digital, o que aumenta a incerteza sobre a eficácia de qualquer proposta de regulação. Neste contexto, vimos que a rapidez das transformações no cenário digital impõe a necessidade de abordagens mais criativas e experimentais na elaboração de regulamentações, a fim de lidar adequadamente com essa tarefa complexa. O contexto em constante evolução exige não apenas um entendimento aprofundado das dinâmicas digitais, mas também a flexibilidade necessária para ajustar as regulamentações à medida que novas tendências e desafios emergem.

Em face dessa incapacidade, surge como alternativa o instituto da autorregulação regulada ou metarregulação, o qual procura conciliar as vantagens e desvantagens da autorregulação e da relação estatal. Por um lado, a autorregulação possui a vantagem da eficiência, por conhecer facilmente as estruturas técnicas e dinâmicas internas de seu próprio setor. Mas, por outro lado, tem a desvantagem de não seguir necessariamente interesses e valores públicos. No caso da regulação estatal, tem a vantagem de perseguir os interesses e valores públicos, mas a desvantagem de não prover do conhecimento necessário para lidar com ambientes dinâmicos como no caso das redes sociais (MARANHÃO *et al.*, 2021).

Na busca por uma abordagem mais equilibrada e adaptável, conciliando vantagens e desvantagens, a autorregulação regulada se apresenta como uma solução inovadora. Esse modelo propõe a criação de um arcabouço regulatório que, embora mantendo a autonomia e a eficiência da autorregulação, incorpora elementos de supervisão e diretrizes estabelecidas pelo poder público. Dessa forma, a autorregulação regulada consegue mitigar as deficiências inerentes à autorregulação pura, que muitas vezes carece de uma supervisão externa robusta para garantir que os interesses públicos sejam adequadamente considerados. Ao mesmo tempo, lida com o problema da regulação estatal tradicional, uma regulação de cima para baixo, que não consegue se adaptar em um ambiente dinâmico e complexo de peculiaridades próprias, permitindo um afastamento da rígida burocracia formalizada, hierarquizada e autocontida inerentes ao aparelho estatal. Assim, essa forma de regulação permite que o Estado consiga lidar melhor com uma sociedade que cada vez mais se se locomove e se distancia de uma sociedade centrada em organizações, conseguindo absorver melhor as incertezas e construir parâmetros melhores de eficácia na regulação.

Como visto no tópico anterior, o Projeto de Lei das Fake News incorporava em seu art. 30 o conceito de "autorregulação regulada", mas ele foi retirado em sua última versão. O dispositivo previa que a autorregulação nesse setor deveria ser certificada pelo "Conselho de transparência e Responsabilidade na Internet". A ideia era vista como uma forma de institucionalizar o "princípio da correção", presente em diversos outros ordenamentos e propostas regulatórias, como na lei alemã para a melhoria da aplicação da lei nas redes sociais (NetzDG, de 2017) ou nas recomendações da União Europeia sobre a regulação das mídias.

Mecanismos de regulação da autorregulação assentam-se em um tripé que busca catalisar a capacidade de aprendizagem e autocontrole organizacional. Inicialmente, esses mecanismos devem assegurar transparência, proporcionando acesso e visibilidade das informações ao público, além de permitir avaliação por corpos independentes, com mandato desvinculado da liderança da própria agência ou departamento monitorado, evitando interferências. Em seguida, é essencial que existam canais para o recebimento e processamento de denúncias

por partes interessadas, bem como para a investigação e sanção de condutas não conformes. Por fim, os mecanismos se legitimam ao procedimentalizar a inclusão decisória das partes afetadas, variando em graus que podem ir desde a simples consulta ou audiência até o conferimento de direitos mais amplos de voto e veto.

O art. 30 do PL das *Fake News* incorporava esses mecanismos e se direcionava aos "provedores de redes sociais e de serviços de mensageria privada", estabelecendo diretrizes para a abertura de canais de reclamação e monitoramento de denúncias. Além disso, delineava procedimentos para a suspensão de contas inautênticas. O dispositivo sugeria a construção de uma normatividade própria por meio de resoluções e súmulas. Também indicava a obrigação de garantir a transparência por meio da apresentação de relatórios periódicos ao Conselho de Transparência e Responsabilidade na Internet, um órgão misto composto por representantes de diversos Poderes, agências do Estado e da sociedade civil.

O instituto da autorregulação regulada proposto na versão antiga do Projeto de Lei das *Fake News* não é o primeiro a aparecer no ordenamento jurídico brasileiro, como no caso do mercado de corretagem de seguros, resseguros, capitalização e previdência complementar aberta, no qual entidades autorreguladoras atuam em auxílio e sob a supervisão da Susep; ou no caso da Anbima, entidade de direito privado que se autorregula e é regulada pelo Banco Central e pela CVM.

A exclusão do dispositivo reflete a influência exercida por outros sistemas no sistema político. Sob a justificativa de que a criação de um órgão regulador poderia equivaler a um "Ministério da Verdade", promovendo censura e repressão, o art. 30 foi removido da última versão. Essa exclusão é vista com pesar, considerando que o conceito de autorregulação regulada representava grande potencial para viabilizar a construção jurídica experimental de parâmetros normativos destinados a enfrentar o fenômeno da disseminação das *fake news*. Isso porque, ao se promover a troca de conhecimentos entre o Direito estatal (atuando como "metarregulador") e o Direito autorregulado, amplia-se a capacidade de compreender a natureza técnica das plataformas digitais e de

convertê-la para formas jurídicas de categorização de condutas, atribuição de responsabilidades e aplicação de sanções.

Nesse sentido, a maior vantagem potencial da autorregulação regulada é procedimentalizar e institucionalizar uma dinâmica de observação e aprendizagem mútua entre Direito estatal e ordens jurídicas privadas, o que parece essencial em tópicos ainda pouco programados pelo sistema jurídico, como aqueles temas relacionados ao desenvolvimento e à difusão das tecnologias digitais.

Conclusão

Esse capítulo procurou explorar as nuances e implicações da crise regulatória em que o Estado brasileiro se encontra para lidar com a dinâmica dos novos meios de comunicação. Dessa forma, vimos que o fenômeno da propagação de *fake news*, com sua natureza inovadora e capacidade de multiplicação em massa, não apenas exige uma resposta normativa criativa, mas também uma redefinição profunda dos mecanismos regulatórios e institucionais por parte do Estado.

Constatamos que o direito, ao enfrentar esse dilema regulatório, não pode se limitar à mera normatização de direitos e deveres ou à principialização das normas, mas deve estender-se à concepção dos próprios canais pelos quais os programas e órgãos decisórios são construídos. Certa versão da proposta legislativa brasileira relativa às *fake news* se mostrava estar caminhando nesse sentido, delineando um modelo para outros setores de políticas públicas, com a proposta de implementar o instituto da autorregulação regulada.

Entretanto, não podemos negligenciar as complexidades inerentes à dinâmica de implementação de qualquer modelo de regulação da internet. Isso porque a regulação da internet esbarra em fundamentos basilares do estado democrático de direito, como vimos na discussão sobre os cenários regulatórios da liberdade de expressão. Cabe ao Estado buscar um cenário onde se tenha uma liberdade de expressão moderada, representando um delicado equilíbrio entre garantir a livre manifestação de ideias, preservando o direito à liberdade de

expressão, e combater a disseminação de *fake news* por meio da regulação do ambiente digital.

Além disso, a partir de uma perspectiva sistêmica, foi possível compreender as controvérsias que impactam a aprovação do Projeto de Lei das Fake News, indicando que a implementação de uma regulação envolve interesses políticos e econômicos que não podem ser ignorados. Vimos que, por conta disso, o instituto da autorregulação regulada foi retirado do projeto na última versão que esteve preparada para votação (em meados de 2023), sob a justificativa de que um órgão regulador poderia surtir em uma espécie de "Ministério da Censura", o que implica que a sua inserção na próxima votação irá depender do jogo político a ser exercido pelos seus defensores na Câmara dos Deputados. Desse modo, espera-se que o instituto volte a ser incluído no Projeto de Lei das *Fake News* (de futuro ainda incerto neste final de 2024), tendo em vista o seu grande potencial para viabilizar a construção jurídica experimental de parâmetros normativos para lidar com o fenômeno da disseminação das *fake news*.

Referências

AMATO, Lucas Fucci. Fake news: regulação ou metarregulação? **Revista de Informação Legislativa**, Brasília, DF, v. 58, n. 230, p. 29-53, abr./jun. 2021. Disponível em: https://www12.senado.leg.br/ril/edicoes/58/230/ril_v58_n230_p29 . Acesso em: 01 out. 2023.

AMATO, Lucas Fucci. PL 2630: Fake news e aprendizagem regulatória. **Jota**, 2023. Dispónivel em: https://www.jota.info/opiniao-e-analise/artigos/fake-news-e-aprendizagem-regulatoria-15062023 . Acesso em: 03 de nov. de 2023.

AMATO, Lucas Fucci; MISSAGIA, Caio Rezende. Ambientes regulatórios experimentais: O sandbox no sistema financeiro brasileiro. **RBSD – Revista Brasileira de Sociologia do Direito**, v. 10, n. 3, p. 143-171, set./dez. 2023.

AMATO, Lucas Fucci; SABA, Diana Tognini; BARROS, Marco Antonio Loschiavo Leme de. Sociologia Jurídica das Fake News Eleitorais nas Eleições

Brasileiras de 2018. **Revista de Direito Público**, Brasília, v. 18, n. 99, p. 539-564, jul./set. 2021. Disponível em: https://www.academia.edu/60323821/Sociologia_Jur%C3%ADdica_das_Fake_News_Eleitorais_uma_Observa%C3%A7%C3%A3o_Sist%C3%AAmica_das_Respostas_Judiciais_e_Legislativas_em_Torno_das_Elei%C3%A7%C3%B5es_Brasileiras_de_2018 . Acesso em: 01 out. 2023.

ARRAES, Bruno Henrique Rodrigues; CAMARGO, Liriane Soares de Araújo de; CARVALHO, A Angela Maria Grossi de; CASTRO, Fabiano Ferreira de. Tecnologias da Informação e Comunicação Como Recurso Interativo na Perspectiva da Ciência da Informação. **Revista Eletrônica Informação e Cognição**, v. 6, n. 1, p. 3-15, 2007.

BRAGON, Ranier; BRANT, Danielle; AZEVEDO, Victoria; MACHADO, Renato; LOPES, Raquel; REZENDE, Constança. PL das Fake News une Lula, Lira e STF contra big techs, bolsonaristas e evangélicos. **A Folha de São Paulo**, publicado em 3 maio 2023. Disponível em: https://www1.folha.uol.com.br/poder/2023/05/pl-das-fake-news-une-lula-lira-e-stf-contra-big-techs-bolsonaristas-e-evangelicos.shtml Acesso em: 10 out. 2023.

CAMILLOTO, Bruno; URASHIMA, Pedro. Liberdade de expressão, democracia e cultura do cancelamento. **Revista de Direito da Faculdade Guanambi**, Guanambi, v. 7, n. 02, p. e317, 2021, p. 8. DOI: 10.29293/rdfg.v7i02.317. Disponível em: https://portaldeperiodicos.animaeducacao.com.br/index.php/RDFG/article/view/13941 . Acesso em: 29 nov. 2023.

CAMPILONGO, Celso Fernandes. **Interpretação do direito e movimentos sociais:** hermenêutica do sistema jurídico e da sociedade. Rio de Janeiro: Campus Elsevier, 2012.

CARROZZA, Jéssica Pereira Arantes Konno. **Direito e movimentos sociais digitais na sociedade complexa:** uma leitura a partir da teoria dos sistemas sociais de Niklas Luhmann. 2023. Dissertação (Mestrado em Direito) – Faculdade de Direito do Sul de Minas, Pouso Alegre, 2023.

CNN BRASIL. Brasil registra 9 ataques em escolas neste ano e atinge patamar recorde; relembre casos. **CNN Brasil**, publicado em 23 out. 2023. Disponível em: https://www.cnnbrasil.com.br/nacional/brasil-registra-9-ataques-em-escolas-neste-ano-e-atinge-patamar-recorde-relembre-casos/ . Acesso em: 10 out. 2023.

FALCAO, Joaquim. Narrativas fake e fake news. **Jota**, 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/narrativas-fake-e-fake-news-14112022. Acesso em: 10 out. 2023.

FAUSTINO, André. **Fake news**. São Paulo: Lura, 2019.

G1. Grupos neonazistas crescem 270% no Brasil em 3 anos; estudiosos temem que presença online transborde para ataques violentos. **G1**, publicado em 16 jan. 2022. Disponível em: https://g1.globo.com/fantastico/noticia/2022/01/16/grupos-neonazistas-crescem-270percent-no-brasil-em-3-anos-estudiosos-temem-que-presenca-online-transborde-para-ataques-violentos.ghtml . Acesso em: 10 out. 2023.

GARCIA, Rafael. 7% dos brasileiros afirmam que Terra é plana, mostra pesquisa. **A Folha de São Paulo**, publicado em 14 jul. 2019. Disponível em: https://www1.folha.uol.com.br/ciencia/2019/07/7-dos-brasileiros-afirmam-que-terra-e-plana-mostra-pesquisa.shtml . Acesso em: 10 out. 2023.

LUHMANN, Niklas. **A realidade dos meios de comunicação**. Tradução de Ciro Marcondes Filho. São Paulo: Paulus, 2005.

LUHMANN, Niklas. **Theory of society**. Translated by Rhodes Barrett. Stanford, CA: Stanford University Press, 2013. v. 2. (Cultural Memory in the Present).

MARANHÃO, Juliano; CAMPOS, Ricardo; GUEDES, Jéssica; OLIVEIRA, Samuel Rodrigues de; GRINGS, Maria Gabriela. **Regulação de "Fake News" no Brasil**. São Paulo: Instituto Legal Grounds, 2021.

MELLO, Marcelo Pereira de. A perspectiva sistêmica na sociologia do direito: Luhmann e Teubner. **Tempo Social, revista de sociologia da USP**, v. 18, n. 1, p. 351-373, 2006.

NEVES, Rômulo Figueira. **Acoplamento estrutural, fechamento operacional e processos sobrecomunicativos na teoria dos sistemas sociais de Niklas**

Luhmann. 2005. Dissertação (Mestrado em Sociologia) – Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2005.

NetLab-UFRJ (LABORATÓRIO DE ESTUDOS DA INTERNET E MÍDIAS SOCIAIS). **A guerra das plataformas contra o PL 2630** - NetLab UFRJ, abril 2023. Disponível em: https://uploads.strikinglycdn.com/files/2cab203d-e44d-423e-b4e9-2a13cf44432e/A%20guerra%20das%20plataformas%20contra%20o%20PL%202630%20-%20NetLab%20UFRJ,%20Abril%202023.pdf . Acesso em: 10 out. 2023.

NEXO. Twitter admite que seus algoritmos favorecem a direita. **Nexo**, 22 out. 2021. Disponível em: https://www.nexojornal.com.br/extra/2021/10/22/Twitter-admite-que-seus-algoritmos-favorecem-a-direita . Acesso em: 10 out. 2023.

O´NEILL, Brendan. **Freedom of Speech and Right to Offend | Proposition.** 2015. Disponível em: https://www.youtube.com/watch?v=BtWrljX9HRA . Acesso em: 10 out. 2023.

PINOTTI, Fernanda. Google retira mensagem contra PL das Fake News da página inicial. **CNN Brasil**, publicado em 2 maio 2023. Disponível em: https://www.cnnbrasil.com.br/politica/google-retira-mensagem-contra-pl-das-fake-news-da-pagina-inicial/ . Acesso em: 10 out. 2023.

ROCHA, João Cezar de Castro. **Guerra cultural e retórica do ódio**: crônicas de um Brasil pós-político. Goiânia: Caminhos, 2021.

SABA, Diana; AMATO, Lucas Fucci; BARROS, Marco Antonio Loschiavo Leme de; PONCE, Paula Pedigoni. **Fake news e eleições:** estudo sociojurídico sobre política, comunicação digital e regulação no Brasil. Porto Alegre: Editora Fi, 2021. Disponível em: https://www.editorafi.org/203fakenews . Acesso em 13 abr. 2024.

SALAS, Javier. Movimento antivacina cresce em meio à pandemia. **El País**, publicado em 4 jun. 2020. Disponível em: https://brasil.elpais.com/ciencia/2020-06-04/movimento-antivacina-cresce-em-meio-a-pandemia.html . Acesso em: 10 out. 2023.

SENADO FEDERAL. **Projeto de Lei n° 2630, de 2020**. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8110634&disposition=inline . Acesso em: 10 out. 2023.

TEUBNER, Gunther. Substantive and reflexive elements in modern law. **Law & Society Review**, v. 17, n. 2, p. 239-285, 1983.

TEUBNER, Gunther. After legal instrumentalism? Strategic models of post-regulatory law. *In*: TEUBNER, Gunther (ed.). **Dilemmas of law in the welfare state**. Berlin: Walter de Gruyter, 1986, p. 299-325. (European University Institute – Series A, 3).

TV SENADO. 8 de janeiro: um ataque à democracia do Brasil. **TV Senado**, publicado em 27 fev. 2023. Disponível em: https://www12.senado.leg.br/tv/programas/tela-brasil/2023/02/8-de-janeiro-um-ataque-a-democracia-do-brasil . Acesso em: 10 out. 2023.

URGENT REPORT **How Meta and Google enabled and profited from the terrorist attacks in Brazil's capital.** Disponível em: https://s3.amazonaws.com/s3.sumofus.org/images/Research_SumOfUs_Brazilian_Riots_January_11th_2023.pdf/ . Acesso em: 10 out. 2023.

VESTING, Thomas. **Legal theory and the media of law**. Londres: Edward Elgar, 2018.