EthicAI
Nº 1
NOVEMBRO/2021
ethicai.com.br

EXPEDIENTE EDITORIAL

Diretor científico: Willis S. Guerra Filho
Vice-diretora científica: Paola Cantarini
Editores executivos: Lucia Santaella, Winfried Nöth, Urbano Nobre Nojosa
Revisão de texto e normatização: Anna Carolina Pinho dos Anjos, Zilda Gonçalves, Jhesica Baccari
Capa e projeto gráfico: Paola Cantarini

CONSELHO EDITORIAL

OBJETIVOS

Pretendemos com a Revista Científica Ethicai alcançar um público mais amplo, não apenas acadêmico, utilizando-se para tanto também da linguagem lúdica das artes, além da abordagem interdisciplinar, buscando assim uma perspectiva includente, democrática, e ao mesmo tempo científica, mas, sobretudo, uma visão não polarizada, por holística e inclusiva para se repensar as ambivalências e contradições nestes campos do pensamento.

O Instituto Ethicai é uma associação sem fins econômicos ou lucrativos com foco em promover a aplicação ética da tecnologia com emprego da IA, por meio do diálogo entre academia, empresas, órgãos governamentais, artistas e estudantes em geral, produzindo estudos científicos e avançados, contribuindo para a discussão científica e mútuo enriquecimento entre as áreas das ciências, "duras" ou não. Visa-se contribuir para o desenvolvimento das pesquisas científicas com foco na interseção da IA, novas tecnologias e humanidades, de forma a promover a inovação, e de outro lado, verificar os principais desafios e impactos, externalidades positivas e negativas.

Visa-se, com tais publicações disponibilizar uma arena e espaço de debate e diálogo democrático, amplamente aberto, a fim de trazer uma visão não polarizada, não pessimista nem otimista, mas realista, holística e inclusiva para se repensar as ambivalências e contradições que se apresentam.

EIXOS TEMÁTICOS

Linhas de pesquisa:

I. TEORIA DA IA
1. IA e humanidades: autonomia, consciência e responsabilidade
2. IA e filosofia: aspectos filosóficos, éticos e críticos da IA
3. IA e sociedade: Impactos sociais e transformações disruptivas causadas pela IA
4. IA e cultura: Cultura digital (cybercultura)
5. IA, política e comunicação
6. IA e educação: aprendizagem, "Educação 4.0"
7. Ética digital intercultural.
8. Arte, Design e IA
9. IA e Negócios: "Indústria, Serviço, Agricultura 4.0"
10. IA e disrupção/inovação: blockchain, internet das coisas, dos serviços e das emoções (IoT), cidades Inteligentes
11. IA e psicologia: affective computing
12. IA e Direito

II. EMPIRIA DA IA

O CONSUMO DE TELEDRAMA-TURGIA SOB A PANDEMIA: UM ESTUDO DE (MEU) CASO

MARCO ANTONIO PERRUSO
– Professor de Sociologia da UFRRJ

No início da pandemia, ainda no primeiro semestre de 2020, muitos de nós entramos em quarentena. Sendo professor de universidade pública, podia me confinar com minha companheira. Entre doações financeiras para trabalhadores pobres e a luta para atenuar toda a precariedade do ensino remoto que impactava os estudantes periféricos, intercalando panelaços contra o genocida Bolsonaro e a participação virtual em atividades científicas, sindicais e partidárias, me dedicava a sondar o que poderia escapar do padrão hollywoodiano em plataformas de streamings de filmes e séries. Era uma das poucas opções de consumo cultural que nos restava.

Depois de alguns meses, percebi que espontaneamente eu passara a buscar obras teledramatúrgicas que coadunassem com o momento que vivíamos – e ainda estamos vivendo, embora o "novo" normal pareça cada vez mais o "velho" normal anterior à pandemia. Filmes e seriados distópicos já estavam na moda bem antes, como Black Mirror, O Conto da Aia, o novo Mad Max e tantos outros. Com a crise mundial do capitalismo, agravada pelo coronavírus, e a ascensão política do populismo de extrema-direita, tão desmoralizante para a burguesia internacional aspirante a uma hegemonia política e cultural sofisticada, o antecedente estilístico e temático já estava dado. Tudo se passava - e ainda se passa – como se as previsões escatológicas estivessem concretizando-se a partir do início de 2020. Podíamos – podemos? – viver o fim do mundo, um momento histórico inigualável que nos horroriza, ao mesmo tempo que, ironicamente, nos honra ao oferecer a oportunidade de presenciá-lo.

No Brasil, parte da classe trabalhadora mais intelectualizada e menos precarizada já vivia tal sensação por conta da crise do lulismo. Muitos apavoraram-se com Temer, figura tétrica que, no entanto, é um gentleman (no bom e no mau sentido da palavra, tanto faz neste caso) perto de Bolsonaro. A partir de 2019, a coisa piorou bastante, como se sabe, a despeito de importantes mobilizações populares (presenciais mesmo, nem um pouco anacrônicas), antes e durante a pandemia.

Alguns filmes ou séries, obviamente realizados antes de março de 2020, de fato pareciam proféticos. Mas certamente nos falavam da nossa condição singular de "quarentenados", relativamente privilegiados, antes do que da situação de vítimas maiores do colapso global, os quais seguem nas ruas trabalhando (ou buscando trabalho) sem direitos sob o capitalismo de plataforma, hiperprecarizador.

Entre as distopias mais ou menos tecnológicas que assisti, quase sempre de fundo romântico, conforme o pensamento social alemão (de Herder até Habermas) que teme a mecanização e o desencantamento das comunidades humanas, vale citar dois seriados: Electric Dreams (produção inglesa de 2017, baseada na ficção científica de Philip K. Dick, cultuado escritor estadunidense da segunda metade do século XX); e a nova versão de Além da Imaginação (com Jordan Peele à frente, entre outros), baseado na série clássica da TV dos EUA do mesmo período histórico. Não é coincidência que a literatura e a teledramaturgia em questão sejam originárias dos anos 1950 em diante, período da Guerra Fria e, portanto, do temor de um fim do planeta via holocausto nuclear (ou ao menos, do fim do american way of life por conta de uma invasão comunista ou – sua metáfora – extraterrestre). A pandemia do covid-19, agravada pelos Trumps e Bolsonaros do mundo, bem como por toda a sociabilidade burguesa, ajusta-se perfeitamente ao papel de substituto contemporâneo do confronto

último dos três campos. Porque o signo é, antes de mais nada, processo (semiose). Trata-se de uma espécie de pacto efêmero, um contrato fragílimo, um conluio entre um nome (representamen), uma coisa (objeto) e uma idéia (interpretante), mal se constitui e evanesce, sempre disposto a se recompor em novos acordos e novas combinações, ilimitadamente, muitas vezes, quiçá em maioria, às largas da vontade de uma consciência[29].

Arte-signo. Arte-processo. Só assim é possível pensar o "significado artístico"[30]. De certo, todas as considerações feitas até aqui devem ser postas em pauta quando o que estiver valendo for a busca pela especificidade deste processo: o que o diferencia de outros processos sígnicos? Há algo que o especifica mesmo? Qual o resultado, em termos de consciência, do signo artístico? Transversalmente, tais questões são atravessadas pela função metafórica[31] e, é possível que, nela se resolvam. No tempo oportuno, por processos incontroláveis e imprevisíveis, a matéria do mundo se organiza para nós em termos de consciência de maneira que dela emane, que brilhe em torno desta matéria, um sentido terceiro, obtuso[32], imponderável; a metáfora; a arte.

Não seria, então, finalmente apenas um problema de interpretação? Que só no nível da interpretação é que o processo poder ser dito se artístico ou não?

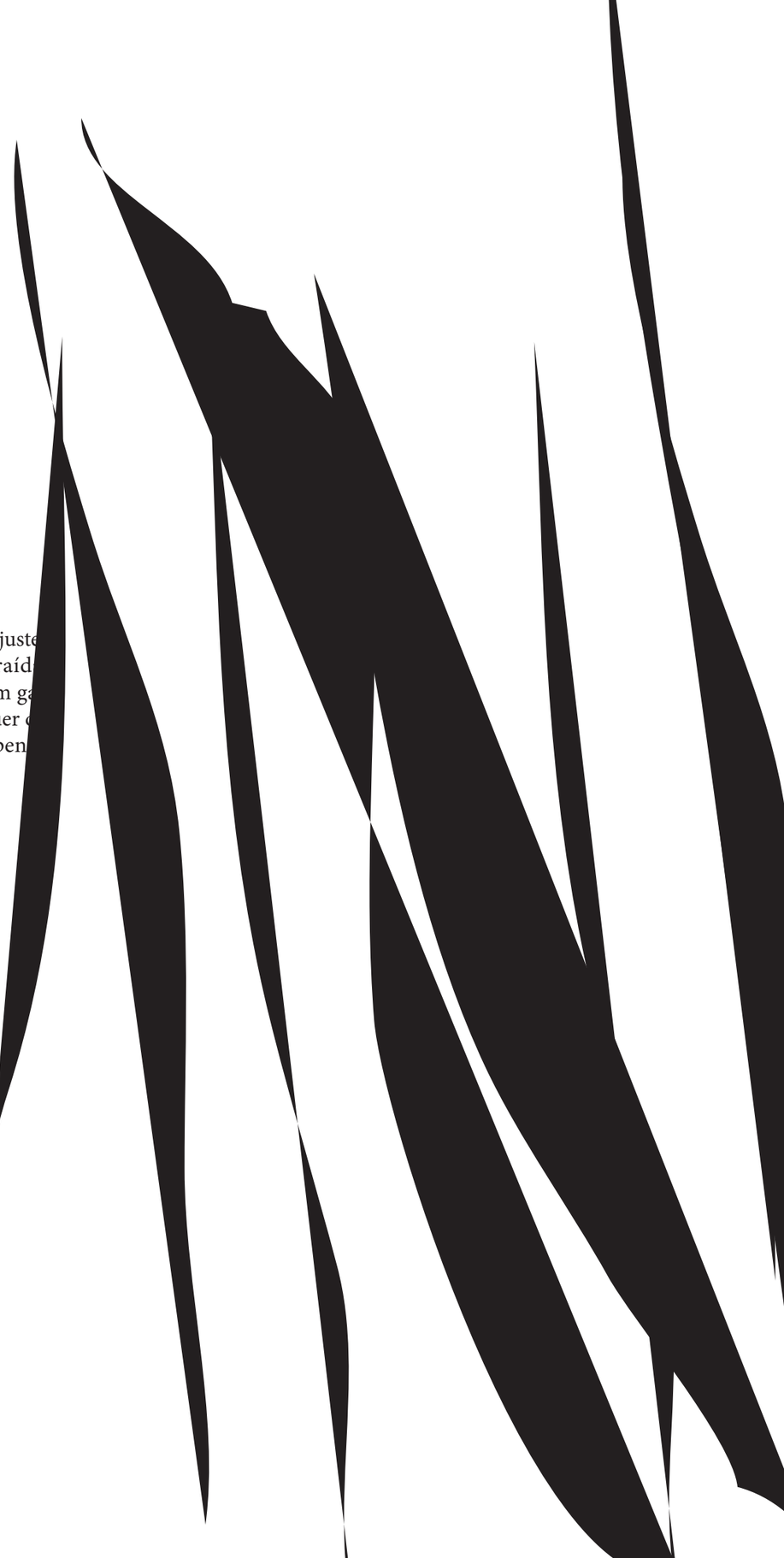
> Interpretation is our reception of events and artifacts, and how we make meaning from them. I expect you are familiar with the semiotic notion that "a sign... is something which stands to somebody for something in some respect or capacity" (Peirce 1932: §2.228). So a sign comes into being as meaningful when it is meaningful to an individual, not because of some intrinsic property the artifact has outside of social communication. What social communication brings is not only the interpreting individual, but also the network of signs that forms a context for interpretation. This shows that the context that we perceive and use, the network, is just one of many possible contexts that are available in any given situation. As I said, context is not just physical situation, but intellectual point-of-view [33]

[Um anjo de rapina... há interpretação possível?]

À cabeceira do menino ele está. Suponho.

(Re)componho a cena do presépio a partir dos fragmentos de memória (o menino Jesus no caixote, o Rei presenteado...) e da presença material concreta do anjo aqui comigo; uma arqueologia mnemônica. Não fosse isso, o método seria no todo dedutivo. Partiria do modelo geral de presépio, estereotipado, aquele que invade as vitrines e cartões durante as festas – nele, mesmo nas versões mais compactas, Jesus+Maria+José, quando aparece, o anjo flota sobre todos com asas abertas em envergadura plena: "Glória in excelcis Deo!" –, sim, partiria dele para imaginar o meu próprio. De algum modo, não abandono a via peremptoriamente, mas a figura do anjo me força a ajuste

Não só as asas contraíd
do mesmo jeito a falta de um ga
cho ou outro recurso qualquer
indicasse um modo de suspen
da estatueta e, por fim e



INTELIGÊNCIA ARTIFICIAL E DIREITO – REGULAÇÃO PELA ARQUITETURA TÉCNICA E TRANSPARÊNCIA DO DESIGN ALGORÍTMICO

PAOLA CANTARINI
WILLIS GUERRA

Resumo:

Problema proposto: como equilibrar via ponderação a necessária observância do segredo industrial e comercial que envolvem os programas de computador e os algoritmos de IA, a proteção via propriedade intelectual, vistos de forma absoluta muitas vezes nesta seara? Ao se analisar de forma literal e gramatical a LGPD em seus artigos 10, § 3º e artigo 20, § 1º e § 2º pode-se chegar à equivocada conclusão de que o segredo industrial sempre irá preva-lecer, mesmo diante de direitos básicos do titular ou de seus Direitos Fundamentais. Co-mo fazer ju e tornar efetivos o principio da explicabilidade e da transparencia, envolvendo não apenas os dados pessoais, banco de dados mas sobretudo, o design técnico e a transpa-rencia algorítmica, de forma a não obstar a inovação e impedir o exercício de atividade económica?

Objetivo da investigação: Visa-se analizar o estado da arte no tocante à problemática apontada, de forma a se observar o princípio da explicabilidade e da transparencia, e tornar efetivos os direitos à explicação e à revisão de uma decisão automatizada, analizando-se as propostas intepretativas na arena internacional e no Brasil.

Metodologia de pesquisa: a metodologia e as técnicas de pesquisa irão conjugar pesquisa teórica no âmbito nacional e internacional, promovendo o diálogo entre os diversos cam-pos do saber, em uma visão interdisciplinar.

Principais conclusões: O direito à explicação, à revisão de uma decisão automatizada em muitos casos dependerá do acesso aos parâmetros da tomada de decisão, mas também da quebra do código fonte, tornando possível o acesso às máximas e aos critérios em que se baseia a decisão, abrangendo a informação utilizada como input e, no caso dos sistemas de aprendizagem, as regras de formação utilizadas, se necessário também o tipo de utilização da análise de Big Data, envolvendo, pois, os aspectos da acessibilidade e compreensibili-dade. O segredo industrial não poderá ser interpretado e reconhecido como sendo um direito absoluto, contudo, tendo em vista a realidade brasileira, diante da insegurança do processo judicial sob segredo de justiça, há que se pensar em outra alternativa, tal como a inversão do ônus da prova, proposta esta que parece estar de acordo com o procedimento da ponderação e aplicação da proporcionalidade, prestigiando todos os direitos fundamen-tais em colisão, no sentido de evitar-se a afronta o núcleo esencial destes.

Palavras-chave: Inteligência artificial; regulação pela arquitectura técnica; transparencia no design

Abstract:

Proposed problem: how to balance via weighting the necessary observance of industrial and trade secrets involving computer programs and AI algorithms, the protection via intellectual property, seen absolutely many times in this field? By analyzing literally and grammatically the LGPD in its articles 10, § 3 and 20, § 1 and § 2, one can reach the mistaken conclusion that industrial secrets will always prevail, even in the face of the holder's basic rights or Fundamental Rights. How to make the principle of explainability and transparency effective, involving not only personal data, databases, but above all, technical design and algorithmic transparency, so as not to hinder innovation and prevent the exercise of economic activity?

Research Aim: The aim is to analyze the state of the art regarding the problem pointed out, in order to observe the principle of explainability and transparency, and make effective the rights to explanation and review of an automated decision, analyzing the interpretative proposals in the international arena and in Brazil.

Research Methodology: The research methodology and techniques will combine theoretical research in the national and international arena, promoting dialogue between the various fields of knowledge, in an interdisciplinary vision.

Main conclusions: The right to explanation, to review an automated decision in many cases will depend on access to the parameters of decision making, but also on the breaking of the source code, making it possible to access the maxims and the criteria on which the decision is based, covering the information used as input and, in

the case of learning systems, the training rules used, if necessary also the type of use of Big Data analysis, thus involving the aspects of accessibility and comprehensibility. The industrial secret cannot be interpreted and recognized as an absolute right, however, in view of the Brazilian reality, in face of the insecurity of the judicial process under secrecy of justice, it is necessary to think of another alternative, such as the inversion of the burden of proof. This proposal seems to be in accordance with the procedure of ponderation and application of proportionality, giving prestige to all fundamental rights in collision, in order to avoid the affront to the essential core of these rights, in such a way as to completely annihilate one of these rights, even in the sense of prestige of the other fundamental right.

Keywords: Artificial intelligence; regulation by technical architecture; design transparency

Artificial intelligence and Law - regulation by technical architecture and transparency of algo-rithmic design

PAOLA CANTARINI
WILLIS GUERRA

1.INTRODUÇÃO

É essencial que as temáticas relativas à Inteligência artificial, big data e proteção de dados sejam analisadas à luz de uma perspectiva inclusiva, interdisciplinar, e a partir do reconhecimento da multidimensionalidade dos Direitos Fundamentais, da coletivização e da risquificação, considerando-se como uma espécie de direito ambiental da proteção de dados pessoais, em especial quando diante de sua relação com o big data.

A partir do reconhecimento da tríplice dimensão ou multidimensionalidade de to-do Direito Fundamental, há o reconhecimento dos seus aspectos individual, coletivo e social, já que relacionados à cidadania e à igualdade material dos tutelados. Trata-se do reconhecimento de que um vazamento de dados ocorre como se fosse um sistema de po-luição de dados, afetando não apenas o titular, mas causando danos coletivos e sociais, devendo haver uma conjugação das formas de responsabilização ex post e ex ante.

É um modelo que deverá ainda ser reconhecido e aplicado no Brasil no âmbito da proteção de dados e big data, seguindo-se a área do direito ambiental de onde originou, contudo, impõe uma interpretação sistemática da legislação, superando-se, por exemplo, o entendimento gramatical, literal e ultrapassado, no sentido de se reconhecer apenas um caráter voluntário aos Relatórios de Impacto à Proteção de Dados, ou seja, que seria ne-cessária sua elaboração apenas após a solicitação pela ANPD. Uma interpretação sistemá-tica e à luz das novas propostas epistemológicas e hermenêuticas citadas no presente artigo demonstram sua ligação ao princípio da prevenção, à ideia de risquificação e coletivização, não havendo sentido sua elaboração "a posteriori", mesmo porque deverá contemplar todo o fluxo de dados e evitar a ocorrência de danos.

A partir do reconhecimento da múltipla dimensionalidade dos Direitos Fundamentais, é reconhecida sua aplicabilidade ou eficácia horizontal, e vertical, devendo ser redesenhada a aplicação da teoria da eficácia horizontal na esfera digital, como bem pontua Gunther Teubner, já que em sua formulação tradicional essa teoria adota uma perspectiva individualista, devendo ser ampliada para uma dimensão coletivo-institucional. Tal perspectiva possui contato com o movimento constitucional denomina-do de Constitucionalismo digital, visando a limitação do poder privado de atores da inter-net, voltando-se mais recentemente para a afirmação de Direitos Fundamentais na inter-net. Haveria uma equivalência com a noção de "declarações de direitos fundamentais na internet" (Internet Bill of Rights), consoante diversos expoentes defensores, Edoardo Ce-leste, Claudia Padovani e Mauro Santaniello e Meryem Marzouki.

Edoardo Celeste explica o conceito de Internet Bill of Rights, no sentido de reco-nhecer a existência de novos direitos fundamentais na internet, como o direito de acesso à internet, o direito ao esquecimento ou o direito à neutralidade da rede, com foco na prote-ção de direitos fundamentais na rede, com foco no dever de transparência . Visa, outros-sim, ao reconhecimento, afirmação e proteção de direitos fundamentais no ciberespaço, bem como no reequilíbrio de poderes entre os diversos atores no ambiente digital diante dos novos desafios e problemáticas relacionados ao uso das novas tecnologias, já que ocorre o estabelecimento das regras do jogo mediante termos de consentimento, termos de uso de serviços e produtos digitais, verdadeiros contratos de adesão, como uma espécie de função adjudicatória de direitos, funcionando como verdadeiros tribunais, o que fica bas-tante claro diante da iniciativa denominada de Comitê de Supervisão do Facebook, o Oversight Board ou "Suprema Corte do Facebook".

Trata-se de uma abordagem contraposta às perspectivas libertárias que reconhecem a melhor e única opção regulatória como sendo a autorregulação, autorregulação regulada, com fundamento na "proceduralização" (rectius: procedimentalização), apostando na téc-nica como forma primordial de solução de problemas complexos, com base em estudos clássicos como os de Lawrence Lessig.

2. MUDANÇA DE PARADIGMA E ARQUITETURA DE GERENCIAMENTO DE RISCOS

Diversos autores apontam para a necessidade de uma mudança de paradigma, ou ponto de virada na moldura teórica com relação à temática da proteção de dados, entre eles Bruno Bioni, Rafael Zanatta, Juliana Abrusio, e Nadezhda Purtova, professora de Til-burg, havendo, pois uma guinada de "informational self-determination" na direção da "in-formation-induced-harms", envolvendo o design responsável dos programas de computa-ção, códigos de boa conduta, certificações, auditorias independentes, e regulamentações ex ante.

No âmbito da regulação da inteligência artificial tal abordagem também vem sendo seguida, como podemos observar da recente proposta de regulamentação da IA pela Co-missão Europeia refletindo a análise entre diversas possibilidades regulatórias do setor, e de articulação com a já existente legislação setorial europeia, com foco na "GDPR – Regu-lamento Geral de Proteção de Dados da UE", no "Digital Services Act", no "Digital Mar-kets Act", no "White paper on IA" e no "Regulamento relativo à responsabilidade civil pelo uso da IA", em preparação. A Comissão Europeia entende, em suma, que a nova re-gulamentação é imprescindível para se possibilitar a inovação tecnológica e os progressos científicos, garantindo a necessária vantagem competitiva e liderança tecnológica da UE, em um contexto de forte concorrência mundial, mas sem deixar a preservação de direitos fundamentais e humanos, e de valores básicos consagrados pela UE, colocando a tecnolo-gia à serviço dos cidadãos europeus. A proposta de regulamentação da IA segue a estraté-gia europeia para a IA apresentada em 04/2018 denominada "Inteligência artificial para a Europa" (COM/2018/237), com foco nos valores europeus como forma de enfrentamen-to dos novos desafios da IA. A nova regulamentação, por sua vez, segue a ótica já traçada pela GDPR, por trazer uma regulamentação forte, em comparação com a regulamentação apenas moderada dos EUA, e fraca do Brasil, segundo parte da doutrina seguindo-se a perspectiva de "human rights by design", "beneficial AI", "AI for good" e "Human-Cente-red AI", ou seja, visa-se trazer um balanceamento entre o desenvolvimento tecnológico, de modo a não obstar a inovação, de um lado, e a proteção dos valores democráticos, direitos humanos e fundamentais, de outro lado. Parte-se da abordagem "centrada no ser huma-no", trazendo o eixo valorativo da pessoa humana e da dignidade humana. Referido docu-mento aponta para as preocupações com a centralização do ser humano, o controle huma-no da tecnologia, destacando o perigo de uma virtual "ligação emocional entre seres hu-manos e robôs", sobretudo em relação a grupos vulneráveis.

Em sentido semelhante a proposta de um "código de conduta para os engenheiros de robótica" (também aplicável aos demais atores na área de IA), trazendo a aplicação do princípio da transparência, por meio da criação de "caixas pretas" para aplicações de IA avançadas, preservando-se um "log" (registro) intangível de dados relativos a todas as ope-rações realizadas, abrangendo inclusive os passos da lógica que envolveu a produção da decisão automatizada.

Outra importante iniciativa no mesmo sentido é o denominado "White paper On Artificial Intelligence - A European approach to excellence and trust", de 19.02.2020, com foco na promoção da inovação científica, na preservação da liderança tecnológica da UE, trazendo a previsão de grande investimento financeiro no setor, mas ao mesmo tempo trazendo a garantia de proteção de direitos fundamentais, e mitigação de riscos, apontando para uma abordagem de análise de risco quanto às aplicações da IA.

Tais propostas vinculam-se, destarte, à abordagem da risquificação ou "risk-based approach", na linha da prática do "compliance", orientada para a probabilidade e gravidade do risco, em um processo proativo, sistemático e contínuo, com o incremento de regula-mentações "ex ante" com base no princípio da precaução, seguindo-se a ótica do direito regulatório.

3. TRANSPARÊNCIA NO DESIGN E NO ALGORITMO – PONDERAÇÃO NO CASO DE SIGILO IN-DUSTRIAL

Como equilibrar via ponderação a necessária observância do segredo industrial e comercial que envolvem os programas de computador e os algoritmos de IA, a proteção via propriedade intelectual, vistos de forma absoluta nesta seara? Ao se analisar de forma literal e gramatical a LGPD em seus artigos 10, § 3º e artigo 20, § 1º e § 2º pode-se chegar à equivocada conclusão de que o segredo industrial sempre irá prevalecer, mesmo diante de direitos básicos do titular ou de seus Direitos Fundamentais.

Segundo a LGPD, a ANPD poderá solicitar o Relatório de Impacto de proteção de dados no caso da base legal do interesse legítimo, observados os segredos comercial e in-dustrial, contudo, deverá ser realizada uma ponderação, diante do caso concreto, face à necessidade de respeitar outros Direitos Fundamentais em colisão, bem como em atenção ao princípio da transparência e da explicabilidade.

Como observar o princípio da explicabilidade, e tornar efetivos os direitos à expli-cação e à revisão de uma decisão automatizada, se não temos acesso aos parâmetros da tomada de decisão, sendo em alguns casos necessária a quebra do código fonte, a fim de melhor compreender os aspectos da decisão, envolvendo, pois, os aspectos da acessibilida-de e compreensibilidade?

Segundo Wolfgang Hoffmann-Riem , a proteção judicial das pessoas adversamente afetadas pode ser possibilitada pela introdução nos tribunais dos denominados procedi-mentos sigilosos; as empresas são obrigadas a revelar ao tribunal os algoritmos, em parti-cular algoritmos que podem ser utilizados para pôr em perigo a liberdade - as máximas e os critérios em que se baseiam, a informação utilizada como input e, no caso dos sistemas de aprendizagem, as regras de formação utilizadas, se necessário também o tipo de utiliza-ção da análise de Big Data. No entanto, essas

informações não deverão tornar-se públicas e não deverão ser acessíveis às partes no processo, ou apenas o serão numa medida limita-da, mas sim ao tribunal que aprecia os problemas, que pode, contudo, se necessário, man-dar proceder a um exame por peritos independentes.

Diante das possíveis limitações da regulação apenas via autorregulação, já que, por exemplo, tomando-se em conta os códigos de conduta, teríamos a elaboração unilateral e seletiva, podendo incrementar ainda mais as já existentes assimetrias de poder, então a heterorregulação estatal é indispensável, devendo ser complementada com incentivos para uma melhor concepção tecnológica, tal como a possibilidade de certificações e de auditori-as independentes, sujeitando-se a autorregulação a precauções materiais e processuais, envolvendo a participação de representantes da sociedade civil com poderes para controlar o cumprimento dos compromissos voluntários.

Os sistemas de regulamentação (heterorregulação e autoregulação) seriam comple-mentares, a fim de por eles se poder alcançar um sistema de proteção proativo, abrangente e sistemicamente seguro, uma proteção sistêmica.

Neste sentido, além da proteção pelo Estado destaca-se cada vez mais de forma complementar a proteção desde a concepção tecnológica (protection by design), envolven-do a criação de arquiteturas de decisão adequadas à proteção com o auxílio da concepção e de ferramentas tecnológicas, como forma de se implementar a segurança (security by de-sign).

Ao se postular pela regulação pela técnica envolvendo além da aplicação das PETS - Pri-vacy--enhancing Technologies -, tecnologias que visam o empoderamento do titular dos dados, trazendo uma melhor proteção aos Direitos Fundamentais, bem como pelo privacy by design e default, falando-se em transparência do design tecnológico, que vai muito além da transparência na coleta e tratamento de dados pessoais, banco de dados utilizado, mas sobretudo, implicaria na transparência do design tecnológico (o projeto técnico) e dos al-goritmos utilizados em cada caso, dos sistemas algorítmicos. No entanto, como bem apon-ta Wolfgang Hoffmann-Riem, a proteção dos segredos comerciais é contrária ao dever de divulgação.

Importante julgado conhecido como caso "Schufa", da lavra do Tribunal Federal de Justiça da Alemanha reconheceu, em princípio, a proteção ao segredo comercial em uma decisão sobre a pontuação do SCHUFA, envolvendo a classificação de crédito, sem levar em consideração que a proteção de segredos oficiais/industriais, não constitui um fim em si mesmo, mas exige igualmente uma coordenação com a proteção de pessoas e de interesses jurídicos diversos. A empresa alemã SCHUFA, ao prestar serviços de proteção ao crédito, no âmbito da avaliação de risco do consumidor, classificava como critério ne-gativo o pedido de acesso aos dados pelo próprio titular, ao interpretar que consumidores que acessavam mais o seu score tinham maior chance de serem inadimplentes.

Analisando tal decisão, Wolfgang Hoffmann Riem afirma que referida decisão não cumpriria com os requisitos do Capítulo III RGPD/GDPR. Pontua, todavia, que a divul-gação do design tecnológico e dos sistemas algorítmicos utilizados iria, por outro lado, interferir demasiado com a autonomia das empresas e afetar os seus legítimos interesses, permitindo o acesso dos algoritmos pelos concorrentes. Em seu entender, a quebra do segredo industrial seria justificada no caso de Direitos Fundamentais, em especial para evitar discriminação, estigmatização e manipulação. Ou no caso de existir outro interesse legítimo na divulgação equivalente à proteção de um segredo comercial. Se necessário, haveria proteção do segredo via procedimento sigiloso.

O direito à informação, previsto no art. 6º, VI da LGPD compreenderia o acesso e esclarecimento quanto aos aspectos principais e a lógica da decisão algorítmica – e, especi-almente os critérios de decisão -, de modo a ter, em princípio, a preservação do se-gredo de empresa, já que não seria necessário revelar o código fonte do algoritmo, mas os aspectos mais relevantes da decisão algorítmica, convertendo-se a linguagem matemática para a linguagem natural. Portanto, o segredo industrial não poderá ser interpretado e re-conhecido como sendo um direito absoluto, mesmo porque a própria Lei de Propriedade Industrial abre exceções ao segredo industrial/de negócios, no caso de ações judiciais, desde que respeitado o segredo de justiça, devendo ser analisado o caso concreto mediante o procedimento de ponderação e aplicação da proporcionalidade (art. 206, da LPI).

4.CONCLUSÃO

Diante da insegurança do processo judicial sob segredo de justiça no Brasil, já que não são raros os casos de publicação sem o respeito a tal limitação e de acesso por tercei-ros aos autos do processo, sem maiores dificuldades, há que se pensar em uma proposta diante da realidade cultural brasileira, bem diversa do contexto europeu neste sentido, sen-do uma alternativa viável a inversão do ônus da prova, proposta esta que parece estar de acordo com o procedimento da ponderação e aplicação da pro-porcionalidade, em especial a proporcionalidade em sentido estrito, a qual determina o respeito a um limite intranspo-nível para qualquer ponderação, qual seja, não afrontar o núcleo essencial de qualquer di-reito fundamental, isto é, a dignidade humana, inviabilizando por completo um dos Direi-tos Fundamentais em colisão.

Explica-se: ao invés de quebrar o segredo industrial, já que no Brasil não podemos garantir o segredo de justiça como suficiente para a preservação apenas entre as partes de tal revelação, poderia haver uma presunção de culpa caso a empresa se recusasse a infor-mar tais dados relativos ao segredo industrial/de negócio, invertendo--se o ônus da causa. Assim, ambos os Direitos Fundamentais estariam sendo protegidos mais adequadamente, sem o sacrifício total de qualquer deles (proporcionalidade em sentido estrito).

Deve ser reconhecido que a abordagem de regulação pelo risco ou risquificação, como uma possível mudança de emolduramento teórico, com destaque para os instrumen-tos de regulação "ex ante", licenças, certificações, análises de risco, processos de documen-tação,

boas práticas e "accountability", não poderá ser encarado como mero processo de ruptura normativa na proteção de dados pessoais, devendo ser interpretado de forma com-plementar aos modelos teóricos envolvidos na proteção dos Direitos Fundamentais. A proposta de risquificação vincula-se ao princípio da precaução, e ao reconhecimento de que danos nesta seara não se limitam ao aspecto individual, já que maioria dos casos, im-plicam em danos também coletivos e sociais, refletindo a multidimensionalidade dos Di-reitos Fundamentais.

Diversos autores na seara internacional contemporânea apontam para tal abordagem na área de proteção de dados e inteligência artificial, com destaque para Serge Gutwirth & Yves Poullet (2013), Raphael Gellert (2015), Alessandro Spina (2017) Claudia Quelle (2015) .

Gellert ao tratar da mudança de paradigma, com foco não mais no "informational privacy", para uma abordagem via "risk regulation" reconhece a aplicação nesta seara do teste de proporcionalidade no tocante à "finalidade legítima", exigindo uma análise con-textualizada acerca do tratamento de dados e suas especificidades.

É o que pontua Claudia Quelle , ao mencionar que as metodologias relacionadas à regulação do risco deverão ser influenciadas pela teoria do balanceamento de Direitos Fundamentais, analisando-se as violações diante dos casos concretos.

Isto fica claro quando temos a compreensão de que não basta a simples substitui-ção da normatividade estatal por uma outra, privada, e substituição de leis principiológicas pela regulação pela técnica já que há sempre o risco de que o controle pela tecnologia digi-tal possa ensejar a perda de regulamentação normativa ou causar fins normativamente indesejáveis.

Bibliografia

BEN-SHAHAR, Omri. Data Pollution, 2019: Volume 11, Journal of Legal Analysis, p. 133 e ss.

BERMAN, Paul Schiff. Cyberspace and the State Action Debate: the cultural value of ap-plying constitutional norms to "private" regulation. University of Colorado Law Review, v. 71, p. 1263- 1310. 2005.

BIONI, Bruno Ricardo, LUCIANO, Maria. O princípio da precaução na regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada?, https://brunobioni.com.br.

CANTARINI, Paola. Teoria fundamental do direito digital: uma análise filosófico-constitucional, Clube de autores, 2020.

_____, e GUERRA FILHO, Willis S. Teoria inclusiva dos direitos fundamentais e direito digital ,Clube de autores, 2020.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. International Review of Law, Computers and Technology, v. 33, n. 1, p. 76–99, 2019.

_____. Terms of service and bills of rights: new mechanisms of constitutionali-sation in the social media environment? International Review of Law, Computers and Technology, v. 33, n. 2, p. 122–138, 2019.

GELLERT, R. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law, 5, 3-20, 2015. GUTWIRTH, S., & POULLET, Y. Introduction. In S. Gutwirth, Y. Poullet, R. Leenes, & P. de Hert, European Data Protection: coming of age (pp. 1-10). Dordrecht: Springer, 2013. HILDEBRANDT, Mireille. Smart Regulation and the End(s) of Law, Publisher: Edward El-gar, 2015.

HOFFMANN-RIEM, Wolfgang. Big Data e Inteligência Artificial: Desafios Para O Di-reito. Journal of Institutional Studies 2 (2020), Revista Estudos Institucionais, v. 6, n. 2, p. 431-506, maio/ago. 2020

_____. Autorregulação, autorregulamentação e autorregulamentação regulada no con-texto digital, Revista da AJURIS – Porto Alegre, v. 46, n. 146, Junho, 2019

LESSIG, Lawrence. CODE version 2.0. New York: Basic Books, 2006.

_____. Reading The Constitution in Cyberspace. Emory Law Review, v. 45, p. 869–910, 1996

MARZOUKI, Meryem. A Decade of CoE Digital Constitutionalism Efforts: Human Rights and Principles Facing Privatized Regulation and Multistakeholder Governance. International Assotiation for Media and communication Research Conference (IAMCR), v. July, n. 1, 2019.

PADOVANI, Claudia; SANTANIELLO, Mauro. Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system. International Communication Gazette, v. 80, n. 4, p. 295–301, 2018.

QUELLE, C. Does the risk--based approach to data protection conflict with the protection of fundamental rights on a conceptual level?, Tilburg Law School Research Paper 1-36, 2015.

SPINA, A. A Regulatory Mariage de Figaro: risk regulation, data protection, and data ethics. European Journal of Risk Regulation, 8, 88-94, 2017.

SUZOR, Nicolas. The Role of the Rule of Law in Virtual Communities. Berkeley Technology Law Journal, v. 25, n. 4, p. 1817-1886. 2010.

TEUBNER, Gunther. Horizontal Effects of Constitutional Rights in the Internet: a legal case on the digital constitution. Italian Law Journal, v. 3, n. 2, p. 485–510. 2017.

NOTAS:

Professora Universitária, Pós doutora em Filosofia, Direito, Sociologia Jurídica (USP, EGS/SUiça, U. Coimbra, PUCSP- TIDD, Reggio Calabria, Doutora em Direito, Filosofia do Direito e em Filosofia, pesquisadora Cátedra Oscar Sala, Instituto Alan Turing, Advanced Institute of IA, pesquisadora C4AI - Centro de Inteligência Artificial, Presidente e Pesquisadora no EthicAI Grupo de Pesquisa em Inteligência Artificial, pesquisadora visitante European University Institute, Law Department (paolacantarini@gmail.com)

Professor da FD-PUCSP, UNIRIO - professor Doutor/titular, doutor em Direito, Filosofia, Comunicação e semiótica e em psicologia política. Pesquisador no EthicAI Grupo de Pesquisa em Inteligência

Artificial (willissantiago@pucsp.br)

CANTARINI, Paola. Teoria fundamental do direito digital: uma análise filosófico-constitucional, Clube de autores, 2020. e GUERRA FILHO, Willis S. Teoria inclusiva dos direitos fundamentais e direito digital ,Clube de autores, 2020.

PADOVANI, Claudia; SANTANIELLO, Mauro. "Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system". International Communication Gazette, v. 80, n. 4, p. 295–301, 2018. MARZOUKI, Meryem. A Decade of CoE "Digital Constitutionalism Efforts: Human Rights and Principles Facing Privatized Regulation and Multistakeholder Governance". International Assotiation for Media and communication Research Conference (IAMCR), v. July, n. 1, 2019.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. International Review of Law, Computers and Technology, v. 33, n. 1, p. 76–99, 2019. CELESTE, Edoardo. Terms of service and bills of rights: new mechanisms of constitutionalisation in the social media environment? International Review of Law, Computers and Technology, v. 33, n. 2, p. 122–138, 2019.

HOFFMANN-RIEM, Wolfgang, "Big Data e Inteligência Artificial: Desafios Para O Direito". JOURNAL OF INSTITUTIONAL STUDIES 2 (2020), Revista Estudos Institucionais, v. 6, n. 2, p. 431-506, maio/ago. 2020

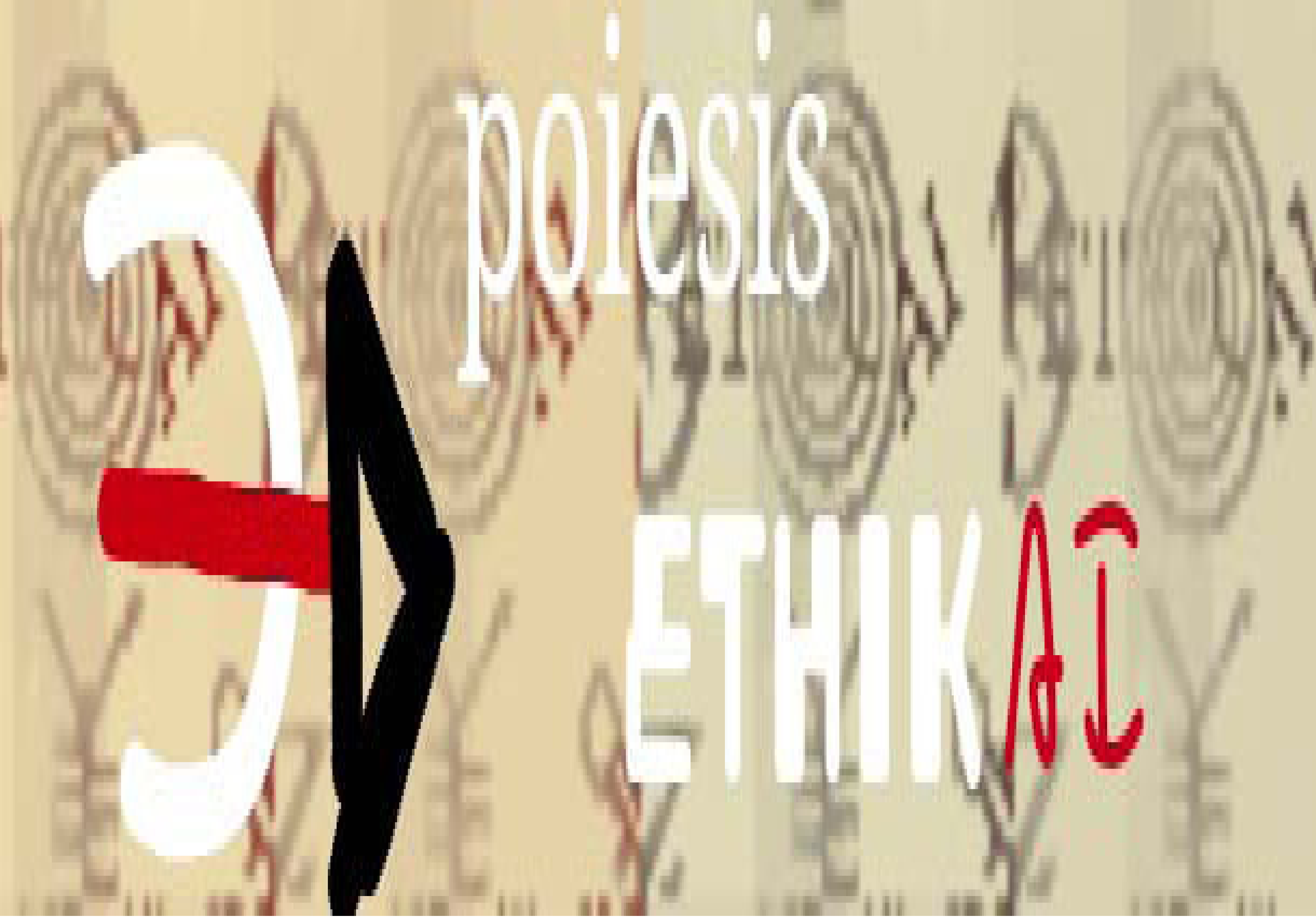
HOFFMANN-RIEM, Wolfgang, "Autorregulação, autorregulamentação e autorregulamentação regulada no contexto digital", Revista da AJURIS – Porto Alegre, v. 46, n. 146, Junho, 2019

GUTWIRTH, S., & POULLET, Y. Introduction. In S. Gutwirth, Y. Poullet, R. Leenes, & P. de Hert, European Data Protection: coming of age (pp. 1-10). Dordrecht: Springer, 2013. GELLERT, R. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law, 5, 3-20, 2015. QUELLE, C. "Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level?", Tilburg Law School Research Paper 1-36, 2015. SPINA, A. A Regulatory Mariage de Figaro: risk regulation, data protection, and data ethics. European Journal of Risk Regulation , 8, 88-94, 2017.

GELLERT, R. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law, 5, 3-20, 2015, p. 7 e ss.

QUELLE, C. "Does the risk--based approach to data protection conflict with the protection of fundamental rights on a conceptual level?", Tilburg Law School Research Paper 1-36, 2015.

poiesis



UMA BREVE HISTÓRIA DOS NEURODIREITOS: DA NEUROCIÊNCIA À INTELIGÊNCIA SUTIL E PERMANENTE DA INTELIGÊNCIA ARTIFICIAL

Edgar Gastón Jacobs Flores Filho. Advogado. Coordenador dos Projetos de Direito da SKEMA Brasil e Professor da PUCMINAS

Marina de Castro Firmo. Especialista em Políticas Públicas e Gestão Governamental. Bacharel em Direito pela PUCMINAS. Bacharel em Administração Pública pela Fundação João Pinheiro.

1 INTRODUÇÃO

A tecnologia está dentro do corpo das pessoas, o uso de um marca-passo gerenciado por computador é um exemplo disso. Por outro lado, detectores de mentira de certa forma invadem a mente das pessoas. Esses são apenas alguns exemplos de como a tecnologia pode agir, dentro ou fora do corpo das pessoas, para interagir com o que temos de mais íntimo ou secreto ou para expandir nossas limites biológicos.

O tema costuma ser abordado como "neurodireitos" e é um assunto que já vinha sendo abordado por estudiosos que relacionam o Direito e a Neurociência. Mas agora, o fluxo massivo de dados e o avanço da ciência, em especial, das neurotecnologias e da Inteligência Artificial (IA) tornou questões assim um tema que precisa ser pesquisado com mais aprofundamento pela comunidade jurídica e regulado por normas legais.

Neste artigo, os neurodireitos observados com uma perspectiva histórica e classificados. O objetivo será de descrever, de forma bastante resumida, a evolução dos estudos das classificações destes direitos, demonstrando, em concomitante, a sua crescente importância e valorização.

2 EVOLUÇÃO E CLASSIFICAÇÃO DOS NEURODIREITOS

Neurociência é uma ciência em alta na atualidade e, embora tenha surgido há 100 anos, se desenvolveu muito nas últimas duas décadas com a introdução de dispositivos de imagem cerebral em tempo real (GAZZANIGA, 2008).

A relação entre Direito e Neurociência também data daquele período, segundo SHEN (2016), o artigo "The Brain on the Stand" (ROSEN, 2007), publicado em 2007 no New York Times Magazine é um marco para a área hoje denominada Neurolaw, nos EUA. O artigo tratava da discussão sobre provas forenses baseadas na discussão sobre funcionamento adequado do cérebro, um tema relacionado à neurociência

O Direito Criminal, parece ser o primeiro e mais explorado ponto de contato da Neurociência com o Direito, tanto assim que, em 2009, Jan Christoph Bublitz e Reinhard Merkel, dois autores alemães da área penal apresentaram um paper no qual discutiam sobre melhoramentos e intervenções no cérebro em face do direito à autonomia e à autenticidade (BUBLITZ; MERKEL, 2009). Eles se preocuparam com intervenções diretas, como produtos farmacêuticos, e indiretas, como a hipnose e a publicidade subliminar. A partir disso questionaram a influência ilegítima de terceiros como um fator a ser considerado em julgamentos. Esta, provavelmente, foi a base para que os pesquisadores olhassem também para a pessoa que sofreu a influência e passassem a arguir qual seria o direito dela agredido pelas intervenções externas.

Outro artigo importante, de autoria de Nita A. Farahany, tratou dos avanços da neurociência nos Tribunais, discutindo a necessidade de uma nova taxonomia para o princípio da não autoincriminação (FARAHANY, 2012). A autora destaca que a proteção desse princípio normalmente se refere a proteção do que as pessoas falam e defendeu que: "uma sociedade interessada na liberdade cognitiva robusta provavelmente desejaria proteger seus cidadãos da detecção injustificada de provas automáticas, memorializadas e proferidas no cérebro". Nesse sentido, questionando o risco de o Poder Judiciário avaliar erroneamente o tema, sugeriu necessidade de uma norma, uma "Lei da Tecnologia da Informação em Neurociências" que protegesse a privacidade mental e a liberdade cognitiva. Este documento foi importante para dar nome aos direitos, e serve como um marco para o surgimento de um movimento a favor dos neurodireitos.

Em 2014, Bublitz e Merkel, inovaram ao debater novos assuntos e delinear um outro neurodireito: o direito humano à autodeterminação mental. Para os autores, a mente deveria ser protegida de uma lesão psíquica, tal como o direito de lesão corporal já protegia o corpo das pessoas (BUBLITZ; MERKEL, 2014).

Outro influente artigo sobre o tema foi publicado em 2017, por Marcello Ienca e Roberto Andorno, com o nome Towards new human

rights in the age of neuroscience and neurotechnology (IENCA; ADORNO, 2017). Neste estudo, foram descritas novas tecnologias e dispositivos neurais, e, em seguida, foram descritos alguns neurodireitos, que podem ser sistematizados da seguinte maneira: (i) liberdade cognitiva ou determinação mental, conforme já proposto por Bublitz e Merkel; (ii) direito à privacidade mental, que protegeria as ondas cerebrais não apenas como dados, mas também como geradores de dados ou fontes de informação, de forma consciente ou não; (iii) direito a integridade mental, no sentido da proteção contra a alteração não autorizada da computação neural de uma pessoa, resultando dano; e (iv) o direito à continuidade psicológica, que tente a preservar a identidade pessoal e a coerência do comportamento do indivíduo contra modificações não consentidas.

Os bens jurídicos protegidos por esses direitos são, principalmente a privacidade, livre escolha e integridade, diretamente relacionados à dignidade da pessoa humana. Esses bens são ameaçados, hoje, por uma desafiadora tecnologia, com grande potencial de transformação: a Inteligência Artificial.

Os direitos relativos aos efeitos neurocientificos da IA são hoje uma preocupação de Rafael Yuste e seu grupo de estudiosos na Universidade de Columbia. No artigo, denominado Four ethical priorities for neurotechnologies and AI, Yuste e seus mais de 20 coautores sugeriram as quatro prioridades que levaram ao desenvolvimento atual dos neurodireitos (YUSTE ET AL., 2017). Ressalta-se a indicação, no trabalho, das seguintes prioridades éticas: (a) privacidade e consentimento, (b) agência e identidade, (c) incrementos e (d) vieses.

Analisando a proposta de YUSTE é possível afirmar que a privacidade visa a proteção dos dados e informações produzidas pela atividade cerebral, os dados neurais. Esses dados são acessíveis por meio da neurotecnologia, inclusive por métodos não invasivos, como a análise dos padrões de digitação. Os neurodados reúnem informações úteis e valiosas que, sem a devida regulação, pavimentariam o solo para possíveis manipulações, voltadas a publicidade ou outros interesses.

Quanto a esse tema, os autores sugeriram, em primeiro lugar, que a capacidade de cancelar o compartilhamento, de impedi-lo, deve ser o padrão. O consentimento voluntário que contenha, de forma explícita, quem usará os dados, para quais fins e por quanto tempo deveria ser a regra aplicada . Propõem, ainda, o rígido controle sobre a comercialização dos dados. Justificam esse controle dizendo que mesmo um grupo limitado de doadores voluntários – ou eventualmente contratados para ceder os dados – poderiam gerar informações que, cruzadas com dados não neurais poderiam ajudar a traçar conclusões sobre terceiros.

A agência, que assume aqui o sentido de agir ou atuar, pode ser descrita como a capacidade influenciar intencionalmente o próprio funcionamento e as circunstâncias da vida (BRANDURA, 2006). Para além as antigas teorias de livre arbítrio, que desprezam componentes como a interação humana e a interação com o ambiente, a noção de agência revela o humano capaz de agir, mas constantemente influenciado pelo que o cerca.

Outra questão relacionada à segunda preocupação ética é a identidade, no sentido de que as interfaces cérebro-máquina podem corromper a visão que as pessoas têm de si. Neste caso, o bombardeamento seletivo feito por redes sociais é um exemplo, assim como o efeito que aplicativos de entrega de alimentos podem gerar quando baseados em dados e informações sobre o comportamento, os desejos e a intimidade das pessoas.

Essencial dar destaque, também, aos vieses provocados pelo processamento de big data por meio de sistemas de IA. Sobre essa matéria, Yuste e seus colaboradores abordam os riscos desses vieses influírem negativamente contra grupos historicamente minoritários e as distorções quanto a gênero e raça. Além disso, o estudo cita problemas gerados por algoritmos que processaram dados com a finalidade de contratar pessoas e, nesses casos, refletiram vieses, a saber, tendências contrárias a mulheres. Por fim, são mencionadas situação em que algoritmos que prejudicaram pessoas negras em casos envolvendo a justiça criminal.

Em suma, vê-se que, desde 2007, os neurodireitos foram se consolidando como um conjunto novo de Direitos Humanos que, hoje, são uma proposta já delineada em vias de ser implementada por alguns países.

3 CONSIDERAÇÕES FINAIS

O tema dos neurodireitos precisa ser abordado e essa necessidade foi detectada a quase duas décadas.

Os dispositivos, drogas e técnicas que melhoram a performance, que salvam vidas e até mesmo que regulam alimentação das pessoas já vinham sendo tratados do ponto de vista jurídico e ético, assim como a discussão sobre os limites da privacidade mental de uma testemunha ou de um réu.

Porém a IA, quando usada para influenciar decisões, pode se tornar um método não invasivo e de manipulação de mentes em grande escala, que pode colocar em risco a liberdade cognitiva e a privacidade mental de toda a sociedade.

Enfim, esse breve relato demonstra que há uma evolução dos estudos sobre neurodireitos na área jurídica e que, talvez, tenha chegado o momento dos mesmos ganharem espaço também nas Leis, Constituições e Tratados Internacionais.

R E F E R Ê N C I A S BIBLIOGRÁFICAS

BUBLITZ, Jan Christoph; MERKEL, Reinhard. Autonomy and authenticity of enhanced personality traits. Bioethics, v. 23, n. 6, p. 360-374, 2009.

BUBLITZ, Jan Christoph; MERKEL, Reinhard. Crimes against minds: on mental manipulations, harms and a human right to mental self-determination. Criminal Law and Philosophy, v. 8, n. 1, p. 51-77, 2014.

FARAHANY, Nita A. Incriminating thoughts. Stan. L. Rev., v. 64, p. 351, 2012.

GAZZANIGA, Michael S. "The law and neuroscience." Neuron 60, no. 3 (2008): 412-415.

I E N C A , M a r c e l l o ; ANDORNO, Roberto. Towards new human rights in the age of neuroscience and neurotechnology. Life sciences, society and policy, v. 13, n. 1, p. 1-27, 2017.

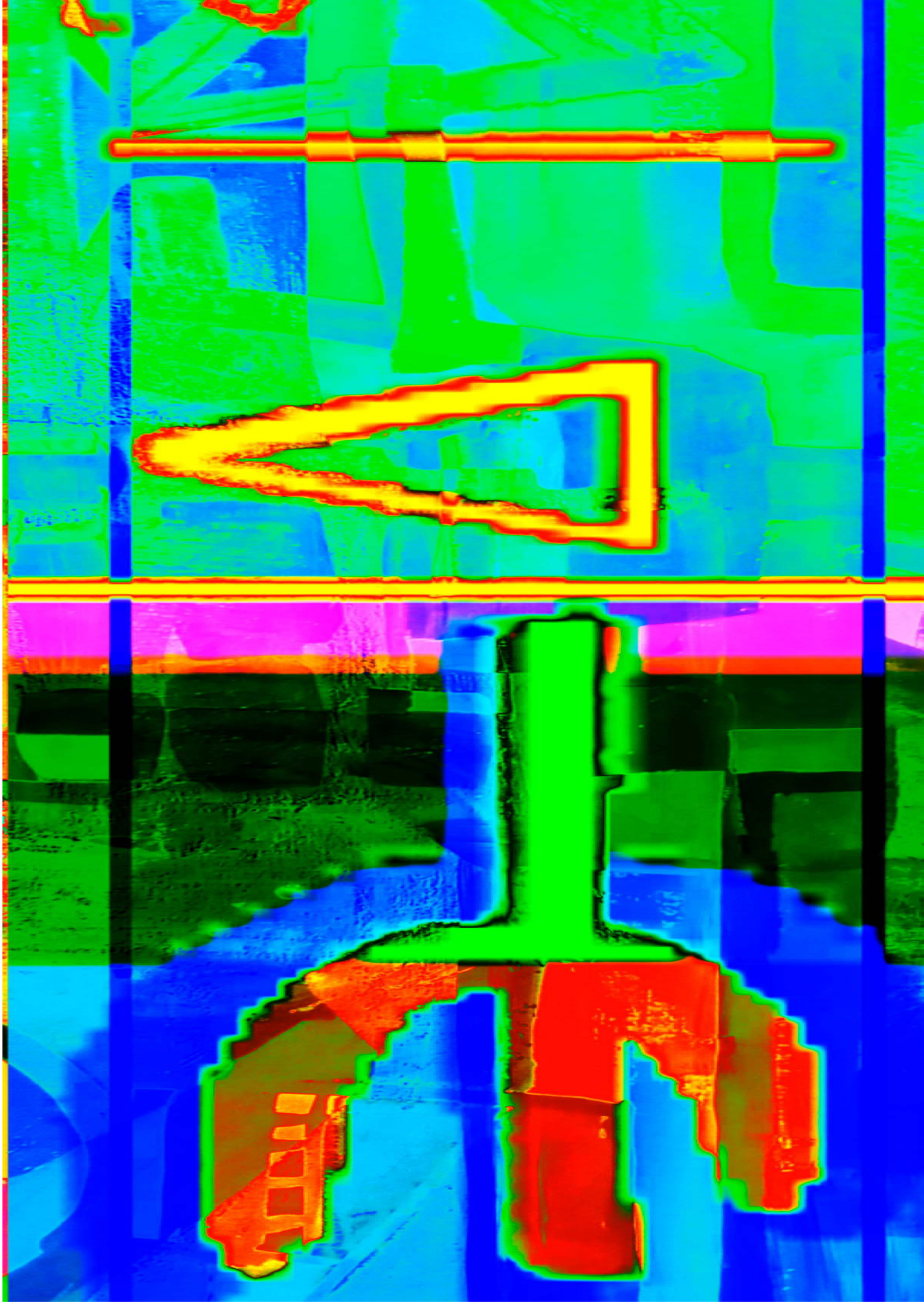
ROSEN, J., The Brain on the Stand, N.Y. TIMES MAGAZINE. (Mar. 11, 2007), http://www.nytimes.com/2007/03/11/magazine/11Neurolaw.t.html

SHEN, Francis X. Law and neuroscience 2.0. Ariz. St. LJ, v. 48, p. 1043, 2016.

YUSTE, Rafael; GOERING, Sara; et. al. Four ethical priorities for neurotechnologies and AI. Nature, Londres, 8 nov 2017., BANDURA, Albert. Toward a psychology of human agency. Perspectives on psychological science, v. 1, n. 2, p. 164-180, 2006.

NOTAS:

No Brasil há Projeto de Lei, o PL 1229/2021, que altera a Lei Geral de Proteção de Dados para incluir proteção quanto aos tratando da proteção de dados neurais e impondo a regra geral de consentimento relativamente a esses dados pessoais.



IETHICAI

ethicai.com.br

Poiesis

A PROTEÇÃO AOS DIREITOS HUMANOS COMO FUNDAMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018

JOSÉ LUIZ DE MOURA FALEIROS JÚNIOR

A proteção aos direitos humanos como fundamento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2

Resumo: Mais do que se aprofundar em detalhamentos técnicos, a Lei Geral de Proteção de Dados Pessoais brasileira (Lei nº 13.709/2018) traz ao ordenamento conjecturas de natureza principiológica, eis que é composta por fundamentos (art. 2º), conceitos (art. 5º) e princípios (art. 6º) que embasam os demais temas tratados de forma sistematizada em seu vasto repertório de regras. É sobre esse tema que esse brevíssimo ensaio se debruçará, tomando-o como premissa para o tema-problema que será explorado, qual seja: a aferição da equivalência dos elementos que compõem o rol de fundamentos da lei. Trabalhar-se-á com a hipótese de que o avanço informacional, catalisado pela propagação dos algoritmos, representa importante desafio para a efetivação da tutela pretendida com a lei, que não pode se desconectar da proteção aos direitos humanos. Será utilizado o método dedutivo, com aportes bibliográficos. Ao final, uma conclusão será apresentada.

Palavras-chave: human rights; personal data protection; General Law for the Protection of Personal Data.

The protection of human rights as a foundation of the General Law for the Protection of Personal Data (Law No. 13709/2018)

Abstract: More than delving into technical details, the Brazilian General Law for the Protection of Personal Data (Law No. 13.709/2018) brings to the Legal System conjectures of a principled nature, as it is composed of fundamentals (art. 2), concepts (art. 5) and principles (art. 6) that underlie the other themes dealt with in a systematic way in its vast repertoire of rules. It is on this theme that this very brief essay will focus, taking it as a premise for the theme-problem that will be explored, which is: the assessment of the equivalence of the elements that make up the list of fundamentals of the law. The essay works with the hypothesis that the informational advance, catalyzed by the spread of algorithms, represents an important challenge for the effectiveness of the protection intended by the law, which cannot be disconnected from the protection of human rights. The deductive method will be used, with bibliographic contributions. At the end, a conclusion will be presented.

Keywords: direitos humanos; proteção de dados pessoais; Lei Geral de Proteção de Dados Pessoais.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais brasileira – Lei nº 13.709, de 14 de agosto de 2018 – é importante marco normativo para a tutela jurídica dos dados pessoais no país. Sua promulgação atende a um comando normativo explicitado pelo legislador no artigo 3º, inciso III, do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), que definiu como um dos princípios regentes da disciplina de uso da Internet no Brasil exatamente a proteção dos dados pessoais.

Mais do que se aprofundar em detalhamentos técnicos, a nova lei traz ao ordenamento conjecturas de natureza principiológica, eis que é composta por fundamentos (art. 2º), conceitos (art. 5º) e princípios (art. 6º) que embasam os demais temas tratados de forma sistematizada em seu vasto repertório de regras.

Quanto aos fundamentos da lei, optou o legislador por uma categorização que está subdividida em sete incisos, todos contidos no artigo 2º da lei. O último deles define como fundamentos da proteção de dados pessoais no Brasil "os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais." É sobre esse tema que esse brevíssimo ensaio se debruçará, tomando-o como premissa para o tema-problema que será explorado, qual seja: a aferição da equivalência dos elementos que compõem o rol de fundamentos da lei.

De início, procurar-se-á estabelecer algumas premissas sobre o contexto jurídico no qual o legislador editou a nova lei e seus fundamentos. A partir dos desdobramentos colhidos da tutela jurídica da privacidade, novas nuances permitiram a contextualização de um direito fundamental à proteção dos dados pessoais – mote da ressignificação regulatória que se almeja para a Internet no país – e, com isso, regras próprias foram traçadas. Nessa linha, trabalhar-se-á com a hipótese de que o avanço informacional, catalisado pela propagação dos algoritmos, representa importante desafio para a efetivação da tutela pretendida com a lei, que não pode se desconectar da proteção aos direitos humanos. Será utilizado o método dedutivo, com aportes bibliográficos. Ao final, uma conclusão será apresentada.

2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SEUS FUNDAMENTOS: CONTORNOS INICIAIS PARA A PROTEÇÃO DOS DIREITOS HUMANOS

O conceito de privacidade, para a Ciência do Direito, tem suas origens no common law. O termo é usualmente resultado de traduções do substantivo inglês "privacy", que remonta ao clássico artigo "The right to privacy", escrito em 1890 por Samuel Warren e Louis Brandeis, em que, por primeiro, se analisa o direito de ser deixado só (right to be let alone) , com o qual a privacidade não se confunde. O primeiro direito se caracteriza pela inadmissão da disseminação não autorizada de informações pessoais, pela não violação do repouso individual dentro do lar e pela garantia de anonimato em ambientes públicos.

Por razões filológicas, há autores que optam por traduzir o termo "privacy" como "privatividade" , que vem de "privativo" e indica o imperativo de tutela contra a perturbação externa, que garante a proteção da intimidade no âmbito individual . Em simples termos, a "privatividade" seria um contraponto à exposição, tendo em vista que cada indivíduo está continuamente envolvido em um processo pessoal de busca pelo equilíbrio entre o anseio de preservar sua própria intimidade e o desejo de se expor e estabelecer comunicação com terceiros, à luz de condicionantes e normas sociais a que se sujeita .

Um dos fundamentos da Lei Geral de Proteção de Dados Pessoais brasileira (Lei nº 13.709/2018, ou simplesmente LGPD) é a autodeterminação informativa (art. 2º, II), que revela essa dimensão de controle capaz de viabilizar as condicionantes para o exercício do equilíbrio sugerido pela leitura do conceito de privatividade. A partir dela, quando se cogita de um direito fundamental à proteção de dados pessoais - , deve-se, invariavelmente, proceder a uma investigação sobre as dimensões do conceito de privacidade, na medida em que a formatação de uma possível nova infraestrutura social , a partir do implemento de técnicas direcionadas à coleta de dados e à formação de perfis para variados fins, representaria ruptura paradigmática capaz de atribuir novos contornos aos mencionados direitos fundamentais à intimidade e à privacidade.

Essa é uma das razões pelas quais o legislador teve o cuidado de conceituar o escopo de proteção desse direito específico a partir de uma conjugação dos demais (intimidade e privacidade) combinados com o direito fundamental à liberdade, na formação do que a lei conceitua como titularidade . Trata-se do fundamento essencial para a retomada do controle, pelo indivíduo, sobre as projeções de sua personalidade, que são lançadas à Internet na construção de novas estruturas passíveis de tutela jurídica.

De acordo com José Eduardo Faria, "(...) a revolução das técnicas de comunicação "diminuiu" o mundo, tornando-o mais independente. Dito de outro modo, tornou-o mais integrado do ponto de vista econômico, porém mais fragmentado do ponto de vista político" , o que se desdobra a partir da substituição da proximidade física dos indivíduos, de forma progressiva, pela interligação tecnológica calcada no incremento comunicacional e na ressignificação do valor da informação. Nesse aspecto, convém lembrar a posição de Bruno Bioni, que se reporta aos escritos de Helen Nissenbaum para propor a perspectiva de privacidade como integridade contextual, que pressupõe "analisar como se dá a dinâmica do tráfego informacional sob a perspectiva da relação que lhe dá origem (...) e, posteriormente, como terceiros podem nele ingressar" , haja vista a identificação de um valor social da proteção conferida aos dados pessoais.

O Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), em seu art. 7º, também "garante especificamente aos

usuários da rede a inviolabilidade da sua intimidade e vida privada e a inviolabilidade e o sigilo do fluxo de suas comunicações e de suas comunicações privadas armazenadas".

Sendo a informação a substância essencial da composição dessa nova morfologia da sociedade , os dados pessoais acabam por se tornar projeções da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável , motivo pelo qual o tratamento de tais dados adquire notável relevância , o que desafia a Teoria do Direito à compreensão e à indicação de soluções para os novos problemas suscitados na nova sociedade da informação .

Nesse passo, a doutrina busca trabalhar a proteção de dados como um direito fundamental que vai além da dicotomia conceitual entre o público e o privado , pois almeja à "promoção de um equilíbrio entre os valores em questão, desde as consequências da utilização da tecnologia para o processamento de dados pessoais, suas consequências para o livre desenvolvimento da personalidade, até a sua utilização pelo mercado" .

A informação ostenta características relevantes, até mesmo do ponto de vista existencial, sendo imperiosa a sua compreensão para além dos requisitos formais que a qualificam como bem jurídico tutelável. Isso porque, na Internet, o escopo informacional transcente a tutela jurídica da propriedade (daí a menção anterior ao conceito de titularidade, explicitado no artigo 17 da LGPD), podendo adquirir, também, contornos existenciais, que se imiscuem ao próprio sujeito, na medida em que "o objeto dos direitos de personalidade não se encontra nem na própria pessoa nem externamente" , mas, em verdade, tendo a personalidade um valor, "as situações existenciais não seriam exauridas na tradicional categoria dos direitos subjetivos".

Stefano Rodotà descreve a formação de um corpo eletrônico, um novo aspecto da pessoa natural que não ostenta apenas a massa física, ou um corpus, mas também uma dimensão digital. Com efeito, Javier Iniesta e Francisco Serna indicam a necessidade de uma regulação voltada ao meio digital exatamente para que seja possível situar as transformações oriundas do desenvolvimento tecnológico.

Esse é o ambiente no qual se inserem os direitos fundamentais à honra e à imagem, também considerados para os propósitos de se estabelecer proteção específica aos direitos humanos na lei. O primeiro é usualmente associado a componentes negativos, de oposição à sua realização, produção, reprodução e divulgação, enfim, ao conhecimento alheio. Por outro lado, também é associado a componentes positivos: de consentir com todas as práticas listadas. A imagem, nesse sentido, é um desdobramento da intimidade. E, exatamente no que concerne à almejada proteção do livre desenvolvimento da personalidade é que reside a proposta defendida, dentre outros, por Bruno Bioni: o enquadramento da proteção de dados como categoria autônoma dos direitos da personalidade, sendo visualizada como liberdade positiva, em contraposição ao direito à privacidade (e não se confundindo com os contornos próprios do direito à intimidade), visto como liberdade negativa . É a partir desse contexto que se cogita, por exemplo, de um direito à não perturbação do sossego na Internet .

Já o direito à honra pode ser analisado como decorrência do respeito que toda pessoa pode exigir para si mesma e perante outrem. Por essa razão, o referido direito apresenta uma faceta subjetiva, consubstanciada no apreço que o ser humano nutre por si mesmo, e uma outra, objetiva, que decorre do interesse que toda pessoa mantém pelo prestígio, reputação e bom nome , não se confundindo com a intimidade, uma vez que, "enquanto o ataque à honra ofende o conceito social, que o sujeito passivo pretende gozar, na agressão à intimidade não existe a finalidade danosa dirigida contra o conceito, mas sim contra o ambiente de privacidade que envolve a vítima" .

Na sociedade da informação, é possível afirmar que, sob o manto de proteção do direito à honra e do direito à intimidade, há aspectos de controle social a se considerar, pois o que se almeja é evitar os efeitos negativos da vigilância de dados (dataveillance) . O tema remete ao chamado "profiling", usualmente traduzido como perfilização, e a LGPD dedicou dispositivo bastante tímido ao tema, inserido em um único parágrafo do artigo que cuida da anonimização de dados (artigo 12, §2º): "Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada." A finalidade da vigilância não pode estar voltada a incursões no espaço mais íntimo do indivíduo e a LGPD descreve a importância de se conferir efetividade às técnicas de anonimização de dados.

Serge Gutwirth e Mireille Hildebrandt defendem a necessidade de que a criação de perfis pressuponha um sistema de proteção contra o processamento de dados que afetam comportamentos (como as restrições de circulação), mesmo que esses dados não possam ser considerados dados pessoais (caso dos dados anonimizados, pela exegese do artigo 12, caput, da LGPD brasileira).

Sem um instrumento vigoroso como a LGPD para que se possa esperar legitimamente um 'uso ético' dos algoritmos , grande nebulosidade continuará a pairar sobre os processos utilizados para o monitoramento social e as bases fundamentais para a definição de tão importante marco protetivo – com destaque para os direitos fundamentais à privacidade, à liberdade e à intimidade – permanecerão no vazio em razão da própria dificuldade de se desvendar abusos e excessos praticados nos processos de coleta e tratamento de dados, ainda que anonimizados.

Esse é o contexto no qual se editou a lei, com vários fundamentos, dentre os quais merece leitura destacada a proteção aos direitos humanos.

3 A PROTEÇÃO AOS DIREITOS HUMANOS COMO FUNDAMENTO EXPRESSO DA LEI

O artigo 2º, inciso VII, da LGPD é categórico a elencar, logo em seu primeiro trecho, a proteção aos direitos humanos como fundamento da lei. Naturalmente, para que não haja regresso, especialmente quanto à proteção jurídica que se deve conferir a tais direitos ,

caminhos devem ser mapeados para conciliar inovação e regulação. Sem dúvidas, o pluralismo jurídico global deve atuar como vetor da função promocional dos direitos humanos , abrindo espaços à tutela subjacente-valorativa da pessoa, mesmo em um ambiente permeado pela disrupção tecnológica.

Sendo o direito um sistema aberto e de segunda grandeza , uma vez que composto de verdadeira rede hierarquizada de princípios e regras que orbitam a Constituição , é insofismável a importância do tema para fixar algumas premissas essenciais do problema sob investigação, pois o atingimento desse desiderato, na esteira do que defende Gustavo Zagrebelsky, somente ocorrerá se determinadas condicionantes estruturais se fizerem presentes, das quais a "ductibilidade" (maleabilidade) dos ordenamentos jurídicos constitucionais é a mais relevante, pois propicia o pacifismo e a integração democrática "através da rede de valores e procedimentos comunicativos que é, ademais, a única visão possível e não catastrófica da política em nosso tempo."

Nesse contexto, segundo Jorge Pereira da Silva:

O desiderato a se atingir é o de que o poder de intervenção estatal e a liberdade dos cidadãos se equilibrem de modo a garantir ao indivíduo tanta protecção quanto a necessária, mas também tanta liberdade pessoal quanto seja possível. Por isso, segundo a denominada concepção pessoal do bem jurídico, tem-se entendido que integram este conceito aquelas "realidades ou fins que são necessários para uma vida social livre e segura, que garantam os direitos humanos e fundamentais do indivíduo, assim como para o funcionamento do sistema estatal erigido para a consecução de tal objectivo. Não que, com esta referência, se pretenda induzir à importação acrítica para o direito constitucional dos resultados (nem sempre pacíficos) atingidos pela doutrina penalista sobre a teoria do bem jurídico – até porque a protecção penal é apenas uma modalidade, entre várias outras, de protecção de direitos fundamentais –, mas é importante reconhecer que a multifuncionalidade dos direitos fundamentais implica uma atenção redobrada ao conceito de bem jusfundamental e a sua colocação no centro do processo construtivo dos conglomerados jurídicos usualmente designados por direitos fundamentais.

Embora não se possa deixar de considerar os impactos que as peculiaridades culturais acarretam para qualquer coletividade, a ponto de ser precipitada uma análise conjectural baseada na ideia de sociedade, do ponto de vista dos direitos humanos, posições identitárias e individuais impõem a ponderação , notadamente para que sejam fixadas firmemente as bases do entrelaçamento entre o público e o privado.

A autodeterminação informativa é vista como pré-condição natural do indivíduo para o exercício de um rol quadrangular de direitos considerados 'básicos'. São os chamados "ARCO rights", sigla para os termos em inglês access, rectification, cancellation e opposition. A ideia que os justifica é a de que, sem que se saiba o mínimo, é impossível buscar a concretização de qualquer direito , e os mais elementares – acesso, retificação, cancelamento e oposição – indicariam quatro dimensões conjugáveis para o exercício do que Orla Lynskey chama de "bloco fundante" (foundational block) sobre o qual se assentam todas as demais construções normativas sobre direitos do titular de dados baseados na acepção de controle, que, paulatinamente, passa a ser compreendida como "processo" (due process).

Em um universo no qual a predição algorítmica está presente de forma tão marcante, nichos de aglutinação de poder desenvolvem ambientes menos seguros à proteção dos direitos humanos. Nesse sentido, Shoshana Zuboff fala na instrumentação e instrumentalização do comportamento para fins de modificação, previsão, monetização e controle ao propor o termo "instrumentarismo" ("instrumentarianism") , que simboliza o epítome do que a própria autora designa como capitalismo de vigilância.

O poder instrumentário, em seus dizeres, realiza a expropriação da experiência humana como um imperativo econômico, processando decisivamente a redistribuição dos direitos humanos elementares dos indivíduos para o capital.

Para frear esse indesejado paradigma é preciso, naturalmente, reconfigurar estruturas protetivas condizentes com o novo momento do desenvolvimento técnico-informacional. Os direitos humanos devem inspirar marcos regulatórios, propostas legislativas e, essencialmente, todo o acervo normativo que se pretenda instituir.

No Brasil, o que guiou a promulgação da Lei Geral de Proteção de Dados Pessoais foi justamente esse "núcleo duro" de parâmetros extraídos de uma compreensão mais ampla do direito à privacidade, previstos no texto legal como fundamentos, em seu artigo 2º, e que atuam como vetores axiológicos para os direitos (e deveres) descritos noutras passagens da lei e, também, para a atuação posterior do Estado, no exercício de seu poder regulatório.

A definição de categorias merecedoras de maior proteção, como a dos dados pessoais adjetivados como "sensíveis" (art. 5º, II, da LGPD) é evidência sólida dessa preocupação do legislador.

Outra evidência disso é estruturação de revisões das decisões automatizadas (art. 20, da LGPD), que devem ser realizadas por agentes humanos. Se a proteção insuficiente não pode ser admitida, sob pena de flagrante violação ao citado fundamento da lei, deve-se estruturar mecanismos de controle que atuem como freios aos desideratos que afastem os humanos de sua essência.

Que fique claro: o recrudescimento valorativo dos direitos humanos não implica considerar um resgate antropocêntrico, egoístico ou que coloque o homem (individualmente considerado) novamente no centro do sistema jurídico – como foi no Estado Liberal –, ou seja, não é o homem econômico (homo economicus) a figura que se pretende ver inserida no vértice constitucional, ainda que este também seja merecedor de proteção pontual, a nível fundamental.

Almeja-se, sim, a maior proteção ao "homem existencial", concebido a partir da proteção de experiências individuais que tenham uma projeção útil para o próprio titular e para a coletividade. É nesse contexto que se colhe o maior valor

da delimitação de fundamentos normativos nos dispositivos introdutórios da norma. Postulados instituídos com tal cariz atuam para além da lei especificamente considerada e inspiram o ordenamento como um todo.

4 CONSIDERAÇÕES FINAIS

A definição de parâmetros protetivos a direitos que refletem os desafios desvelados pela inovação indica os principais motivos para que se defina fundamentos normativos. Na LGPD, o rol de sete incisos do artigo 2º indica uma preocupação do legislador com o estabelecimento de metaparâmetros, para além das regras, cujas definições – mais abstratas – permitem ao operador colmatar lacunas e zonas cinzentas ainda não totalmente tuteladas e claramente compreendidas no contexto dos demais dispositivos da norma.

Questões como a vigilância de dados, a ruptura das estruturas de controle e a imposição de limitações a direitos individuais projetados na web a partir do tratamento de dados se tornam desafiadoras em razão do ritmo acelerado da inovação. Definir os direitos humanos como um dos fundamentos da lei revela uma preocupação quanto a esses fenômenos e traz à lume preocupações que vão além dos tecnicismos da LGPD.

É imprescindível que o operador atento se mantenha consciente de que a LGPD não é uma legislação definitiva. A própria morfologia social muda em ritmo acelerado e, sem dúvidas, novas tecnologias (ou novos usos para tecnologias já conhecidas) trarão novos desafios, que precisarão ser interpretados e tutelados, mesmo na ausência de regramentos mais específicos. Para isso, alçar os direitos humanos a tal patamar contribui de forma decisiva! É esse o propósito essencial dessa delimitação, que confirma a hipótese explorada nesse brevíssimo ensaio.

Referências

AMARANTE, Aparecida. Responsabilidade civil por dano à honra. 6. ed. Belo Horizonte: Del Rey, 2005.

ASCENSÃO, José de Oliveira. A dignidade da pessoa e o fundamento dos direitos humanos. Revista da Faculdade de Direito da Universidade de São Paulo, São Paulo, v. 103, p. 277-299, jan./dez. 2008.

ÁVILA, Humberto. Teoria dos princípios: da definição à aplicação dos princípios jurídicos. 5. ed. São Paulo: Malheiros, 2005.

AZEVEDO, Antonio Junqueira de. O direito como sistema complexo e de 2ª ordem; sua autonomia. Ato nulo e ato ilícito. Diferença de espírito entre responsabilidade civil e penal. Necessidade de prejuízo para haver direito de indenização na responsabilidade civil. Civilistica.com, Rio de Janeiro, ano 2, n. 3, jul./set. 2013.

BASAN, Arthur Pinheiro; JACOB, Muriel Amaral. Habeas Mente: a responsabilidade civil como garantia fundamental contra o assédio de consumo em tempos de pandemia. Revista IBERC, Belo Horizonte, v. 3, n. 2, p. 161-189, maio/ago. 2020.

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

BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

CLARKE, Roger A. Information technology and dataveillance. Communications of the ACM, Nova York, v. 31, n. 5, p. 498-512, maio 1988.

COMPARATO, Fábio Konder. A afirmação histórica dos direitos humanos. 7. ed. São Paulo: Saraiva, 2010.

COSTA JÚNIOR, Paulo José da. O direito de estar só: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.). Direito digital: direito privado e Internet. 3. ed. Indaiatuba: Foco, 2020.

DOTTI, René Ariel. Proteção da vida privada e liberdade de informação: possibilidades e limites. São Paulo: Revista dos Tribunais, 1980.

DUFF, Alistair S. Information society studies. Londres: Routledge, 2000.

FARIA, José Eduardo. Informação e democracia na economia globalizada. In: SILVA JÚNIOR, Ronaldo Lemos; WAISBERG, Ivo (Org.). Comércio eletrônico. São Paulo: Revista dos Tribunais, 2001.

FERNANDES, Milton. Proteção civil da intimidade. São Paulo: Saraiva, 1977.

GONZÁLEZ FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. Cham: Springer, 2014.

GUTWIRTH, Serge; HILDEBRANDT, Mireille. Some caveats on profiling. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul (Eds.). Data protection in a profiled world. Cham: Springer, 2010.

HERRERA FLORES, Joaquín. Teoria crítica dos direitos humanos: os direitos humanos como produtos culturais. Tradução de Luciana Caplan. Rio de Janeiro: Lumen Juris, 2009.

HILDEBRANDT, Mireille. The public(s) onlife. In: FLORIDI, Luciano (Ed.). The onlife manifesto: being human in a hyperconnected era. Cham/Londres: Springer

OpenAccess, 2015.

HUNT, Lynn. A invenção dos direitos humanos: uma história. Tradução de Rosaura Eichenberg. São Paulo: Cia. das Letras, 2009.

INIESTA, Javier Belda; SERNA, Francisco José Aranda. El paradigma de la identidad: hacia una regulación del mundo digital. Revista Forense, Rio de Janeiro, v. 422, jul./dez, p. 181-202, 2015.

JOELSONS, Marcela. Autodeterminação informativa em direito comparado: análise dos contextos históricos e decisões paradigmas das cortes constitucionais alemã e brasileira. Revista de Direito Constitucional e Internacional, São Paulo, v. 199, p. 233-272, maio/jun. 2020.

LYNSKEY, Orla. The foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. A anonimização de dados pessoais: consequências jurídicas do processo de reversão, a importância da entropia e sua tutela à luz da Lei Geral de Proteção de Dados. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). Direito & Internet IV: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura; BASAN, Arthur Pinheiro. A responsabilidade civil pela perturbação do sossego na Internet. Revista de Direito do Consumidor, São Paulo, v. 128, p. 239-265, mar./abr. 2020.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. Pensar: Revista de Ciências Jurídicas, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (Coord.). Lei Geral de Proteção de Dados: aspectos relevantes. Indaiatuba: Foco, 2021.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: mapping the debate. Big Data & Society, Londres: Sage, Original Research Article, p. 1-21, jul./dez. 2016. Disponível em: https://doi.org/10.1177/2053951716679679. Acesso em: 15 out. 2021.

MOYN, Samuel. Not enough: human rights in an unequal world. Cambridge: Harvard University Press, 2018.

NISSENBAUM, Helen. Privacy in context: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

PÉREZ LUÑO, Antonio Enrique. Los derechos fundamentales. Temas clave de la Constitución Española. 10. ed. Madrid: Tecnos, 2011.

PÉREZ LUÑO, Antonio-Enrique. Manual de informática e derecho. Barcelona: Ariel, 1996.

RECASÉNS SICHES, Luis. Filosofia del derecho. México: Porrúa, 2008.

RODOTÀ, Stefano. Intervista su privacy e libertà. Roma/Bari: Laterza, 2005.

RODRIGUEZ, Daniel Piñeiro. O direito fundamental à proteção de dados: vigilância, privacidade e regulação. Rio de Janeiro: Lumen Juris, 2021.

ROSENVALD, Nelson. A LGPD e a despersonalização da personalidade. Migalhas de Proteção de Dados, 20 ago. 2021. Disponível em: https://s.migalhas.com.br/S/F546F9 Acesso em: 15 out. 2021.

ROUVROY, Antoinette; POULLET, Yves. The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cécile; NOUWT, Sjaak (Ed.). Reinventing data protection? Cham: Springer, 2009.

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2010.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel. DONEDA, Danilo. SARLET, Ingo Wolfgang. RODRIGUES JR, Otavio Luiz (Coords.); BIONI, Bruno Ricardo (Org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal Brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. Direitos Fundamentais & Justiça, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020.

SILVA, Jorge Pereira da. Deveres do Estado de protecção de direitos fundamentais: fundamentação e estrutura das relações jusfundamentais triangulares. 3. ed. Lisboa: Universidade Católica Editora, 2015.

STAPLES, William G. Encyclopedia of privacy. Westport: Greenwood Press, 2007.

SZANIAWSKI, Elimar. Direitos de personalidade e sua tutela. 2. ed. São Paulo: Revista dos Tribunais, 2005.

VAN DIJK, Jan. The network society. 3. ed. Londres: Sage Publications, 2012.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harvard Law Review,

Cambridge, v. 4, n. 5, p. 193-220, dez. 1890. https://www.jstor.org/stable/1321160. Acesso em: 15 out. 2021.

WESTIN, Alan. Privacy and freedom. Nova York: IG Publishing, 2015.

WESTIN, Alan; BAKER, Michael. Databanks in a free society. Nova York: Quadrangle Books, 1972.

ZAGREBELSKY, Gustavo. El derecho dúctil. Ley, derechos y justicia. Tradução do italiano para o espanhol de Marina Gascón. Madri: Trotta, 1995.

ZAMPIER, Bruno. Bens digitais. Indaiatuba: Foco, 2017.

ZUBOFF, Shoshana. "We make them dance": surveillance capitalism, the rise of instrumentarian power, and the threat to human rights. In: JØRGENSEN, Rikke Frank (Ed.). Human rights in the age of platforms. Cambridge: The MIT Press, 2019.

NOTAS:

Doutorando em Direito Civil pela Universidade de São Paulo – USP/Largo de São Francisco. Doutorando em Direito, na área de estudo 'Direito, Tecnologia e Inovação', pela Universidade Federal de Minas Gerais – UFMG. Mestre e Bacharel em Direito pela Universidade Federal de Uberlândia – UFU. Membro do Instituto Avançado de Proteção de Dados – IAPD e do Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC. Advogado. E-mail: jfaleiros@usp.br ORCID: https://orcid.org/0000-0002-0192-2336

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harvard Law Review, Cambridge, v. 4, n. 5, p. 193-220, dez. 1890. https://www.jstor.org/stable/1321160. Acesso em: 15 out. 2021.

COSTA JÚNIOR, Paulo José da. O direito de estar só: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995. p. 25.

FERNANDES, Milton. Proteção civil da intimidade. São Paulo: Saraiva, 1977. p. 90.

WESTIN, Alan. Privacy and freedom. Nova York: IG Publishing, 2015. p. 7.

Excelente exploração histórica do conceito de autodeterminação informativa pode ser colhida de rica pesquisa realizada por Laura Schertel Mendes. Como afirma a autora, "Ainda que a concepção da esfera privada tenha importante papel na jurisprudência constitucional, as críticas à relatividade da esfera privada e ao contexto do uso dos dados evidenciaram seus déficits no contexto da sociedade da informação e ensejaram uma evolução desse conceito". MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. Pensar: Revista de Ciências Jurídicas, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. p. 15. Também é importante lembrar da distinção da autodeterminação informativa em relação à proteção de dados pessoais, embora sejam dois direitos fundamentais amplamente reconhecidos. Como lembra Ingo Sarlet, "O que se pode afirmar, sem temor de incorrer em erro, é que seja na literatura jurídica, seja na legislação e jurisprudência, o direito à proteção de dados vai além da tutela da privacidade, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade." SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal Brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. Direitos Fundamentais & Justiça, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020. p. 191. Em arremate, recomenda-se a leitura de: MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (Coord.). Lei Geral de Proteção de Dados: aspectos relevantes. Indaiatuba: Foco, 2021. p. 13-22; JOELSONS, Marcela. Autodeterminação informativa em direito comparado: análise dos contextos históricos e decisões paradigmas das cortes constitucionais alemã e brasileira. Revista de Direito Constitucional e Internacional, São Paulo, v. 199, p. 233-272, maio/jun. 2020. Recomenda-se, ainda, a leitura integral de RODRIGUEZ, Daniel Piñeiro. O direito fundamental à proteção de dados: vigilância, privacidade e regulação. Rio de Janeiro: Lumen Juris, 2021.

Sintetizando o contexto no qual tal direito emergiu na União Europeia, conferir GONZÁLEZ FUSTER, Gloria. The emergence of personal data protection as a fundamental right of the EU. Cham: Springer, 2014. p. 48.

O tema é de tamanha relevância que, embora a doutrina já sinalize a consagração da proteção de dados pessoais como direito fundamental, tramita perante o Congresso Nacional a Proposta de Emenda à Constituição 17/2019, que visa inclui-la entre os direitos e garantias fundamentais do cidadão. A PEC ainda define como de competência exclusiva da União o poder para legislar sobre o assunto. No plano doutrinário, há tempos já se destaca a existência e a força normativa desse direito fundamental implícito. Sobre o tema, conferir, por todos, DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.). Direito digital: direito privado e Internet. 3. ed. Indaiatuba: Foco, 2020, p. 34. SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel. DONEDA, Danilo. SARLET, Ingo Wolfgang. RODRIGUES JR, Otavio Luiz (Coords.); BIONI, Bruno Ricardo (Org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 21-59. Ademais, no contexto jurisprudencial, em maio de 2020, o Supremo Tribunal Federal reconheceu o direito fundamental à proteção de dados ao suspender a Medida Provisória n.º 954, que determinava o compartilhamento dos dados pessoais dos usuários de telefonia pelas empresas telefônicas ao IBGE (STF, ADIs n.º 6.387, 6.388, 6.389, 6.390 e 6.393. Relatora Min. Rosa Weber. Julgado em 07/05/2020).

VAN DIJK, Jan. The network society. 3. ed. Londres: Sage Publications, 2012. p. 6.

Nesse contexto, são eloquentes os registros de William Staples quanto à violação que isso causa ao direito fundamental à privacidade:

"Key issues in the debate over the authority to violate personal privacy concern racial or ethnic profiling, wiretapping, monitoring of personal communications via cellular telephones, access to personal records that show the reading habits of private citizens, monitoring of electronic mail and other Internet use, monitoring of personal movement via the Global Positioning System (GPS), and the use of radio frequency identification (RFID) chips to track the movement of pets, personal goods, and items shipped, among others." STAPLES, William G. Encyclopedia of privacy. Westport: Greenwood Press, 2007. p. 93.

É o que prevê o artigo 17 da LGPD: "Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei." Sobre o dispositivo, valiosa a leitura das reflexões de ROSENVALD, Nelson. A LGPD e a despersonalização da personalidade. Migalhas de Proteção de Dados, 20 ago. 2021. Disponível em: https://s.migalhas.com.br/S/F546F9 Acesso em: 15 out. 2021.

FARIA, José Eduardo. Informação e democracia na economia globalizada. In: SILVA JÚNIOR, Ronaldo Lemos; WAISBERG, Ivo (Org.). Comércio eletrônico. São Paulo: Revista dos Tribunais, 2001. p. 20.

Destaca a autora: "We have a right to privacy, but it is neither a right to control personal information nor a right to have access to this information restricted. Instead, it is a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones. This is the right I have called contextual integrity, achieved through the harmonious balance of social rules, or norms, with both local and general values, ends, and purposes. This is never a static harmony, however, because over time, conditions change and contexts and norms evolve along with them." NISSENBAUM, Helen. Privacy in context: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010. p. 231.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 213.

DUFF, Alistair S. Information society studies. Londres: Routledge, 2000. p. 86.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.). Direito digital: direito privado e Internet. 3. ed. Indaiatuba: Foco, 2020. p. 33 et seq.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 169. E, nesse contexto, a autora sustenta que: "(...) a vitalidade e a continuidade da Constituição dependem da sua capacidade de se adaptar às novas transformações sociais e históricas, possibilitando uma proteção dos cidadãos contra novas formas de poder que surgem na sociedade".

PÉREZ LUÑO, Antonio-Enrique. Manual de informática e derecho. Barcelona: Ariel, 1996. p. 10 et seq.

HILDEBRANDT, Mireille. The public(s) onlife. In: FLORIDI, Luciano (Ed.). The onlife manifesto: being human in a hyperconnected era. Cham/Londres: Springer OpenAccess, 2015. p. 181 et seq.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 407.

SZANIAWSKI, Elimar. Direitos de personalidade e sua tutela. 2. ed. São Paulo: Revista dos Tribunais, 2005. p. 87.

ZAMPIER, Bruno. Bens digitais. Indaiatuba: Foco, 2017, p. 55.

RODOTÀ, Stefano. Intervista su privacy e libertà. Roma/Bari: Laterza, 2005. p. 121-122. Comenta: "La necessità di una tutela forte del corpo fisico, dunque, fa parte della tradizione giuridica e civile dell'Occidente. Però non c'è ancora altrettanta sensibilità per il «corpo elettronico» che pure rappresenta oggi la nostra identità. (...) Possiamo in effetti parlare di una rivincita del corpo fisico, di un suo ritorno alla ribalta proprio nel momento in cui sembrava soppiantato dal corpo virtuale, «elettronico». L'incontro tra corpo fisico e tecnologie d'avanguardia è stato alla base di questa nuova attenzione proprio nel momento in cui l'esperienza mostrava i limiti dell'identificazione elettronica."

INIESTA, Javier Belda; SERNA, Francisco José Aranda. El paradigma de la identidad: hacia una regulación del mundo digital. Revista Forense, Rio de Janeiro, v. 422, jul./dez, p. 181-202, 2015. p. 184. Com efeito: "Pero, realmente, ¿en qué lugar podemos situar lo virtual? Con la aparición de Internet se da un cambio fundamental, la comunicación fluye de todos a todos. Hasta ahora, se ha visto esta realidad como un cambio cuantitativo, más que cualitativo, en las relaciones interpersonales, que habla de la disponibilidad ininterrumpida del otro y de formas de acercamiento afectivo, que hasta ahora requerían inexorablemente la co-presencia física de los actores. Evidentemente, esta variación de parámetros ha provocado un desenfoque de la visión que se tenía hasta el momento, dando lugar al surgimiento de conflictos de complejo enfoque jurídico. Así, Internet se nos presenta como un espacio abierto que permite interactuar en diversos contextos tomando distintas identidades, estas identidades – denominadas virtuales – se alejan de la noción de identidad basada en los presupuestos culturales de la persona que hasta ahora eran el paradigma de nuestra visión del ser humano".

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 92-93.

Confira-se: MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura; BASAN, Arthur Pinheiro. A responsabilidade civil pela perturbação do sossego na Internet. Revista de Direito do Consumidor, São Paulo, v. 128, p. 239-265, mar./abr. 2020; BASAN, Arthur Pinheiro; JACOB, Muriel Amaral. Habeas Mente: a responsabilidade civil como garantia fundamental contra o assédio de consumo em tempos de pandemia. Revista IBERC, Belo Horizonte, v. 3, n. 2, p. 161-189, maio/ago. 2020.

AMARANTE, Aparecida.

Responsabilidade civil por dano à honra. 6. ed. Belo Horizonte: Del Rey, 2005, p. 37.

DOTTI, René Ariel. Proteção da vida privada e liberdade de informação: possibilidades e limites. São Paulo: Revista dos Tribunais, 1980. p. 87.

Trata-se de um acrônimo para "data surveillance" (vigilância de dados), a indicar uma nova espécie ou técnica de vigilância em razão do surgimento de novos métodos de monitoramento, como a vigilância de dados pessoais e a vigilância de dados em massa, que exigem salvaguardas mais eficazes e uma estrutura política formal. Sobre o tema, confira-se CLARKE, Roger A. Information technology and dataveillance. Communications of the ACM, Nova York, v. 31, n. 5, p. 498-512, maio 1988.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. A anonimização de dados pessoais: consequências jurídicas do processo de reversão, a importância da entropia e sua tutela à luz da Lei Geral de Proteção de Dados. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). Direito & Internet IV: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019. p. 74.

GUTWIRTH, Serge; HILDEBRANDT, Mireille. Some caveats on profiling. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul (Eds.). Data protection in a profiled world. Cham: Springer, 2010. p. 37.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: mapping the debate. Big Data & Society, Londres: Sage, Original Research Article, p. 1-21, jul./dez. 2016. Disponível em: https://doi.org/10.1177/2053951716679679. Acesso em: 15 out. 2021.

José de Oliveira Ascensão aduz que os direitos do homem (direitos humanos, em sentido amplo), quando positivados em documentos internacionais de proteção e promoção da pessoa humana são considerados direitos humanos; quando positivados nas Cartas Constitucionais são considerados direitos fundamentais; e quando positivados na legislação civil são direitos de personalidade. ASCENSÃO, José de Oliveira. A dignidade da pessoa e o fundamento dos direitos humanos. Revista da Faculdade de Direito da Universidade de São Paulo, São Paulo, v. 103, p. 277-299, jan./dez., 2008. p. 278.

Conferir, por todos, SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2010. p. 79; HUNT, Lynn. A invenção dos direitos humanos: uma história. Tradução de Rosaura Eichenberg. São Paulo: Cia. das Letras, 2009. p. 113-145; COMPARATO, Fábio Konder. A afirmação histórica dos direitos humanos. 7. ed. São Paulo: Saraiva, 2010. p. 91-92; RECASÉNS SICHES, Luis. Filosofia del derecho. México: Porrúa, 2008. p. 1-19.

PÉREZ LUÑO, Antonio Enrique. Los derechos fundamentales. Temas clave de la Constitución Española. 10. ed. Madrid: Tecnos, 2011. p. 151.

AZEVEDO, Antonio Junqueira de. O direito como sistema complexo e de 2ª ordem; sua autonomia. Ato nulo e ato ilícito. Diferença de espírito entre responsabilidade civil e penal. Necessidade de prejuízo para haver direito de indenização na responsabilidade civil. Civilistica.com, Rio de Janeiro, ano 2, n. 3, jul./set. 2013.

ÁVILA, Humberto. Teoria dos princípios: da definição à aplicação dos princípios jurídicos. 5. ed. São Paulo: Malheiros, 2005. p. 167.

ZAGREBELSKY, Gustavo. El derecho dúctil. Ley, derechos y justicia. Tradução do italiano para o espanhol de Marina Gascón. Madri: Trotta, 1995. p. 15, tradução livre. No original: "a través de la red de valores y procedimientos comunicativos que es además la única visión no catastrófica de la política posible en nuestro tiempo."

SILVA, Jorge Pereira da. Deveres do Estado de protecção de direitos fundamentais: fundamentação e estrutura das relações jusfundamentais triangulares. 3. ed. Lisboa: Universidade Católica Editora, 2015. p. 354.

HERRERA FLORES, Joaquín. Teoria crítica dos direitos humanos: os direitos humanos como produtos culturais. Tradução de Luciana Caplan. Rio de Janeiro: Lumen Juris, 2009. p. 97-98.

ROUVROY, Antoinette; POULLET, Yves. The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cécile; NOUWT, Sjaak (Ed.). Reinventing data protection? Cham: Springer, 2009, p. 45-76.

LYNSKEY, Orla. The foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015, especialmente o capítulo 6.

O tema é desenvolvido, na Europa, por Westin e Baker (Cf. WESTIN, Alan; BAKER, Michael. Databanks in a free society. Nova York: Quadrangle Books, 1972, p. 356-370), mas importantes estudos têm sido publicados, no Brasil, a partir das pesquisas de autores como Bruno Bioni, em especial quanto ao consentimento (BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz; BIONI, Bruno Ricardo (Coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.)

ZUBOFF, Shoshana. "We make them dance": surveillance capitalism, the rise of instrumentarian power, and the threat to human rights. In: JØRGENSEN, Rikke Frank (Ed.). Human rights in the age of platforms. Cambridge: The MIT Press, 2019. p. 28. Segundo a autora: "As to the new species of power, I have suggested that it is best understood as instrumentarianism, defined as the instrumentation and instrumentalization of behavior for the purposes of modification, prediction, monetization and control. In this formulation, "instrumentation" refers to the ubiquitous, sensate, computational, actuating global architecture that renders, monitors, computes, and modifies human behavior. Surveillance capitalism is the puppet master that imposes its will through the vast capabilities of this connected puppet to produce

instrumentarian power, replacing the engineering of souls with the engineering of behavior."

MOYN, Samuel. Not enough: human rights in an unequal world. Cambridge: Harvard University Press, 2018. p. 220. O autor assevera: "Human rights will return to their defensible importance only as soon as humanity saves itself from its low ambitions. If it does, for the sake of local and global welfare, sufficiency and equality can again become powerful companions, both in our moral lives and in our political enterprises."

ethicAI.com.br

ETHICAI

poiesis

DÚVIDA & ÉTICA
NOTA SOBRE O PRINCÍPIO "IN DUBIO PRO REO"

PAULO FERREIRA DA CUNHA

Os princípios jurídicos têm recortes que se diriam ontológicos (a sua essência, o seu ser próprio, que os individualiza e distingue) e lógicos (não podendo incluir contradição nos seus termos ou na sua aplicação), assim como teleológicos (não podem ser contrariadas as suas finalidades, ínsitas na sua essência), e deontológicos (nem podem ser usados contra o seu sentido e papel, a sua teleologia não pode ser contrariada por uma praxis que perverta ou sinuosamente contorne a sua razão de ser e intencionalidade). Mas, de entre todos, nos princípios há recortes (que também se poderiam dizer "limites") éticos.

Não seria possível um princípio jurídico contrário àquele mínimo ético mais ou menos consensual na nossa sociedade pluralista, que nos faz concordar em larga medida com uma percentagem enormíssima dos princípios consagrados pela lei, pela doutrina e pela jurisprudência. Sabemos que há minudências e bizantinismos complexos e por vezes inteligentes e subtis sobre a fragmentação ética e comportamental contemporânea. Mas será que estaria alguém realmente disposto a prescindir dos principais crimes do Código Penal?

O princípio in dubio pro reo (doravante, simplesmente dito "princípio" algumas vezes) não foge aos referidos requisitos de fundo. E não foge também a uma regra de eticidade. Evidentemente que a razão que o determina é obviamente de alto valor ético: porque poderá ser condenado alguém se houve realmente dúvidas no espírito do julgador? Se o próprio julgador tem dúvidas, será eticamente correto (antes de se colocar a questão jurídica) condenar alguém? Claro que, residualmente decerto, alguns preferem o princípio contrário, mas que é o inverso também da ética: «Tuez-les tous! Dieu reconnaitra les siens». Foi, diz-se, a justificação (antiética) do massacre dos Albigenses de Béziers. Nestas matérias nunca se conseguirá uma completa unanimidade, mas não serão dissentimentos contrários à razoabilidade, à proporcionalidade, à equidade, à justiça, que poderão fazer recuar esse relativo consenso em que se vive, apesar de tudo, e que a ordem jurídica (sempre permeável à evolução, e portanto ao aperfeiçoamento) consagra.

Voltemos ao princípio. Não raro, em sede de discussão sobre a aplicabilidade, em concreto, do princípio in dubio pro reo alguns sobressaltos ocorrem, e ele parece ser invocado não somente a propos e como muitas vezes sans propos.

Parece, assim, ser de sublinhar, atentas as derivas de utilização (invocação) do princípio, que, por vezes, não é o Tribunal recorrido que tem quaisquer dúvidas (e isso é que releva para a aplicação do princípio). Será, nesses casos, alguém por ele, ou ninguém, mas podem agitar-se dúvidas até simplesmente hipotéticas.

Obviamente, não se crê que os recorrentes, verdadeiramente, em caso nenhum as tenham, porque esses saberão bem o que terá ocorrido – salvo casos excecionais de ação sob o domínio da hipnose ou afim. Não é esse o problema. O que ocorre é que o recorrente por vezes coloca em crise os factos dados como provados, invocando o princípio. Como uma espécie de versão outra do princípio da presunção da inocência, o que é coisa diversa. Enquanto este salienta a necessidade de se tratar como inocente quem não foi condenado com sentença transitada em julgado, aquele, de que tratamos agora, cura de real e efetiva dúvida que se haja (houvesse) instalado no espírito do julgador. Não se tratando, assim, de uma presunção sistemática de dúvida, porque, na verdade, tal não ocorre. Tal não é o que a experiência comum demonstra. É curioso – diga-se entre parêntesis – como uma certa mitologia representa ficcionalmente o juiz indeciso na véspera de dar a sentença, decidindo-se conforme pie a coruja ou cante a condenação uma qualquer ave agoirenta. Não parece ser o comum.

Não se trata de presumir inocência por se dar como assente ter anteriormente havido dúvida, ainda que esta última presunção seja apenas um pano de fundo tácito subentendido e não confessado como ponto fixo de Arquimedes em que se estribe o erróneo pensamento.

Vejamos o que ocorre por vezes. De algum modo, verifica-se que o recorrente coloca múltiplos obstáculos (fácticos, conjeturais, de toda a ordem) às certezas, mas estas não deixaram de se firmar (de se encontrar já estabelecidas). Ora, para a aplicação do princípio, é necessário que a dúvida seja do julgador, daquele julgador em concreto que está (estava) a apreciar o caso sub judice. Não se trata de dúvidas abstratas ou tidas ou induzidas pelo recorrente, que no espírito julgador não tenham tido acolhimento.

Há um choque de realidades, ou, se preferirmos, realidades paralelas. O recorrente afirma, por vezes com grande certeza e ênfase, a existência de violação do princípio. Mas, ao mesmo tempo, analisados os autos, não se vislumbram elementos substanciais que fundamentem a existência de qualquer dúvida da parte do julgador. Note-se que princípio em causa não se confunde com qualquer complexidade ou nebulosidade da lide. Elas podem existir sem que ele acabe por emergir, desde que o olhar do julgador haja conseguido deslindar os meandros, e alcançado ver claro de forma a não ter dúvidas.

Atente-se no Sumário do Ac. STJ de 21/10/2020, Proc. nº 1551/19.9T9PRT.P1.S1 (Relator: Conselheiro Manuel Augusto de Matos):

"XIV - Inexistindo dúvida razoável na formulação do juízo factual que conduziu à condenação do arguido, fica afastado o princípio do in dubio pro reo e da presunção de inocência, sendo que tal juízo factual não teve por fundamento uma imposição de inversão da prova, ou ónus da prova a cargo do arguido, mas resultou do exame e discussão livre das provas produzidas e examinadas em audiência, como impõe o artigo 355º nº 1 do CPP, subordinadas ao princípio do contraditório, conforme art°32°n° 1 da Constituição da República". (sublinhado nosso).

2.Tomando mais algum recuo teórico, para enquadramento da questão: é verdade que o princípio in dubio pro reo suscita, por vezes, algumas confusões, as quais, contudo, de modo algum deveriam existir, porquanto se encontra perfeitamente balizado jurisprudencialmente.

Por exemplo, veja-se o Acórdão deste STJ de 12/03/2009 proferido no Proc.º n.º 07P1769 (Relator: Conselheiro Soreto de Barros)

"II - O «in dubio pro reo é um princípio geral do processo penal, pelo que a sua violação conforma uma autêntica questão-de-direito que cabe, como tal, na cognição do STJ. Nem contra isto está o facto de dever ser considerado como princípio de prova: mesmo que assente na lógica e na experiência (e por isso mesmo), conforma ele um daqueles princípios que (…) devem ter a sua revisibilidade assegurada, mesmo perante o entendimento mais estrito e ultrapassado do que seja uma «questão-de-direito» para efeito do recurso de revista» – Figueiredo Dias, Direito Processual Penal, 1.ª ed. (1974), Reimpressão, Coimbra Editora, 2004, págs. 217-218; cf., ainda, Cristina Líbano Monteiro, In Dubio Pro Reo, Coimbra, 1997, e Pinto de Albuquerque, Comentário do Código de Processo Penal, Universidade Católica Editora, 2007, pág. 437.

III- O princípio do in dubio pro reo constitui uma imposição dirigida ao julgador no sentido de se pronunciar de forma favorável ao arguido, quando não tiver certeza sobre os factos decisivos para a decisão da causa; como tal, é um princípio que tem a ver com a questão de facto, não tendo aplicação no caso de alguma dúvida assaltar o espírito do juiz acerca da matéria de direito.

IV- Este princípio tem implicações exclusivamente quanto à apreciação da matéria de facto, quer seja nos pressupostos do preenchimento do tipo de crime, quer seja nos factos demonstrativos da existência de uma causa de exclusão da ilicitude ou da culpa.

V- Não existindo um ónus de prova que recaia sobre os intervenientes processuais e devendo o tribunal investigar autonomamente a verdade, deverá este não desfavorecer o arguido sempre que não logre a prova do facto; isto porque o princípio in dubio pro reo, uma das vertentes que o princípio constitucional da presunção de inocência (art. 32.º, n.º 2, 1.ª parte, da CRP) contempla, impõe uma orientação vinculativa dirigida ao juiz no caso da persistência de uma dúvida sobre os factos: em tal situação, o tribunal tem de decidir pro reo.

VI- Daqui se retira que a sua preterição exige que o julgador tenha ficado na dúvida sobre factos relevantes e, nesse estado de dúvida, tenha decidido contra o arguido. Já o saber se, perante a prova produzida, o tribunal deveria ter ficado em estado de dúvida é uma questão de facto que não cabe num recurso restrito à matéria de direito, mesmo que de revista alargada.

VII - A apreciação pelo STJ da eventual violação do princípio in dubio pro reo encontra-se dependente de critério idêntico ao que se aplica ao conhecimento dos vícios da matéria de facto: há-de ser pela mera análise da decisão que se deve concluir pela violação deste princípio, ou seja, quando, seguindo o processo decisório evidenciado através da motivação da convicção, se chegar à conclusão de que o tribunal, tendo ficado num estado de dúvida, decidiu contra o arguido, ou quando a conclusão retirada pelo tribunal em matéria de prova se materialize numa decisão contra o arguido que não seja suportada de forma suficiente, de modo a não deixar dúvidas irremovíveis quanto ao seu sentido, pela prova em que assenta a convicção."

O facto de se dever dar prevalência ao valor da liberdade e à presunção da inocência sobre a possibilidade da culpabilidade, em nada colide com a construção do princípio, assente na existência de verdadeira dúvida, dúvida que efetivamente tenha ocorrido.

Porém, não se trata de uma dúvida de um observador ideal, híper cético, porventura, nem dúvida sugerida ou acalentada meramente pela defesa, mas, depois de tudo somado, de tudo devidamente apreciado, estará em causa, para a aplicação do princípio, uma dúvida subsistente no julgador. É dessa dúvida que se trata. O tribunal teria tido que se encontrar na situação de algum impasse decisório, por eventualmente pender, algo pendularmente, entre possibilidades. E é no sentido de desfazer essa dúvida que se deve decidir em favor do réu. Ora, quando não se vislumbrar nos autos nada que indicie que essa dúvida existiu torna-se impossível, por falta dos requisitos essenciais do princípio, fazer uso dele.

O princípio, em termos absolutos, entre nós, acaba, assim, por ter um conteúdo algo mais preciso que a "proof beyond reasonable doubt", a qual, contudo, pode lançar alguma luz sobre as dúvidas dos tribunais. Mas que terão, elas próprias, de existir. Assim, no fundo, a própria dúvida de um tribunal, não poderá ser fruto de uma consciência tecnicamente dita "escrupulosa" (cf., v.g., Rafael Gomez Perez, Deontología Jurídica, 4.ª ed., Pamplona, EUNSA, 1999), não se tratando de estar acima de toda e qualquer dúvida, ou da mais leve dúvida. Se assim ocorresse, se se tratasse de uma total inexistência da mais ténue sombra de dúvida, decerto quase não haveria condenações; antes terá que ser uma dúvida de acordo com o padrão geralmente aceite pelo conhecimento e experiência das pessoas (segundo Neil van Dokkum, Evidence, Dublin, Thomson Round Hall, 2007, p. 9).

Porém, insista-se: no caso deste princípio, não se trata de dúvidas que pudessem pairar no espírito geral, ainda que com as características apontadas por van Dokkum, mas de dúvidas, desse mesmo tipo, mas concretamente existentes nos julgadores, e que se tenham traduzido em expressa documentação nos autos. Pois não se pode sondar o ânimo íntimo da mente dos juízes sem a existência de qualquer materialização da mesma, ainda que em obter dicta. Está obviamente em causa a consciência dos juízes, de cada juiz, e tal é matéria sensível, e não pode deixar de ser qualificada como ética. O juiz, se dúvidas teve, e sabendo da existência do princípio, tem o dever de externalizar explicitamente o que se passou consigo. Tanto mais que tem o dever de decidir e não pode refugiar-se no non liquet, nas nossas ordens jurídicas.

O Supremo Tribunal de Justiça em Portugal, por exemplo, só pode apreciar uma eventual violação do princípio do in dubio pro reo se da própria decisão recorrida resultar que, no caso, um Tribunal da Relação (no caso de não se estar perante recurso per saltum) teve

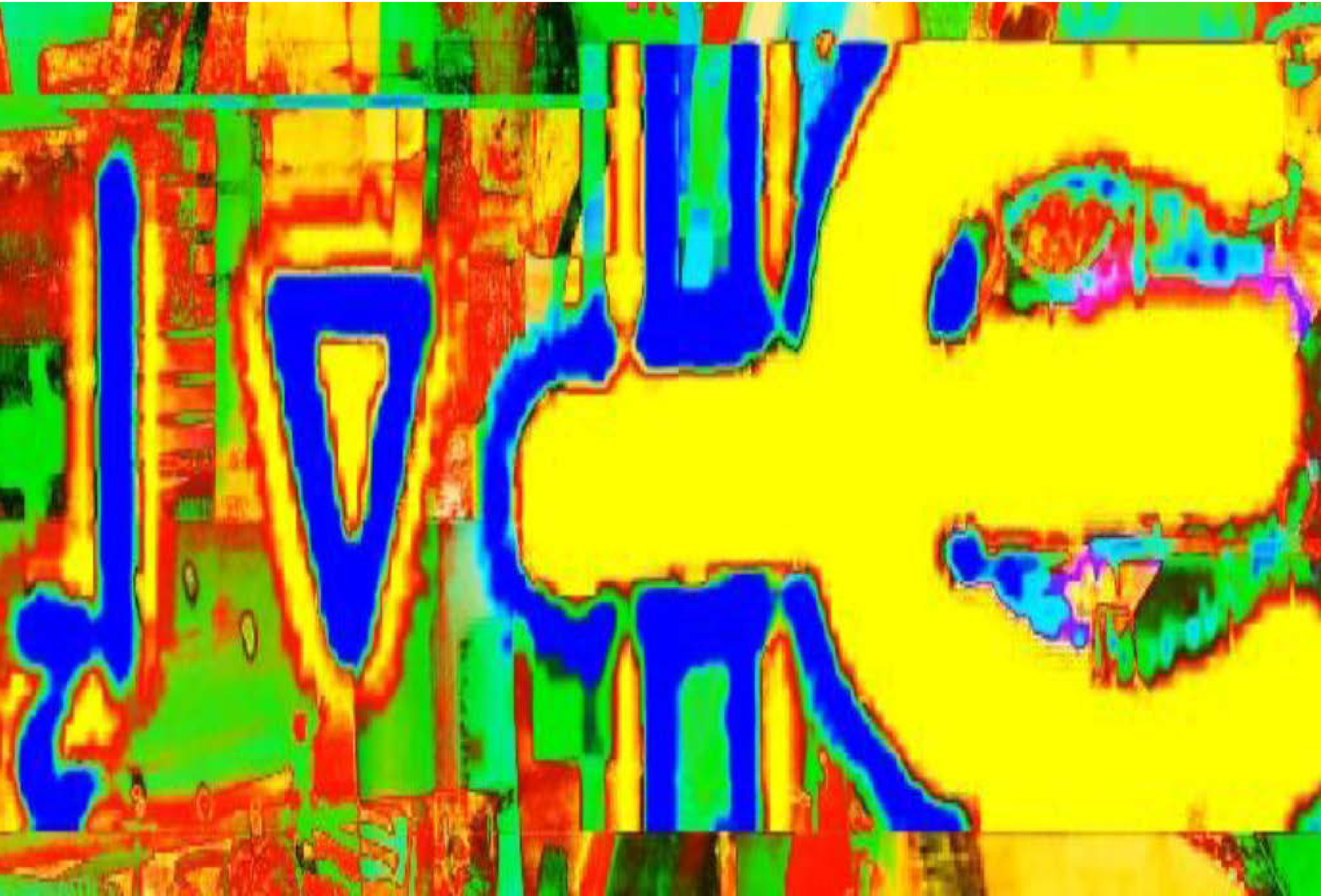
dúvidas sobre a veracidade dos factos imputados ao arguido e, não se detendo nesse obstáculo, nem, por via dele, fazendo uso do princípio em causa, ainda assim lhe atribuísse, por exemplo, a sua autoria desses factos fundantes da incriminação (cf. Acórdão do STJ de 09/07/2020, proferido no Proc.º n.º 2275 /15. 1JAPRT.P2. S1 (Relator: Conselheiro Francisco Caetano).

Importa ainda que tenha havido uma sentença contra o recorrente cujas provas não sejam irrefutáveis (materialmente arrasadoras), e que, portanto, se firmem em dúvida do tipo subjetivo – cfr. o Ac. STJ de 17/09/2020, in Proc. n.º 658/17.1PZLSB.L1.S1 (Relator: Conselheiro Clemente Lima). Porquanto, como bem se compreende, se (por absurdo) um tribunal que bem julgasse, ainda que com dúvidas (erróneas) sobre elementos objetivíssimos de que não haveria (não deveria ter havido) plausível dúvida possível, não teria percorrido no seu juízo um iter impecável, mas a sua dúvida não seria legítima.

É de ter em atenção que, nesta análise dos requisitos de aplicação do princípio em apreço, é de dúvida legítima, plausível, e efetiva que se trata. Caso contrário, seria pouco ético atender a um erro de avaliação, a uma irresolução condenável, a uma irrealista convocação de nuvens cinzentas sobre a limpidez do pensamento, no caso de um julgador até exarar em sentença que duvidou. Terá duvidado, sim (não nos será legítimo duvidar nesse caso hipotético), mas afigura-se-nos que, pela consistência ética do princípio, se não haveria, pelas regras da experiência comum, razões para que duvidasse, não deveria ter duvidado. Pelo menos, exige-se uma análise crítica da aplicação do princípio. Do mesmo modo que não basta invocá-lo para que se ponha em marcha, também não bastará que se encontre provada uma qualquer dúvida, de qualquer índole, mesmo fútil, mesmo absurda, para que intervenha.

Não se trata de limitar a utilização do princípio, mas apenas de a balizar de acordo com o seu sentido, a sua ratio, que é de índole irrecusavelmente ética, e por isso não pode compadecer-se com usos simplesmente formais. Em contrapartida, pode ocorrer que o julgador se encontre numa situação de pudor em revelar a sua dúvida. E apenas de forma imperfeita, indiciária, mas clara a olhos objetivos e indagadores, deixe registada a sua dúvida. Esse caso merece apreciação. Entre uma confessada dúvida sem pertinência, resultante apenas de um erro de observação ou de cálculo, ou ainda de uma atitude laxista ou escrupulosa muito subjetiva do julgador, e uma dúvida claramente expressa, mas de forma insinuada, sobre questões que, no caso, pertinentemente podem concitar dúvida, cremos que este último caso é mais suscetível de apreciação do que o primeiro. Embora, evidentemente, ambas as questões tenham que passar pelo crivo da interpretação – para se aquilatar realmente do que se passou, antes de mais.

Paulo Ferreira da Cunha
Juiz Conselheiro do Supremo Tribunal de Justiça (Portugal)
Professor Catedrático da Faculdade de Direito da
Universidade do Porto (funções suspensas para exercício da magistratura)



LGPD E A INCLUSÃO DA PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

LUCAS CARINI
FAUSTO SANTOS DE MORAIS

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais - LGPD, desde o seu projeto até a sua promulgação conturbada e parcial em meio a pandemia da corona vírus, intensificou as discussões sobre a temática no Brasil. A complexidade da nova legislação aliada a transversalidade massiva da sua aplicação na sociedade, atingindo de formas diferentes as pessoas físicas no sentido de titulares de dados e as pessoas jurídicas, empresas e entes públicos na posição de quem trata e faz o uso desses dados, trouxe à tona a discussão sobre a necessidade de inclusão da proteção de dados como direito fundamental, positivado no artigo 5º da Constituição Federal Brasileira.

Diante desse cenário que vem a baila o problema abordado no presente artigo: há necessidade de inclusão da proteção de dados pessoais em meios digitais como direito fundamental frente às legislações vigentes no Brasil que tratam desse direito? Considerando o objeto de pesquisa proposto, canaliza-se a elucidação do problema através da seguinte hipótese: a inclusão como direito fundamental dará maior efetividade para a proteção de dados pessoais. Para tanto objetiva-se com a presente pesquisa: I – mapear as legislações vigentes no Brasil que tratam sobre a proteção de dados; II - analisar os principais pontos da Proposta de Emenda à Constituição n° 17 de 2019, que acrescenta o inciso XII-A ao art. 5º, e o inciso XXX ao art. 22 da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria; III – verificar a necessidade de inclusão da proteção de dados como um direito fundamental.

A metodologia utilizada para a presente pesquisa é o dialético e o monográfico, e a técnica de pesquisa bibliográfica.

2 MAPA DA LEGISLAÇÃO BRASILEIRA SOBRE PROTEÇÃO DE DADOS PESSOAIS

Para uma compreensão mais acurada sobre a proteção de dados pessoais no Brasil, é preciso olhar o cenário com uma perspectiva mais ampla. Assim como no dito popular, as vezes se faz necessário parar e dar alguns passos para trás, não no sentido de regressar, mas para expandir o campo de visão, com uma postura lato sensu sobre a legislação brasileira vigente que é aplicada sobre a proteção de dados pessoais.

Assim, desenvolveu-se uma busca das legislações que tratam da proteção dos dados pessoais no Brasil. O objetivo é apresentar brevemente a legislação vigente no país que aborda a proteção de dados pessoais, seja de forma direita ou indireta, para demonstrar que não existe somente uma lei geral de proteção de dados acerca do tema.

Existem outras leis que antes mesmo da LGPD já tratavam desse direito no Brasil e que, ao contrário da visão negacionista conflitante, podem oferecer importantes subsídios para a jurisprudência e para a própria aplicação da proteção dos dados pessoais no país.

Para iniciar podemos citar a Lei 12.965/2014 conhecida como Marco Civil da Internet – MCI, que tem mais de dez menções à proteção de dados pessoais, com destaque para a seção II, a partir do artigo 10 que trata da proteção aos registros, aos dados pessoais e às comunicações privadas . Ainda, cabe destacar o Decreto 8.771/16 que regulamentou aspectos do MCI, instituindo no seu artigo 13, por exemplo, padrões de segurança e sigilo dos registros, que devem ser observados pelos provedores de conexão, com diretrizes sobre padrões de segurança .

Em matéria de relações de consumo é possível mencionar a Lei 8.078/90 que institui o Código de Defesa do Consumidor – CDC, que a partir do artigo 43 aborda a questão dos bancos de dados e cadastros de consumidores, concedendo o direito de acesso às informações existentes em cadastros, fichas, registros e dados pessoais. Após o CDC sobreveio a Portaria nº 5, de 27 de agosto de 2002, que passou a considerar abusiva, nos contratos de fornecimento de produtos e serviços, a cláusula que autorize o envio do nome do consumidor, e/ou seus garantes, à bancos de dados e cadastros de consumidores, sem comprovada notificação prévia.

Ainda em matéria consumerista, a Lei 12.414/2011 que disciplinou o chamado cadastro positivo, que trata sobre a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Com destaque para o direito de o titular dos dados ser informado previamente sobre o armazenamento e o objetivo do tratamento dos dados pessoais, bem como poder solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados, além de ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados , determinações que convergem, com as previsões da própria LGPD.

Em uma norma mais recente, se comparada a data de promulgação do CDC, o Decreto 7.962/2013 dispôs sobre a contratação no comércio eletrônico, e trouxe no seu artigo 4º, inciso VII, a obrigação de o fornecedor utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor .

Na área da saúde, ainda vinculado de certo modo com os direitos do consumidor, é possível referenciar três principais resoluções. A primeira, Resolução nº 2.145/2016 do Conselho Federal de Medicina que trata do Código de Processo Ético-Profissional. Introduzindo as normas técnicas referentes à digitalização, uso, manuseio e guarda dos documentos dos prontuários dos pacientes,contém todos os dados pessoais destes. Sobressai-se entre os considerandos da resolução o destaque para a ressalva de que os dados constantes nos prontuários pertencem ao paciente e só podem ser divulgados com sua autorização ou a de seu responsável, ou por dever legal ou justa causa.

A segunda é proveniente da Agência Nacional de Vigilância Sanitária – ANVISA através da sua Diretoria Colegiada publicou a Resolução – RDC nºº 44, de 17 de agosto de 2009, que dispõe sobre boas práticas farmacêuticas e disciplina nos artigos 59e 82 sobre a proteção de dados pessoais, assegurando a confidencialidade, privacidade e sigilo . Outra agência

governamental, como terceiro destaque tem a ANS - Agência Nacional de Saúde Suplementar, também através da sua diretoria colegiada editou a Resolução Normativa - RN Nº- 341, de 27 de Novembro de 2013, a qual aborda a questão do tratamento de dados e institui um padrão obrigatório para troca de informações na saúde suplementar.

Além da área cível, consumerista e saúde, o setor financeiro introduz diversas normas, decretos, instruções e resoluções que estabelecem regras e procedimentos a serem seguidos quanto ao tratamento de dados pessoais. Nesse aspecto, chama atenção o Decreto nº 4.489 de 28 de novembro de 2002, que impacta diretamente nos dados pessoais, pois regula o acesso aos dados sobre transferências, referindo-se à quebra do sigilo bancário, podendo serem tais dados repassados para Secretaria da Receita Federal do Ministério da Fazenda. O decreto ainda prevê a identificação dos usuários dos serviços, de maneira com que os titulares dos dados, conseguem através do número de inscrição no Cadastro de Pessoas Físicas (CPF) (artigo 2º, §3º) , indicar violação da proteção de dados pessoais, conflitando principalmente com a LGPD no que tange a consentimento e anonimização dos dados.

Da Comissão de Valores Mobiliários – CVM, é possível destacar ao menos três instruções. A Instrução nº 380 de 23 de dezembro de 2002, que estabelece as normas para a troca de dados nas operações realizadas pela internet . A CVM também regulou a política de divulgação de dados através da Instrução nº 461, de 23 de Outrubro de 2007. A referida norma, prevê a possibilidade de recuperação dos dados sobre as operações realizadas. Inclusive com a identificação dos beneficiários finais (Art. 68, inciso IV, alínea "a") , o que poderá ocasionar conflitos com a LGPD e também com a lei europeia de proteção de dados, a General Data Protection Regulation (GDPR), já que o aludido artigo referencia a transmissão de dados para bolsa de valores estrangeira. A terceira instrução da CVM que merece relevo é a Instrução nº 467 de 2008, a qual criou mecanismos de compartilhamento de dados sobre operações com contratos derivativos (art. 4º) além de ter incorporado a partir do ano de 2010 a possibilidade de compartilhamento de dados mediante consentimento expresso das contrapartes envolvidas na operação .

O Banco Central do Brasil – BACEN também editou normas que abordam a proteção e tratamento de dados pessoais. A Circular nº 3.567, de 12 de dezembro de 2011, dispõe sobre o tratamento dos dados de forma individualizada dos clientes integrantes de conglomerados econômicos . Em medidas mais recentes, o BACEN tratou da gestão de documentos digitalizados com a Resolução nº 4.474, de 31 de março de 2016, que prevê cópias de segurança dos dados digitalizados. A Resolução nº 4.480, de 25 de abril de 2016, traz (art. 7º) a previsão de armazenamento dos dados referente a abertura e encerramento de contas de depósito por meio eletrônico, pelo prazo mínimo de cinco anos pelo Banco Central do Brasil .

Não são só normas recentes que abordam a temática de tratamento de dados pessoais. Ao contrário do que se possa pensar, existem no Brasil legislações desde a década de oitenta, que tratam desse assunto. A exemplo da Lei nº 7.232, de 29 de outubro de 1984 que tem como disposição principal a Política Nacional de Informática, mas que traz entre seus princípios (art 2º, inciso VIII), por exemplo, o estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas.

Na sequência, a lei ainda menciona no mesmo artigo com princípios (art. 2º, inciso IX) a previsão de estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas . Ambas previsões que se assemelham ao que está previsto na própria LGPD no seu respectivo artigo 18 para citar como exemplo.

A Lei Orgânica do Tribunal de Contas da União – TCU, traz entre as obrigações dos servidores (Art. 86º) o sigilo sobre dados e informações obtidos em decorrência do exercício de suas funções, prevendo o uso exclusivamente, para a elaboração de pareceres e relatórios destinados à chefia imediata.

No caso do Ministério Público da União – MPU, a lei que dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União, tem uma previsão com potencial conflitante com a proteção de dados pessoais. A legislação até então permite que o MPU poderá nos procedimentos de sua competência ter acesso incondicional a qualquer banco de dados de caráter público (art. 8º, inciso VIII) . Isso poderá gerar conflito de competência com a LGPD e com a própria ANPD, visto que a Lei Geral de Proteção de Dados (art. 26º) normatiza que o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas, além de serem respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei, ou seja, não prevê acesso incondicional.

A legislação eleitoral também está repleta de previsões que discutem a questão dos dados pessoais, como exemplo mais latente, pode-se citar a Lei nº 9.504, de 30 de setembro de 1997 , que estabelece normas para as eleições. O artigo 33 é um norte de como essa legislação será afetada pela LGPD, visto que trata das pesquisas e testes pré-eleitorais, ou seja, da coleta de dados e do trabalho de campo. Vale destacar que a LGPD considera a informação sobre filiação partidária (art. 5º, inciso II) um dado pessoal sensível.Muitas outras normas tratam direta ou indiretamente sobre a coleta, tratamento e uso de dados pessoais. Em função do objetivo proposto na presente pesquisa, limitarse-á a citá-las como forma de indicar as previsões legais que tratam da temática, para atender a finalidade e respeitar o limite de extensão do trabalho.

Assim, cita-se: Lei 12.527/2011: Lei de acesso à informação (Art. 4º IV e Art. 31) ; Decreto 8.777/16: Política de Dados Abertos do Governo Federal ; Decreto nº 8.764/16: Institui o Sistema Nacional de Gestão de Informações Territoriais - SINTER ; Lei nº 13.444/17 Dispõe sobre a Identificação Civil Nacional (ICN); Decreto 6.425/2008: Dispõe sobre o censo anual da educação ; Lei

9.472/97: Lei Geral de Telecomunicações (Art. 3º, IX) ; Lei 10.703/2003: Dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos e dá outras providências ; Decreto-Lei 2.848/1940 ("Código Penal"): Arts. 153, §1-A, 313- A, Art. 154-A, artigos 13-A (requisição, sem ordem judicial de dados cadastrais) e 13-B (requisição judicial de dados de localização) ; Lei 7.492/86: Define os crimes contra o sistema financeiro nacional (Art. 18, considera crime a violação do dever de sigilo das instituições financeiras) ; Lei 9.296/96: Lei de Interceptação Telefônica; Lei 12.737/2012: Crime de invasão de dispositivos informáticos (Lei Carolina Dieckmann) ; Lei 12.846/2013: Lei anticorrupção .

Ainda cabe destaque seguramente, a lei que regulou o Habeas Data, a qual não poderia deixar de ser mencionada. Com previsão constitucional como direito fundamental, no artigo 5º, inciso LXXII, o Habeas Data foi regulado pela lei nº 9.507, de 12 de novembro de 1997 , e traz previsões que possibilitam em tese o titular dos dados a ter acesso as informações constantes de registro ou banco de dados de entidades governamentais ou de caráter público, além de prever também a possibilidade de retificação dos dados (Art. 7º).

Outra norma que poderá gerar intenso debate sobre a proteção e principalmente uso do banco de dados, é o decreto que dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal. O decreto nº 6.135, de 26 de junho de 2007, traz algumas previsões de que os dados coletados são sigilosos e somente poderão ser utilizados para as finalidades de formulação e gestão de políticas públicas, e realização de estudos e pesquisas (Art. 8º) , todavia, não traz garantias de que haverá anonimização, conforme prevê a LGPD (Art. 7º, inciso IV).

O objetivo do presente tópico foi apresentar sumariamente a legislação vigente no Brasil que trata, direta ou indiretamente, da proteção de dados no país. Obviamente que não esgotou aqui nessa pesquisa todas as normas com disposições sobre dados pessoais, entretanto, desconstruiu-se a ideia de que o Brasil não possuía leis e normas que protegiam os dados pessoais. É neste contexto que passamos para o tópico final do presente trabalho, para analisar a necessidade de positivar o direito de proteção dos dados pessoais como direito fundamental.

3 PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL, PRINCIPAIS PONTOS DE DEBATE SOBRE A PROPOSTA DE EMENDA À CONSTITUIÇÃO Nº 17, DE 2019

As discussões sobre a proteção de dados entraram em um novo rumo após a promulgação da LGPD e a sua entrada em vigor em 18 de 09 de 2020.

Contudo, existem ainda debates abertos, como é o caso da proposta de Emenda à Constituição nº 17, de 2019 , que propõe o acréscimo do inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22 da Constituição Federal, para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

A PEC nº 17/2019 põe na mesa a discussão sobre a (des) necessidade de inclusão da proteção de dados no rol de direitos fundamentais, em outras palavras, inaugura o debate sobre a necessidade da proteção ser tratada como um direito fundamental autônomo.

Agora em 2020, mesmo após a vigência da LGPD, essa discussão ainda está ativa, visto que a PEC foi aprovada pelo Senado mas ainda carece de apreciação pelo plenário da Câmara dos Deputados Federais. Todavia, já conta nessa casa legislativa com aprovação, tanto pela Comissão de Constituição e Justiça e De Cidadania (CCJC), quanto pela Comissão Especial .

Antes da emissão dos pareceres favoráveis pelas comissões especial e CCJC, foram realizadas audiências públicas, nas quais houveram participações multisetoriais, com a finalidade de discussão sobre a PEC. Podendo citar entre os participantes, da parte da academia, Universidade de Brasília (UnB), Instituto Brasiliense de Direito Público (IDP), Pontifícia Universidade Católica do Rio de Janeiro (PUC/RJ) e Laboratório de Políticas Públicas e Internet da Universidade de Brasília (Lapin).

Ainda, as audiências públicas contaram com integrantes do terceiro setor, sendo representados pelo Instituto Nacional de Defesa do Consumidor, Instituto Brasileiro de Defesa do Consumidor (Idec), Coding Rights, InternetLab, Intervozes, ITS-Rio e Data Privacy Brasil. No ramo empresarial foram ouvidas associações empresariais como a Brasscom, Febraban, ANBI, Abratel, ASSESPRO, Confederação Nacional dos Dirigentes Lojistas (CNDL), Coalizão da Comunicação Social e CNI, além de empresas representando o governo como a Serpro e o Banco Central do Brasil.

Da série de audiências públicas (disponíveis na íntegra, 1 , 2 , 3 e 4), é possível constatar a inclinação para o consenso em torno da aprovação da PEC. No que tange os argumentos apresentados, verificam-se poucas discordâncias e quase ausência de discordâncias discrepantes, sinal disso é que nenhum dos vinte e dois debatedores manifestou posição contrária a proposta de emenda à constituição.

O principal argumento mobilizado em defesa desta mudança foi que, embora a Constituição tutele a intimidade e a vida privada (art. 5º, X), há uma distinção essencial entre privacidade, uma liberdade negativa, de não-intervenção, e proteção de dados pessoais, liberdade positiva, que se espraia para além do ambiente privado e diz respeito à circulação e controle sobre dados pessoais, que justifica a necessidade de sua garantia enquanto direito fundamental autônomo.

Pode-se destacar que, de modo geral, o principal argumento utilizado nas audiências e mobilizado para defender esta mudança é que embora a Constituição proteja a intimidade e a vida privada (Artigo 5 X), existem diferenças essenciais entre privacidade, liberdade negativa, não ingerência e proteção de dados pessoais. A liberdade positiva não se limita ao ambiente privado, mas envolve também a circulação e o controle dos dados pessoais, o que provaria a necessidade de positivar a proteção de dados pessoais como direito fundamental autônomo .

Sobre a temática, o doutrinador Ingo Wolfgang Sarlet recentemente posicionou-se no sentido de que o direito fundamental à

proteção de dados pessoais deve ser compreendido e aplicado no contexto daquilo que se tem chamado de um constitucionalismo de múltiplos níveis, sem falar da recepção doutrinária e jurisprudencial, de experiências de outros países, como se deu (e dá) justamente na seara da proteção de dados, bastando aqui, em caráter ilustrativo, apontar para o direito à autodeterminação informativa e à influência do Regulamento Geral Europeu de proteção de dados sobre a nossa LGPD .

Outro elemento a ser considerado quando se demanda a respeito de direitos fundamentais, e o âmago da discussão aqui é justamente a inclusão da proteção dos dados pessoais como direito fundamental, é em relação ao dever de proteção. Segundo Morais, a "atuação ou omissão do Estado implica a assunção de efetivar o dever de proteção (Schutzpflicht), que nada mais é do que reconhecer a condição compromissória e dirigente da Constituição", ou seja, "assumiu-se um compromisso com os Direitos Fundamentais, inclusive, dotando o sistema jurídico de instrumentos processuais apropriados que garantam essa concretização através do poder judiciário."

É exatamente sobre essa conjuntura que encaixa o enfoque dado por Vieira de Andrade, que aponta para o requisito do dever de proteção ao nível da intervenção legislativa e para além da "obrigatoriedade de legislação específica" contida na tutela dos direitos fundamentais na Constituição. Também determinou a sua formulação inspirada no princípio da proibição do excesso, um princípio de proibição de déficit (Übermaβverbot). De acordo com este princípio, o Estado é obrigado a garantir a proteção mínima adequada dos direitos fundamentais, sendo inclusive responsável por eventuais omissões legislativas que não assegurem o cuprimento dessa condição impositiva genérica.

Sobre essas perspectivas, para além da discussão sobre a inclusão ou não da proteção dos dados pessoais como direito fundamental e a sua distinção como direito autônomo, está o papel do Estado pelo seu dever de proteção, zelar ativamente, pela consistência e efetividade não só da LGPD mas de todas as normas e leis vigentes no Brasil que dizem respeito a proteção dos dados pessoais.

3 CONCLUSÕES

Para além e antes da LGPD, o cenário regulatório do Brasil para a proteção de dados pessoais é muito mais complexo. Como restou demonstrado, existem múltiplos diplomas legais, códigos, leis, decretos, resoluções e instruções, que tratam direta ou indiretamente a temática dos dados pessoais.

Essa situação é desafiadora para empresas e usuários, para a doutrina e a jurisprudência, bem como para a própria efetividade do direito de proteção aos dados pessoais. Diante de uma teia complexa e entrelaçada, com dezenas de normas vigentes que abordam a proteção dos dados pessoais, elas não podem ser tratadas de maneira isolada, principalmente com a vigência da lei geral de proteção de dados, assim a possibilidade de conflitos entre essas regras é iminente e inevitável.

Diante desse cenário, a inclusão da proteção dos dados pessoais como direito fundamental, conforme propõe a PEC nº 17/2019, mostra-se adequada. Conclusão que aponta através dessa perspectiva para a confirmação da hipótese em resposta ao problema proposto. Entendimento ainda consubstanciado diante do dever de proteção do Estado.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. CIRCULAR Nº 3.567, DE 12 DE DEZEMBRO DE 2011. Dispõe sobre o fornecimento de informações relativas a operações de crédito ao Sistema de Informações de Créditos (SCR), de que trata a Resolução nº 3.658, de 17 de dezembro de 2008. Disponível em https://www.bcb.gov.br/pre/normativos/circ/2011/pdf/circ_3567_v1_O.pdf. Acesso em: 06 out. 2020.

BANCO CENTRAL DO BRASIL. RESOLUÇÃO Nº 4.480, DE 25 DE ABRIL DE 2016. Dispõe sobre a abertura e o encerramento de contas de depósitos por meio eletrônico e dá outras providências. Disponível em https://tinyurl.com/y2qfrh7a. Acesso em: 06 out. 2020.

BRASIL. Agência Nacional de Saúde Suplementar. RESOLUÇÃO NORMATIVA - RN Nº- 341, DE 27 DE NOVEMBRO DE 2013. Dispõe sobre Boas Práticas Farmacêuticas. Disponível em: https://tinyurl.com/y6enlryc. Acesso em: 02 out. 2020.

BRASIL. Agência Nacional De Vigilância Sanitária – ANVISA. Resolução da diretoria colegiada – rdc nº 44, de 17 de agosto de 2009. Dispõe sobre Boas Práticas Farmacêuticas. Disponível em: https://www20.anvisa.gov.br/segurancadopaciente/index.php/legislacao/item/rdc-44-2009. Acesso em: 02 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Reunião Deliberativa Ordinária – 05/11/2019. Disponível em: https://www.camara.leg.br/evento-legislativo/58409. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Reunião Deliberativa Ordinária – 12/11/2019. Disponível em: https://www.camara.leg.br/evento-legislativo/58535. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Reunião Deliberativa Ordinária - 22/10/2019. Disponível em: https://www.camara.leg.br/evento-legislativo/58183. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Reunião Deliberativa Ordinária - 29/10/2019. Disponível em: https://www.camara.leg.br/evento-legislativo/58296. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Proposta de Emenda à Constituição n° 17, de 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 08 out. 2020.

BRASIL. DECRETO Nº 4.489, DE 28 DE NOVEMBRO DE 2002. Regulamenta o art. 5º da Lei Complementar nº 105, de 10 de janeiro de 2001, no que concerne à prestação de informações à Secretaria da Receita Federal do Ministério da Fazenda, pelas instituições financeiras e as entidades a elas equiparadas, relativas às operações financeiras efetuadas pelos usuários de seus serviços. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2002/D4489.htmAcesso em: 02 out. 2020.

BRASIL. DECRETO Nº

6.135, DE 26 DE JUNHO DE 2007. Dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/d6135.htm. Acesso em: 08 out. 2020.

BRASIL. DECRETO Nº 7.962, DE 15 DE MARÇO DE 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: https://tinyurl.com/yyyxxpyc. Acesso em: 30 set. 2020.

BRASIL. DECRETO Nº 8.764, DE 10 DE MAIO DE 2016.

Institui o Sistema Nacional de Gestão de Informações Territoriais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8764.htm. Acesso em: 08 out. 2020.

BRASIL. DECRETO Nº 8.771, DE 11 DE MAIO DE 2016. Regulamenta a Lei nº 12.965/2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 30 set. 2020.

BRASIL. DECRETO Nº 8.777, DE 11 DE MAIO DE 2016.
Institui a Política de Dados Abertos do Poder Executivo federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm. Acesso em: 08 out. 2020.

BRASIL. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08 out. 2020.

BRASIL. LEI COMPLEMENTAR Nº 75, DE 20 DE MAIO DE 1993. Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp75.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 12.414, DE 9 DE JUNHO DE 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 30 set. 2020.

BRASIL. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011.
Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 12.846, DE 1º DE AGOSTO DE 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 08 out. 2020.

BRASIL. Lei Nº 12.965, de 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 set. 2020.

BRASIL. LEI Nº 13.444, DE 11 DE MAIO DE 2017.

Dispõe sobre a Identificação Civil Nacional (ICN). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 7.232, DE 29 DE OUTUBRO DE 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7232.htm. Acesso em: 06 out. 2020.

BRASIL. LEI Nº 7.492, DE 16 DE JUNHO DE 1986. Define os crimes contra o sistema financeiro nacional, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7492.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 30 set. 2020.

BRASIL. Lei Nº 8.443, DE 16 DE JULHO DE 1992. Dispõe sobre a Lei Orgânica do Tribunal de Contas da União e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8443.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 9.296, DE 24 DE JULHO DE 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 9.472, DE 16 DE JULHO DE 1997.
Dispõe sobre a organização dos serviços de telecomunicações. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 9.504, DE 30 DE SETEMBRO DE 1997. Estabelece normas para as eleições. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997.
Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: http://www.planalto.gov.br/CCIVIL_03/LEIS/L9507.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº10.703, DE 18 DE JULHO DE 2003.
Dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.703.htm. Acesso em: 08 out. 2020.

BRASIL. Portaria nº 5, de 27 de agosto de 2002.. Complementa o elenco de cláusulas abusivas constante do art. 51 da Lei n º 8.078, de 11 de setembro de 1990. Disponível em: https://tinyurl.com/y4w3c7qk. Acesso em: 30 set. 2020.

BRASIL. SENADO FEDERAL. Proposta de Emenda à Constituição n° 17, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 08 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS – CVM. INSTRUÇÃO CVM No 380, DE 23 DE DEZEMBRO DE 2002. Estabelece normas e procedimentos a serem observados nas operações realizadas em bolsas e mercados de balcão

organizado por meio da rede mundial de computadores e dá outras providências. Disponível em: http://www.cvm.gov.br/export/sites/cvm/legislacao/instrucoes/anexos/300/inst380consolid.pdf. Acesso em: 02 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS – CVM. Instrução nº 461, de 23 de Outrubro de 2007. Disciplina os mercados regulamentados de valores mobiliários e dispõe sobre a constituição, organização, funcionamento e extinção das bolsas de valores, bolsas de mercadorias e futuros e mercados de balcão organizado. Disponível em: http://www.cvm.gov.br/legislacao/instrucoes/inst461.html. Acesso em: 02 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS – CVM. Instrução nº 467, de 10 de Abril de 2008. Dispõe sobre a aprovação de contratos derivativos admitidos à negociação ou registrados nos mercados organizados de valores mobiliários. Disponível em: http://www.cvm.gov.br/legislacao/instrucoes/inst467.html. Acesso em: 02 out. 2020.

CONSELHO FEDEAL DE MECIDINA. Resolução nº 2.145/2016. Aprova o Código de Processo Ético-Profissional (CPEP) no âmbito do Conselho Federal de Medicina (CFM) e Conselhos Regionais de Medicina (CRMs). Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2016/2145. Acesso em: 30 set. 2020.

MORAIS, Fausto Santos de. Ponderação e Arbitrariedade: A Inadequada Recepcção de Alexy pelo STF / coordenador Lenio Luiz Streck – 2. Ed. Ver. e atual.-Salvador:Jurpodvm, 2018. p. 33.

RIELLI, Mariana. Et al. Os dilemas do Direito Constitucional à proteção de dados. Disponível em: https://tinyurl.com/y26p72hd. Acesso em: 08 out. 2020.

SARLET, Ingo Wolfgang. Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF?. Disponível em: https://tinyurl.com/y6ohg4x5. Acesso em: 08 out. 2020.

VIEIRA, José Carlos de Andrade. Os direitos fundamentais na Constituição portuguesa de 1976. 2.ed. Coimbra: Almedina, 2001. p. 144.

NOTAS:

Mestre em Direito pela Faculdade IMED com pesquisa voltada em Inteligência Artificial e Direito. Latim Legum Magister – L.L.M em Direito Empresarial pela Fundação Getúlio Vargas – FGV. Direito em Startups pelo Insper – São Paulo (2018). Pós-graduado em Direito Educacional pela Faculdade Unyleya do Distrito Federal (2017). Graduação em Direito pela Universidade de Passo Fundo (2014). Editor Executivo da Revista Brasileira de Inteligência Artificial e Direito – RBIAD (ISSN 2675-3146). Membro Fundador da Associação Ibero Americana de Inteligência Artificial e Direito/AID-IA. Membro da Comissão de Estudos sobre Constituição de Justiça – CECJ – da Ordem do Advogados do Brasil. Integrante do Grupo de Estudos sobre Inteligência Artificial e Direito – IAJUS – certificado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq. Certificação em LGPD, Segurança de dados e Responsabilidade Digital – PUC/RS.

Doutor em Direito pela UNISINOS. Pesquisador com apoio da Fundação Meridional. Coordenador do projeto de pesquisa: Direitos Fundamentais, Hermenêutica e Proporcionalidade: crítica ao desenvolvimento prático-teórico do dever de proteção aos Direitos Fundamentais e do IAJUSTEAM – Grupo de Pesquisa em IA e Direito. Link Currículo Lattes: http://lattes.cnpq.br/2028518764749733

BRASIL. Lei Nº 12.965, de 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 set. 2020.

Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

BRASIL. DECRETO Nº 8.771, DE 11 DE MAIO DE 2016. Regulamenta a Lei nº 12.965/2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 30 set. 2020.

BRASIL. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 30 set. 2020.

BRASIL. Portaria nº 5, de 27 de agosto de 2002.. Complementa o elenco de cláusulas

abusivas constante do art. 51 da Lei n º

8.078, de 11 de setembro de 1990. Disponível em: https://tinyurl.com/y4w3c7qk. Acesso em: 30 set. 2020.

BRASIL. LEI Nº 12.414, DE 9 DE JUNHO DE 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 30 set. 2020.

BRASIL. DECRETO Nº 7.962, DE 15 DE MARÇO DE 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.

. Disponível em: https://tinyurl.com/yyyxxpyc. Acesso em: 30 set. 2020.

CONSELHO FEDEAL DE MECIDINA. Resolução nº 2.145/2016. Aprova o Código de Processo Ético-Profissional (CPEP) no âmbito do Conselho Federal de Medicina (CFM) e Conselhos Regionais de Medicina (CRMs). Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2016/2145. Acesso em: 30 set. 2020.

BRASIL. Agência Nacional De Vigilância Sanitária – ANVISA. Resolução da diretoria colegiada – rdc nº 44, de 17 de agosto de 2009.

Dispõe sobre Boas Práticas Farmacêuticas. Disponível em: https://www20.anvisa.gov.br/segurancadopaciente/index.php/legislacao/item/rdc-44-2009. Acesso em: 02 out. 2020.

BRASIL. Agência Nacional de Saúde Suplementar. RESOLUÇÃO NORMATIVA - RN Nº- 341, DE 27 DE NOVEMBRO DE 2013. Dispõe sobre Boas Práticas Farmacêuticas. Disponível em: https://tinyurl.com/y6enlryc. Acesso em: 02 out. 2020.

BRASIL. DECRETO Nº 4.489, DE 28 DE NOVEMBRO DE 2002. Regulamenta o art. 5º da Lei Complementar nº 105, de 10 de janeiro de 2001, no que concerne à prestação de informações à Secretaria da Receita Federal do Ministério da Fazenda, pelas instituições financeiras e as entidades a elas equiparadas, relativas às operações financeiras efetuadas pelos usuários de seus serviços. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2002/D4489.htmAcesso em: 02 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS – CVM. INSTRUÇÃO CVM No 380, DE 23 DE DEZEMBRO DE 2002. Estabelece normas e procedimentos a serem observados nas operações realizadas em bolsas e mercados de balcão organizado por meio da rede mundial de computadores e dá outras providências. Disponível em: http://www.cvm.gov.br/export/sites/cvm/legislacao/instrucoes/anexos/300/inst380consolid.pdf. Acesso em: 02 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS – CVM. Instrução nº 461, de 23 de Outrubro de 2007. Disciplina os mercados regulamentados de valores mobiliários e dispõe sobre a constituição, organização, funcionamento e extinção das bolsas de valores, bolsas de mercadorias e futuros e mercados de balcão organizado. Disponível em: http://www.cvm.gov.br/legislacao/instrucoes/inst461.html. Acesso em: 02 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS – CVM. Instrução nº 467, de 10 de Abril de 2008. Dispõe sobre a aprovação de contratos derivativos admitidos à negociação ou registrados nos mercados organizados de valores mobiliários. Disponível em: http://www.cvm.gov.br/legislacao/instrucoes/inst467.html. Acesso em: 02 out. 2020.

Alteração incluída pela Instrução CVM nº 487/10, que modificou a Instrução nº 467/2008.

BANCO CENTRAL DO BRASIL. CIRCULAR Nº 3.567, DE 12 DE DEZEMBRO DE 2011. Dispõe sobre o fornecimento de informações relativas a operações de crédito ao Sistema de Informações de Créditos (SCR), de que trata a Resolução nº 3.658, de 17 de dezembro de 2008. Disponível em https://www.bcb.gov.br/pre/normativos/circ/2011/pdf/circ_3567_v1_O.pdf. Acesso em: 06 out. 2020.

BANCO CENTRAL DO BRASIL. RESOLUÇÃO Nº 4.480, DE 25 DE ABRIL DE 2016. Dispõe sobre a abertura e o encerramento de contas de depósitos por meio eletrônico e dá outras providências. Disponível em https://tinyurl.com/y2qfrh7a. Acesso em: 06 out. 2020.

BRASIL. LEI Nº 7.232, DE 29 DE OUTUBRO DE 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7232.htm. Acesso em: 06 out. 2020.

BRASIL. Lei Nº 8.443, DE 16 DE JULHO DE 1992. Dispõe sobre a Lei Orgânica do Tribunal de Contas da União e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8443.htm. Acesso em: 08 out. 2020.

BRASIL. LEI COMPLEMENTAR Nº 75, DE 20 DE MAIO DE 1993. Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp75.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 9.504, DE 30 DE SETEMBRO DE 1997.
Estabelece normas para as eleições. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011.
Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 08 out. 2020.

BRASIL. DECRETO Nº 8.777, DE 11 DE MAIO DE 2016.
Institui a Política de Dados Abertos do Poder Executivo federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm. Acesso em: 08 out. 2020.

BRASIL. DECRETO Nº 8.764, DE 10 DE MAIO DE 2016.
Institui o Sistema Nacional de Gestão de Informações Territoriais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8764.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 13.444, DE 11 DE MAIO DE 2017.
Dispõe sobre a Identificação Civil Nacional (ICN). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 9.472, DE 16 DE JULHO DE 1997.
Dispõe sobre a organização dos serviços de telecomunicações. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº10.703, DE 18 DE JULHO DE 2003.
Dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.703.htm. Acesso em: 08 out. 2020.

BRASIL. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 7.492, DE 16 DE JUNHO DE 1986.
Define os crimes contra o sistema financeiro nacional, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7492.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 9.296, DE 24 DE JULHO DE 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

Acesso em: 08 out. 2020.

BRASIL. LEI Nº 12.846, DE 1º DE AGOSTO DE 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 08 out. 2020.

BRASIL. LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997.

Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: http://www.planalto.gov.br/CCIVIL_03/LEIS/L9507.htm. Acesso em: 08 out. 2020.

BRASIL. DECRETO Nº 6.135, DE 26 DE JUNHO DE 2007. Dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/d6135.htm. Acesso em: 08 out. 2020.

BRASIL. SENADO FEDERAL. Proposta de Emenda à Constituição n° 17, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Proposta de Emenda à Constituição n° 17, de 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Reunião Deliberativa Ordinária - 22/10/2019. Disponível em: https://www.camara.leg.br/evento-legislativo/58183. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Reunião Deliberativa Ordinária - 29/10/2019. Disponível em: https://www.camara.leg.br/evento-legislativo/58296. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Reunião Deliberativa Ordinária – 05/11/2019. Disponível em: https://www.camara.leg.br/evento-legislativo/58409. Acesso em: 08 out. 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Reunião Deliberativa Ordinária – 12/11/2019. Disponível em: https://www.camara.leg.br/evento-legislativo/58535. Acesso em: 08 out. 2020.

RIELLI, Mariana. Et al. Os dilemas do Direito Constitucional à proteção de dados. Disponível em: https://tinyurl.com/y26p72hd. Acesso em: 08 out. 2020.

SARLET, Ingo Wolfgang. Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF?. Disponível em: https://tinyurl.com/y6ohg4x5. Acesso em: 08 out. 2020.

MORAIS, Fausto Santos de. Ponderação e Arbitrariedade: A Inadequada Recepcção de Alexy pelo STF / coordenador Lenio Luiz Streck – 2. Ed. Ver. e atual.-Salvador:Jurpodvm, 2018. p. 33.

VIEIRA, José Carlos de Andrade. Os direitos fundamentais na Constituição portuguesa de 1976. 2.ed. Coimbra: Almedina, 2001. p. 144.

ELDFA. LIVES
ESCOLA LIVRE
DIREITO FILOSOFIA
E ARTE

projeto poiesis

LIVES

VALOR (E ANTIVALOR) ECONÔMICO APLICADO À REGULAMENTAÇÃO NORMATIVA PARA A GIG ECONOMY

THIAGO FELIPE S. AVANCI, PH.D.

A indústria 4.0 é algo inexorável e provocou profundas mudanças na forma como o ser humano compreende a vida em sociedade. Em breves linhas, conceitua-se indústria 4.0 como sendo uma nova fase inaugurada a partir de um conjunto de mudanças nas relações sociais, para a economia de mercado e de trabalho, consequentemente, provocadas pela massificação do uso da tecnologia e da internet, em especial a partir dos anos 2000. Fruto deste fenômeno e mudanças, a gig economy também é inserida neste contexto, podendo ser compreendida como modalidade de trabalho – autônomo ou não – em que o prestador do serviço atua junto ao tomador do serviço a partir da intermediação de uma ferramenta, normalmente tecnológica.

Estabelecendo-se uma análise econômica do Direito, percebe-se que todo o processo de normatização deve – necessariamente – buscar gerar valor econômico , de modo que possibilite a atividade saudável do mercado. Em sede de simplificação e considerando o espaço "escasso" para o debate neste ensaio, dentro de uma economia capitalista neoliberal, valor econômico pode ser considerado como a riqueza gerada pelo mercado, ao passo que antivalor consiste justamente em perdas de riqueza. Valor econômico não se confunde com valor axiológico; o valor econômico atribuído à mercadoria deriva não somente do valor-uso do bem, mas do valor-troca do mesmo, sendo este definido por sua escassez (oferta) e por sua utilidade (procura), representado pelo preço da mercadoria.

Com esta preliminar análise superficial dos conceitos arranhados neste ensaio, começa-se a perceber uma problemática inerente à métrica macroeconômica como um todo: quais são os limites da intervenção do Estado na gig economy, sem que isso gere antivalor? Esta é o objeto que se pretende analisar.

O que se tem observado empiricamente, em análise preliminar, é que o equilíbrio econômico capaz de gerar, otimizadamente, valor econômico – riqueza – a todos é extremamente delicado: intervenção excessiva do Estado sobre a economia pode gerar antivalor; ausência de intervenção do Estado sobre a economia pode gerar antivalor, também. Não é demais salientar que este equilibro delicado foi descrito, em análise econômica, pela teoria do deadweight. Assim, quando se fala em intervenção do Estado, entenda-se que está se tratando de normatização como o meio pelo qual se gerará potencialmente este "peso morto".

Por óbvio, observa-se que o "peso morto" deve ser limitado ao mínimo. A construção normatizadora de um instituto como o gig economy pode ser regulamentada, mas isso não significa que cada aspecto desta nova expressão do mercado precise de um instrumento normativo limitador ou tolhedor. Muito ao contrário. Esta expressão nasce com espirito de liberdade alternativo à métrica da relação de emprego convencional e mesmo à prestação de serviços convencional. Por outro lado, deixar de regular determinados Direitos, especialmente dos prestadores, que aparentemente encontram-se em posição de hipossuficiência, também significa agredir o Estado Social Democrático de Direito constituído no Brasil. Deveras, o equilíbrio de Nash e o ótimo de Parreto explicam a delicadeza de tal construção, a partir de uma análise pela teoria dos jogos.

Em sede de conclusão, se propõe que a normatização da gig economy observe sua finalidade de gerar valor econômico à sociedade e ao Estado. Para que isso seja possível, de forma otimizada, sugere-se que sejam observados os seguintes pontos para a construção normativa do instituto em questão: excesso de intervenção gera antivalor, porquanto cria obrigações excessivas ao investidor, gera burocracia e tolhe a livre inciativa; falta de intervenção gera antivalor porque agride o Estado Social Democrático de Direito.

Referências

ABBOTT, D.; HARMER, G. P.; PARRONDO, J. New Paradoxical Games Based on Brownian Ratchets. PHYSICAL REVIEW LETTERS, v. 85, n. 24, p. 5226, dezembro 2000. Disponível em: <https://www.academia.edu/18847964/New_Paradoxical_Games_Based_on_Brownian_Ratchets>.

COASE, R. H. The Problem of Social Cost. The Journal of Law and Economics, p. 1-44, out./1960.

FOOT, P. The Problem of Abortion and the Doctrine of the Double Effect in Virtues and Vices. Oxford Review, p. Number 5, s/p, 1967. Disponivel em:<. Disponível em < http://www2.econ.iastate.edu/classes/econ362/hallam/Readings/FootDoubleEffect.pdf >>. Acesso em: 01 jan. 2019.

FULLERTON, D. Laffer curve. The New Palgrave Dictionary of Economics, 2006. Disponivel em: <doi:10.1057/9780230226203.0922 >. Acesso em: 19 jul. 2019.

KEYNES, J. M. Teoria geral do emprego, do juro e da moeda (General theory of employment, interest and money). Tradução de Mário Ribeiro da CRUZ. São Paulo: Atlas, 1992.

KONDRATIEV, N. Los ciclos largos de la coyuntura economica. Tradução de Luis Sandoval RAMÍREZ. 2ª ed. ed. México D.F: UNAM, 1992.

LAFFER, A. The Laffer Curve: Past, Present, and Future. Laffer Associates, 01 jun. 2004. Disponivel em: <https://www.heritage.org/taxes/report/the-laffer-curve-past-present-and-future>. Acesso em: 12 jul. 2019.

MARSLEV, K.; SANO, H.-O. HUMAN RIGHTS AND ECONOMIC GROWTH AN ECONOMETRIC ANALYSIS OF FREEDOM AND PARTICIPATION RIGHTS. the Danish Institute for Human Rights, 2016. Disponivel em: <https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/udgivelser/working_papers_2016/the_economics_of_human_rights_2016.pdf>. Acesso em: 20 jun. 2019.

MARX, K. O capital: crítica de economia política. Livro I: O processo de produção do capital. Tradução de Rubens Enderle. São Paulo: Boitempo, 2013.

MOKYR, J. Thinking About Technology and Institutions. Macalester International, v. Article 8, p. 19-24, 2013.

NASH JR, J. F. Equilibrium points in n-person games. PNAS, 1950. Disponivel em: <https://doi.org/10.1073/pnas.36.1.48>. Acesso em: 2019 dez. 20.

NEUMANN, J. V.; MORGENSTERN, O. Theory of games and economic behavior. 3ª Ed. ed. Princeton: Princeton University Press , 1953.

OLIVEIRA, F. D. O SURGIMENTO DO ANTIVALOR. UFPB, 2013. Disponivel em: <https://www.ets.ufpb.br/pdf/2013/1%20Estado%20e%20Politicas%20Publicas/EPP%2005_Oliveira_O%20surgimento%20do%20antivalor.pdf>. Acesso em: 25 jul. 2019.

PARETO, V. MANUAL DE ECONOMIA POLÍTICA. Tradução de João Guilherme Vargas Netto. São Paulo: Nova Cultural, 1996.

SCHWAB, K. A quarta revolução industrial. Edipro: São Paulo, 2018.

SEN, A. A Ideia de Justiça. São Paulo: Schwarcz, 2009.

SMITH, A. A Riqueza das Nações. Tradução de Alexandre Amaral Rodrigues e Eunice Ostrensky. São Paulo: Martins Fontes, 2003.

REGULAMENTAÇÃO DA EMPRESA E PROTEÇÃO DE DIREITOS NA ERA TECNOLÓGICA

ANNA CAROLINA PINHO

A vida contemporânea está a ser dominada pela realidade digital e as tecnologias da informação. Presenciamos profundas transformações sociais com o surgimento de novas oportunidades e problemas sem precedentes. A revolução tecnológica tem um impacto profundo no cotidiano, nas relações sociais e nas formas de participação na vida pública, influenciando o progresso e o comportamento humano.

O direito continua a ter a função de disciplinar as tecnologias da informação e da realidade digital de natureza contemporânea, delineando regras, princípios e valores compartilhados, governando o comportamento, definindo responsabilidades, protegendo conflitos e direitos. No cumprimento de sua função, a lei está disposta a mudar o que decorre das próprias características da era tecnológica. Em primeiro lugar, o objeto de regulação, hoje feito de bens intangíveis; em vez da produção de bens materiais, típica da sociedade industrial, a geração e o uso de dados adquirem contrações: os bens se transformam em serviços; o paradigma da propriedade cede em frente ao do acesso. Em segundo lugar, as tecnologias são regidas por instruções e códigos, regras computacionais capazes de condicionar o comportamento humano, tornando certas ações tecnicamente possíveis e, portanto, condicionando qualquer outra forma de regulação, inclusive as legais.

Na era tecnológica, destaca-se também a mudança da dimensão temporal de referência. A tecnologia evolui de forma extremamente rápida, enquanto o direito é estruturalmente mais lento, pois é o resultado do processo democrático e de complexos equilíbrios entre direito e interesses diferentes.

Até agora, o mundo se tem caracterizado por uma pluralidade de sistemas jurídicos relativos aos vários Estados, que estabeleceram as regras em seus territórios. As fronteiras nacionais estão hoje sobrecarregadas pela revolução digital que requer soluções jurídicas homogêneas para serem eficazes. As atividades e as relações já não atingem o limite geográfico e isso determina a necessidade de as respostas jurídicas assumirem uma conotação supranacional homogênea, paralelamente às questões que estão sendo regulamentadas.

A Internet é o maior espaço público descentralizado e aterritorial, sobre o qual ninguém pode ostentar um poder exclusivo. Como resultado, surgem dificuldades na identificação da lei aplicável e surge um repensar do poder nacional acompanhado de uma inevitável erosão dos monopólios estatais, também ameaçados pelo papel assumido pelos poderes privados. Os gigantes tecnológicos como Google, Facebook, Amazon, Apple, Microdoft, aliás, ao contrário dos Estados, conquistaram a dimensão global, regulando o acesso aos serviços: esta é uma nova "lei" feita de regras capazes de afetar a vida das pessoas. Desta forma, os gigantes tecnológicos tornam-se efetivamente os controladores da área de acesso à vida digital, fragilizando o poder legislativo nacional e acabando por afetar os direitos e liberdades das pessoas: a era tecnológica passa, portanto, a definir novas geometrias de poder, confundindo a fronteira entre a dimensão pública soberana e a dimensão privada de interesses particulares.

Na difícil regulação devido ao cruzamento de fronteiras territoriais e à necessidade de novas formas de proteção, surge o risco de que o poder público deixe o campo livre às forças do mercado, dedicando-se à proteção de direitos e liberdades, cedendo à possibilidade de sua violação e outorga ao indivíduo a força para se proteger. A eventual renúncia aos poderes públicos para o exercício da sua função acarreta o perigo de uma espécie de privatização da rede, dominada pelo domínio dos mais fortes e caracterizada por um desrespeito sistemático dos direitos.

À luz desses perfis, a regulação jurídica da era tecnológica diz respeito à fisionomia a ser oferecida à sociedade futura, aos equilíbrios a serem traçados e à proteção a ser garantida aos direitos: a proteção dos direitos precisa do papel da lei.

A proteção da liberdade cibernética e dos direitos digitais, portanto, surge como questão incontornável da sociedade contemporânea, para evitar o risco de devolver a proteção ao próprio sujeito, parte débil na relação tanto com o Estado quanto com os gigantes tecnológicos.

As características da era tecnológica e da Internet, como em particular a abordagem descentralizada e a superação de barreiras geográficas, são particularmente reveladoras, uma vez que conduzem à necessidade de soluções supranacionais adequadas à nova dimensão global de referência. Por essas razões, não faltam teorias que qualificam a Internet como uma ordem jurídica autônoma: é o caso da "Declaração de Independência do Ciberespaço" de John Perry Barlow de 1996; a rede é interpretada como um espaço espontâneo regulado pela lex informática, baseado na autorregulação dos usuários e na co-regulação entre estados.

A este respeito, a nível internacional, a Declaração Universal dos Direitos do Homem, adotada pelas Nações Unidas a 10 de Dezembro de 1948, assinala, quando descreve o direito à liberdade à manifestação do pensamento como o direito de "procurar, receber e divulgar informação e ideias por qualquer meio e sem respeito pelas fronteiras (art. 19), com qualificação também adequada à sociedade tecnológica.

A Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais (CEDH) de 4 de novembro de 1950, posteriormente alterada e ampliada, também fala de liberdade de expressão "sem limites diante de nós", que só pode estar sujeita às limitações legais necessárias, em uma sociedade democrática, para proteger uma série de interesses protegidos (artigo 10) a serem protegidos também na Internet e na realidade digital, conforme afirmado em várias ocasiões pelo Tribunal Europeu dos Direitos do Homem.

Nesta direção observa o "Guia de Direitos Humanos para usuários de Internet" de 2014, a Recomendação CM / Rec (2014) 6 aos Estados Membros adotada em 16 de abril de 2014, na qual o Comitê de Ministros do Conselho da Europa esclarece que os Estados são obrigados a garantir os direitos humanos e as liberdades fundamentais a todas as pessoas também no contexto da Internet, aplicando os direitos

igualmente online e offline.

Na Carta dos Direitos Fundamentais da União Europeia, proclamada em 2000 e juridicamente vinculativa por ocasião da promulgação em vigor em 2009 do Tratado de Lisboa de 2007, também são estabelecidos princípios e direitos que podem constituir um fundamento na interpretação das liberdades da era digital, como a protecção da dignidade humana (artigo 1.º), a protecção dos dados pessoais (artigo 8.º) e a liberdade de expressão e informação (artigo 11.º).

A necessidade de proteger os direitos e as liberdades na sociedade tecnológica é expressa pelas instituições europeias também através de ações, resoluções e recomendações: é o caso da resolução do Parlamento Europeu de 6 de julho de 2006 sobre a liberdade de expressão na Internet, que afirma o papel da Internt, bem como o de exercer a liberdade de expressão, incluído para reforçar a democracia e contribuir para o desenvolvimento económico e social e a Recomendação do Parlamento Europeu de 26 de Março de 2009 sobre o reforço da segurança e das liberdades fundamentais na Internet. Na resolução do Parlamento Europeu de 15 de junho de 2010 "sobre a governança da Internet: os próximos passos", a Internet é definida como um bem público global e o seu acesso é descrito como um direito fundamental, essencial para o exercício de inúmeros direitos e liberdades. Na Resolução do Parlamento Europeu de 16 de março de 2017 "sobre a e-democracia na União Europeia: potencialidades e desafios" proclama-se que o acesso em igualdade de condições a uma rede neutra é um requisito essencial para garantir a eficácia dos direitos fundamentais da pessoa.

O Regulamento (UE) 2015/2120 de 25 de novembro de 2015 estabelece medidas relativas ao "acesso a uma Internet aberta" e descreve o princípio da neutralidade da rede que visa definir regras comuns para garantir o justo e o tratamento não discriminatório do tráfego na prestação de serviços de acesso à Internet e para proteção e direitos conexos dos usuários finais.

Algumas Constituições recentes ou recentemente modificadas referem-se explicitamente ao habeas data e às liberdades digitais; é o caso das Cartas Constitucionais da América Latina como o Brasil, Paraguai e México, da Constituição da Federação da Rússia de 1993, da República da África do Sul de 1996 e de algumas Cartas Européias como a Portuguesa e a Grega, após a revisão constitucional de 2001. Outros países preferiram expressar direitos relacionados às novas tecnologias na lei, como a Estônia e Filândia.

No contexto internacional, destaca-se o denominado Marco Civil da Internet, assim como a Lei 12.965 de 23 de abril de 2014 do Brasil, que em seus 32 artigos "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil "(artigo 1º) e garante os direitos que caracterizam a realidade digital, como o direito de acesso à Internet, liberdade de expressão e proteção de dados pessoais, acesso à informação e conhecimento, neutralidade, segurança das redes e seus natureza livre, aberta e participativa, o empoderamento dos agentes e a liberdade econômica.

Outros sistemas jurídicos regidos por Constituições que datam de um período anterior à revolução digital, no entanto, a fim de oferecer proteção à liberdade do computador, basearam-se na interpretação evolucionária das regras existentes: significativo a este respeito é a Suprema Corte dos EUA de 1997, Reno v. American Civil Liberties Union (ALCU) , que identifica o acesso à Internet como um pré-requisito para a liberdade de comunicação e expressão; a sentença n.12790 de 30 de julho de 2010 da Sala Constitucional de la Corte Suprema de Justicia da Costa Rica, que recorda expressamente a decisão francesa e reconhece o acesso à Internet como um direito fundamental e a Internet como uma ferramenta necessária e primária para facilitar o exercício de direitos fundamentais relativos à esfera pública e privada.

A realidade global da rede implica uma mudança nos limites geográficos da regulação e torna necessário chegar a soluções compartilhadas a nível supranacional. O vasto supranacional é necessário para garantir a eficácia das normas, evitando a tensão entre a dimensão global das questões e a dimensão territorial das disposições a aplicar.

A aprovação de tal ato não significa minar a soberania do Estado, uma vez que a regulação permaneceria confiada a sistemas supranacionais e sistemas jurídicos individuais e a regulação das relações individuais, além disso, ficaria para a autonomia de negociação.

A proteção jurídica deve inovar em profundidade os mecanismos de proteção para torná-los eficazes no contexto de referência alterado e deve ser capaz de trazer o equilíbrio entre os interesses de volta ao direito, ou seja, às regras ontologicamente apontadas para fazê-lo, garantindo o funcionamento democrático da sociedade contemporanea.

O desafio consiste em ser capaz de garantir uma proteção jurídica capaz de enfrentar a realidade atual, fazendo com que o direito cumpra a sua missão de estabelecer as normas que fundamentam a convivência civil e democrática. Para isso, é necessário um caminho que conduza a sociedade atual a uma constituição global, capaz de traçar bases sólidas e compartilhadas para a proteção dos direitos e das liberdades na era tecnológica. A abordagem deste caminho deve ser multinível e multissetorial, dando vida a novas formas de cooperação e colaboração entre os Estados e valendo-se da participação dos diversos atores e produtores de normas, poderes públicos e privados, de forma a criar princípios e critérios que nós têm força para serem eficazes.

Só um ato com uma gênese como a descrita e que se apresenta com um papel constitucional tem o poder de limitar e direcionar a ação dos Estados e gigantes digitais em relação à pessoa e seus direitos.

É um processo complexo de constitucionalismo digital, necessário para restabelecer o papel da lei e a força dos direitos, colocando a dignidade e a capacidade de afetar a era tecnológica.

NOTAS

Advogada, inscrita nas Ordens do Brasil e de Portugal. Doutoranda em Direito Internacionai e Estudos Europeus e Mestre em Direito Internacional pela Faculdade de Direito da Universidade de

Lisboa. annapinholaw@gmail.com

www.eff.org/cyberspace-indenpendence

O artigo 19 do Pacto Internacional sobre os Direitos Civis e Políticos, adotado pelas Nações Unidas em 19 de dezembro de 1966 e que entrou em vigor em 1976, tem o mesmo sentido.

por exemplo, o acórdão do Tribunal Europeu de Homem dos Direitos Humanos Yldirim v. Turquia, de 18 de dezembro de 2012, processo n.º 3111/10.

SCUS, Reno, Procurador-Geral dos Estados Unidos, et

live!
14/10
13:30h

ETHICAI

Paola Cantarini
Willis S. Guerra Filho
Zilda Gonçalves
Thiago Felipe Avanci

Projeto Ethics AI Lab POIESIS
www.youtube.com/c/ThiagoFelipeAvanci

O CRESCENTE DESAFIO MORAL FRENTE ÀS TECNOLOGIAS: INTERNET, REDES SOCIAIS, IOT, BLOCKCHAIN E INTELIGÊNCIA ARTIFICIAL

PATRICIA G.V. HUELSEN 1
, MARCELO A. VIEIRA GRAGLIA 2
, NOÊMIA LAZZARESCHI 3
1 Pontifical Catholic University of São Paulo Brasil, phuelsen@pucsp.br
2 Pontifical Catholic University of São Paulo Brasil, mgraglia@pucsp.br

Resumo: O estudo avalia cinco tecnologias ou arranjos tecnológicos: internet, redes sociais, internet das coisas, blockchain e inteligência artificial. Estas tecnologias estão em diferentes graus de maturidade e compõem a nova onda de inovação tecnológica, cujos efeitos causarão transformações severas na economia, nas relações de trabalho, no emprego e na sociedade em geral. O objetivo desta pesquisa é realizar uma avaliação básica destas tecnologias em termos de suas características, implicações e impactos sobre as relações humanas e sociais, expandindo a análise para a compreensão das questões éticas e valores humanos envolvidos, com ênfase na realidade brasileira. O método utilizado é de uma pesquisa exploratória, multidisciplinar, que utiliza como referências, entre outras, obras das ciências sociais e da filosofia, base para a ética. O primeiro tópico discorre sobre o desamparo ético em que vivemos na atualidade; segue-se a análise dos contextos das tecnologias e os dilemas morais envolvidos; termina com a avaliação dos valores humanos e virtudes presentes na interação com as tecnologias analisadas.

Palavras-chave: human values, ethics, artificial intelligence, blockchain, internet of things, social networking.

1 Introdução

A questão da ética diante da expansão e uso das novas tecnologias tem provocado um intenso debate, especialmente pelo avanço da Inteligência Artificial. Este debate envolve questões centrais ainda não resolvidas, pois somos uma sociedade construída sob diferenças raciais, de gênero e econômicas. Apesar da imensa contribuição à ética e a moral trazidas por Aristóteles, Platão, pelos iluministas Kant e Hegel, por exemplo, estes pensadores da moral e da ética, conviveram e não se opuseram à sociedade escravocrata, como lembra Freitag (2013). Os algoritmos, cada vez mais presentes no mundo contemporâneo, estão replicando preconceitos a partir do uso de bases de dados impregnadas de vícios humanos. A internet, por sua vez, tem sido um ambiente caracterizado pela liberdade. Entretanto, ainda é um ambiente inseguro e inacessível para muitas pessoas. As redes sociais, um fenômeno marcante neste início de século, traz benefícios interessantes para a sociedade. Por outro lado, é um campo de propagação de mentiras, discursos de ódio e desinformação. As tecnologias de monitoramento aumentam a segurança, mas, por outro lado, contribuem para a falta de privacidade e vigilância exagerada. A interação cada vez maior entre pessoas e tecnologias e sua crescente aplicação por empresas e outras organizações reforça a necessidade de revisitar preceitos éticos e reforçar certos valores morais.

2 Argumentação teórica

O homem pós-moderno tem vivido desamparado pela ética e

convive com uma moral limitada, isto é o que relatam importantes pensadores de nosso tempo, como Morin, Bauman e Lipovetsky. Bauman (2011) entende que os valores éticos se perdem na sociedade fragmentada e que soluções dependem mais que nunca da moral individual. Lipovetsky (2009) demonstra que as fantasias do consumo auxiliaram na busca da felicidade como fim último, deixando o dever para segundo plano. Morin (2005) esclarece que os desafios éticos são grandes, pois a ética individual foi sufocada pelo egocentrismo e a comunitária já não encontra a solidariedade merecida.

Em Cegueira Moral, Bauman (2013) lembra que o mal de nossos tempos não está restrito às ideologias totalitárias, mas se revela ao deixarmos de reagir ao sofrimento de outras pessoas, quando nos recusamos a compreender os outros ou nos mostramos insensíveis a dor alheia. Para ele, uma forma invisível de maldade é quando o poder econômico e político de um país está acima do valor de cada indivíduo, quando os interesses financeiros superam o respeito por cada um. Para o sociólogo, a mentalidade individualista e egocêntrica dos seres humanos é parte de um processo que se deu com a Idade Moderna, na medida em que os homens se

distanciaram das religiões, tornaram-se individualistas. Os processos modernos os forçaram a tomar as rédeas de suas vidas, dissipando seus esforços. O vazio trazido pela distância da religião e a vida moderna não pôde ser preenchido pelas regras impostas pela legislação e pelo Estado (Bauman, 2014).

Morin (2005) confere ao conceito moral uma certa identidade mística, racional e também emocional. O pensador vê que a moralidade depende de um ato de religação com o outro, religação com uma comunidade. Mostra ainda que a moral é de certa forma natural, pois corresponde à natureza do sujeito e da sociedade. A consciência individual é a consciência intelectual e moral. Esta consciência surge do desenvolvimento do que ele chama de relação indivíduo - espécie - sociedade. Entretanto, há um antagonismo nesta relação: a política nem sempre obedece a ética e a economia, por sua vez, considera a ética dos negócios, seguindo os imperativos do lucro, que tende a induzir a exploração de seres humanos. A própria ciência, por vezes, coloca o conhecimento pelo conhecimento, ou à serviço da economia ou da política, levando-o para fins imorais. É o que ocorre com as guerras ou a manipulação genética indevida. Desta forma, as atividades humanas precisam de uma ética profissional. Esta ética profissional deve sempre incluir a perspectiva moral dos seres humanos. A crise ética que Morin (2005) narra é uma crise geral dos fundamentos da certeza, uma crise do próprio conhecimento.

Lipovetsky (2009) entende que a pós-modernidade sofre uma desmoralização, uma época em que a ética está nas trevas. O título da sua obra, sugestivo, que trata desta questão, é Le crepúscule du devoir. Esta designação tem o sentido do dever debilitado, de uma época em que a noção de sacrifício pessoal perdeu sua justificação social, em que a moral não é devota a um fim superior e onde os direitos subjetivos preponderam sobre os mandamentos imperativos. A moralidade, na medida do sacrifício que esta implica, é atropelada pela vontade de uma vida melhor, baseada no consumo e no entretenimento. O responsável por este desmantelo do dever foi a civilização do bem-estar consumista, que não tem mais freios para o desejo. A cultura da felicidade nos distancia da introspecção subjetiva e normalmente desencadeia uma dinâmica geradora de ansiedade, pois está sempre se buscando o futuro feliz, a aparência ideal, nunca se está satisfeito. Lipovetsky relata com metafóricos adjetivos o comportamento típico dos dias atuais onde estamos em busca permanente da felicidade em pequenos termos, mas ela nos parece cada vez mais distante. O paraíso não está mais no outro mundo, está neste aqui e depende do progresso da lei e das condições materiais da existência. A humanidade não aceita sofrer passivamente, mas quer o ideal de felicidade no conforto, nos prazeres. Ele relata que na sociedade do pós-dever o mal é espetáculo atraente, não existem mais heróis, não é preciso ser virtuoso.

3 Metodologia da análise

Foram consideradas neste trabalho as tecnologias ou arranjos tecnológicos que trazem impacto relevante em termos de ganhos de eficiência, redução de custos e melhorias nos processos, benefícios indiretos aos seres humanos, mas, cujo impacto é fortemente percebido em suas vidas: seja por conta da mudança nas forma de trabalho, relacionamentos, estilos de vida, aprendizagem ou contato social. Optou-se por não se considerar as tecnologias diretamente relacionadas à preservação da vida; ou seja, não foram consideradas aqui as tecnologias mais ligadas às áreas médicas e da saúde, tais como: biotecnologia e engenharia genética. O trabalho é exploratório e reúne, entre outras, referências de obras das ciências sociais e da filosofia para apoiar o debate sobre a ética e valores morais. Há um recorte específico, mas não restrito, à realidade brasileira.

4 Tecnologias e seus respectivos requisitos morais

4.1 Internet: o princípio da liberdade e a necessidade de maior segurança

As redes promoveram mudanças nos fluxos sociais e urbanos condicionadas pela fluidez dos fluxos de capital, adicionando novas estruturas e novos serviços. Há pelo menos dois fluxos: o fluxo de circuitos eletrônicos, telecomunicações, sistemas de transportes em alta velocidade e os fluxos que compõem os nós desta rede: centros de comunicação - que têm a função de coordenação na passagem da informação. A expansão e consolidação dos recursos em telecomunicação e em tecnologia não só reduziram as distâncias entre as pessoas, mas também mudaram o seu fluxo, influenciando o processo de globalização e de desenvolvimento local (Castells, 2006).

Com a mudança do fluxo da informação provocada pela Internet, houve também uma quebra na comunicação de massa, cujo fluxo caracterizava-se por possuir sentido único: de um interlocutor para

vários receptores. Com a Internet, o fluxo da comunicação passou a ser multidirecional e isto trouxe protagonismo para novos atores. Muito antes das redes sociais dominarem a Internet, a Internet, como tecnologia em si, foi capaz de colocar os seres humanos no centro do processo comunicacional. As empresas de comunicação passaram a ter

papel de troca dividido com os demais internautas. Muitos criaram seus blogs, sites e passaram a produzir conteúdo e divulgar informações competindo com as empresas de comunicação e criando um novo espaço para a liberdade de expressão. A Internet viabilizou uma mudança estrutural nos meios de comunicação, onde algumas mídias tradicionais foram extintas (como é o caso do CD), outras foram reduzidas significativamente (revistas e jornais impressos) e outras estão sendo ameaçadas, como é o caso da TV aberta, pelas soluções de vídeo online e on demand. As empresas de mídia tradicionais foram para a comunicação online, aberta, livre e gratuita, competindo com a geração de conteúdo de indivíduos comuns e outras empresas entrantes.

Junto com a web surgiu uma série de comportamentos específicos do ciberespaço, tema já estudado por muitos pesquisadores como Santaella (2008), Lemos (2015) e Levy (2010) que levantaram questões como a da privacidade, da segurança, da liberdade desmedida e como a vida foi transformada por completo com a imersão no on-line. Uma das tribos típicas deste universo é a tribo dos hackers. O movimento hacker praticamente surgiu com a Internet e se caracterizou por indivíduos, programadores e adeptos da web livre que criaram comunidades de troca de códigos. A atividade de hackear pode ter propósitos legítimos, como o de buscar falhas dos sistemas e melhorá-los e propósitos ilegítimos, como invadir sistemas e roubar dados para fins ilegais. A maioria das atividades ilegais ocorre na chamada deep web (Graglia, Huelsen, Cacciari, 2018). A deep web, também conhecida como internet invisível, mantém o anonimato de quem a acessa, mas não garante a segurança do usuário. Utiliza-se esta terminologia para se referir a endereços que não são indexados por motores de busca. Há ainda uma subdivisão da deep web, uma parte pequena chamada dark web, que não é indexada e onde são realizadas as transações mais obscuras. Neste ambiente, há um pouco de tudo: informações fechadas acessadas por empresas comuns, bibliotecas, dados confidenciais de governos, acessos a redes de prostituição, venda de drogas, tráfico de pessoas, falsificações, encomendas de assassinatos (WRIGHT, 2017, BECKETT, 2009).

4.2 Redes sociais: aceleração da interação social, a prática da verdade e do respeito

O fenômeno das redes sociais, assim como outros arranjos tecnológicos e suas aplicações, só pôde existir pela existência da Internet. Assim, parte dos valores e dos dilemas morais relatados a seguir também se relacionam com a web. As redes sociais caracterizam-se por ser um espaço de compartilhamento de informações e trocas sociais de forma acelerada e intensa. As comunicações mediadas por computadores (CMC) propiciaram o surgimento de grupos e redes de comunicação específicas, denominadas por Rheingold (1996) de comunidades virtuais. A palavra comunidade traduz confiança e ligação emocional; no entanto, isto parece não acontecer verdadeiramente, como bem avalia Bauman (2004, p. 23): "As relações puras são o presságio, não tanto da mutualidade da libertação, mas de uma mutualidade da insensibilidade". As redes sociais mostram o desafio do respeito e do bom convívio humano, num ambiente de relações intensificadas por milhões de acessos, pautadas por pseudo amizades e por forte exposição de imagens. Um fenômeno recorrente, relatado como a bolha das redes, mostra a formação de grupos de interesses que se fecham em seus próprios preconceitos. Isto se deve pelo uso de sistemas de inteligência artificial, em que algoritmos das plataformas de redes sociais direcionam notícias, produtos e sugestões de amizade de acordo com escolhas anteriores do usuário, deixando os indivíduos restritos em suas bolhas de intenção e de conforto. Bakshy, Messing e Adamic (2015) pesquisaram dez milhões de usuários estadunidenses no Facebook e descobriram que usuários que foram sujeitos a ações de algoritmos que recomendavam notícias direcionadas e que não tiveram acesso a opiniões de outras pessoas com visões diferentes, tiveram maior tendência a não mudar de opinião sobre os temas noticiados do que aqueles que não foram submetidos a estas condições.

Dentre os aspectos negativos, não há só o individualismo exacerbado descrito pelos sociólogos do pós- moderno, mas também o exibicionismo, o voyeurismo, o divertimento desmedido, o trabalho não remunerado, a prática de ilegalidades, as mentiras constantes. As redes sociais são um ambiente para a liberdade, mas também um espaço de máscaras e identidades falsas e um lugar de manipulação de informações. A manipulação parte dos usuários, de hackers, de empresas de dados, de empresas de tecnologia, e mesmo de governos. Se, por um lado, se promovem encontros e protestos a favor da democracia, por outro funcionam como espelho das maldades humanas: redes de pedofilia, grupos extremistas, vendas ilegais; a insegurança existe em toda parte. As redes sociais promovem a liberdade, mas, junto disso, provocam o medo, a falta de privacidade, a insegurança e a propagação de inverdades (Huelsen, 2018, 2019)

Dentre as ações positivas presentes nas redes, destacam-se as trocas de conhecimento, comuns em blogs e comunidades online ou mesmo os grupos de ação colaborativa e solidária que por meio do chamado crowdfunding conseguem arrecadar fundos para financiar projetos. Castells (2006) relatou a solidariedade e o valor da possibilidade de expressar a sinceridade nas redes, mesmo que as pessoas não tenham laços fortes. Outro aspecto é o da mobilização social na transposição de interesses de grupos das redes sociais para as ruas por meio de mobilização social, o que foi chamado por Castells (2013) como "redes de indignação e esperança" e por Negri (2016) de "multitude". O Brasil vivenciou dois grandes momentos de mobilização social pelas redes nos últimos anos. O primeiro momento se deu com os protestos de junho de 2013, que marcaram as

manifestações de cidadãos comuns, muitos mascarados, reivindicando o cancelamento do aumento da tarifa de ônibus, a redução da violência, melhorias das condições de vida, entre outras reivindicações que começaram nas ruas de São Paulo e estenderam-se por todo país. O outro momento foi em maio de 2018 com a paralização dos caminhoneiros que se reuniram por meio de redes sociais (sobretudo WhatsApp) e pararam os transportes do país por dez dias. As consequências foram sérias: desabastecimento de produtos e falta de combustível, além da redução do crescimento econômico naquele ano. Não há dúvida que também fizeram parte destas manifestações grupos organizados, mas a forma de organização foi em grande parte autônoma e espontânea e se deu pelas redes sociais (Lazzareschi, Graglia, Huelsen, 2020).

É inquestionável a importância política e social que estas plataformas sociais adquiriram. Por outro lado, o uso de contas falsas, o uso de algoritmos e robôs que direcionam e propagam mensagens de ódio e fake news, colocam à prova a democracia brasileira. Mais recentemente, o Facebook, Twitter e WhatsApp têm adotado medidas de controle para conter os abusos, como a suspensão de contas, bloqueio de postagens e restrição dos limites permitidos para compartilhamento de mensagens. O fenômeno das fake news no país tem gerado tamanho impacto que há investigações sendo conduzidas pelo Supremo Tribunal Federal, pelo Congresso Nacional, através de uma Comissão Parlamentar Mista de Inquérito, e pelo Tribunal de Contas da União (Graglia, 2020). Há acusações de injúrias a opositores do governo, de formação de redes antidemocráticas que espalham notícias de ódio e desinformação por meio divulgação de dados falsos e sem comprovação científica sobre a pandemia de COVID-19 - confundindo brasileiros quanto à realidade da situação, seus riscos, a eficácia de medicamentos e das medidas sanitárias para combate ao coronavírus. Estas situações mostram que os crimes digitais, assim como as tecnologias, vão mais rápido do que a justiça.

4.3 Internet das Coisas – IoT: oportunidades de controle dos recursos e o medo da vigilância

A Internet das coisas não é em si uma tecnologia única, pois depende de uma série de tecnologias existentes para acontecer. Este arranjo tecnológico prosperou com a chegada da computação em nuvem, do big data e da web analytics, sistemas capazes de coletar muitos dados, avaliá-los estatisticamente e predizer ações futuras (Patel, Patel, 2016). Um grande avanço para o progresso da IoT se deu com o IPv6, versão mais atual do IP. A liberação dos números de controle IP para o mundo é centralizada na Autoridade para Administração de Números Internet (Iana) e, até recentemente, utilizava-se exclusivamente a versão 4 do IP (IPv4), que permite uma combinação de 4,3 bilhões de protocolos. Esta quantidade de endereços IP não seria suficiente para suportar bilhões de objetos com potencial de serem conectados. Com a implantação do IPv6, é possível uma combinação de 3,4x1038 endereços, ou seja, há capacidade suficiente para se criar uma identidade do tipo IP para todo dispositivo ou equipamento existente. Esta nova versão de protocolo ainda vai conviver com a antiga por muitos anos (Oliveira, 2011). A IoT depende, além da necessidade de protocolar cada aparelho com um IP, da existência de uma rede abrangente e eficiente de transmissão de dados, como as já existentes 4G, 5G, GSM, RFID etc., sensores sem fio, assim como sistemas e plataformas de controle e armazenamento de dados, além de sistemas de inteligência capazes de tratar os dados coletados (Patel, Patel, 2016). A Internet das Coisas deve ganhar escala nos próximos anos com o aumento de aparelhos e dispositivos conectados pelo IPv6. As aplicações de IoT envolvem diferentes áreas e setores, como agricultura, transporte e logística, construção civil, varejo, indústria em geral, controle de energia e do meio ambiente.

Para a agricultura de exportação brasileira, o uso de IoT tem muito a contribuir: 70% das grandes propriedades já realizam aplicação de corretivos de solo a taxas variáveis, mas ainda tem muito a realizar com o uso de semeaduras automáticas, monitoramento de colheitas, pilotos automáticos e a aplicação em larga escala de IoT. A chegada deste arranjo tecnológico e das redes ao campo significam melhor aproveitamento de recursos (Teleco, 2020). Mas não é só no campo, a Internet das Coisas torna possível controlar e monitorar cidades inteiras com câmeras, sensores e sistemas inteligentes em diversas aplicações, como em semáforos inteligentes, gerenciamento da energia elétrica, centros de emergência, controle atmosférico, gestão do consumo de água, serviços públicos, entre outras, colaborando para aplicação do conceito de cidades inteligentes ou smart cities.

Os benefícios de segurança e controle trazidos por esta tecnologia são enormes, mas, junto com isto, coloca-se a questão já anunciada por Foucault (1987) da disposição a uma vida vigiada e sujeita a ações punitivas. A vigilância dos cidadãos poderia, por exemplo, excluir bons e maus pagadores, agir a favor do segregacionismo social ou atentar contra os direitos humanos. Estes sistemas devem, ao contrário, garantir o convívio da autonomia e da heteronomia, em uma sociedade de respeito e tolerância. O código moral feito pelo homem moderno, e para ele, preconiza que a liberdade deve ser "cuidada" para que os homens não ajam para o mal. Uma liberdade "vigiada", se não pelo indivíduo, pelo que está fora, pelos agentes da justiça e pensadores que garantam o melhor juízo, que sejam capazes de mostrar que não compensa fazer o mal. A autonomia do indivíduo e a heteronomia da administração racional não poderia estar um sem o outro, mas as suas existências implicam necessariamente em conflitos. Essa é uma contradição aporética, sem superação. O conflito entre o

melhor ajuste do indivíduo e os interesses comuns é um marco da modernidade que tentou buscar soluções, via a universalidade e a fundamentação, mas sem muito sucesso (Bauman, 2013).

4.4 Blockchain: desburocratização, transparência e risco de crescimento da desigualdade

O Blockchain é uma tecnologia do tipo distributed ledger (registro distribuído). Tem como princípio a organização dos registros em blocos (grupos de registros que tem número fixo), um a um em uma cadeia, seguindo uma lógica matemática que os relaciona a um sistema distribuído de base de dados em log e que é gerenciado de forma descentralizada por uma rede P2P (peer to peer) (Formigone Fo, Braga, Leal, 2016?). A tecnologia pode ser aplicada em diferentes tipos de indústria para reduzir burocracias e aumentar o controle, inclusive é usada de forma associada a outras tecnologias e arranjos tecnológicos, como Inteligência Artificial (IA) e Internet das Coisas (IoT). A tecnologia blockchain tem grande potencial para uso no setor público, por exemplo, em aplicações para sistemas de registros de cidadãos (documentos em geral) e controle de benefícios. Também para o setor privado, como em sistemas de transação bancária, gestão da cadeia de fornecimento, logística, varejo entre outras.

No Brasil, a tecnologia blockchain tem sido aplicada sobretudo no sistema financeiro e na indústria de meios de pagamentos, que está em grande transformação. A chegada desta tecnologia permite a transferência direta de valores com muito mais segurança e potencial de redução de intermediários. Os ganhos atuais obtidos por empresas que se beneficiam da alta complexidade e das fronteiras criadas artificialmente entre as redes de pagamento, são impactados pela tecnologia blockchain. Por exemplo, por conta da manutenção unificada de registros nos blocos, os serviços de compensação e liquidação financeira podem se tornar desnecessários por conta da possibilidade da reconciliação de extratos e valores ser totalmente automatizada. Desta forma, partes inteiras dos processos de pagamentos são eliminadas e os elos da cadeia deixam de fazer sentido; já os distribuidores, chamados de adquirentes e subadquirentes, as bandeiras de cartões e o próprio banco também podem deixar de existir (Holotiuk, Pisani, Moormann, 2017). De fato, esta tecnologia, que foi marginalizada por se tratar de uma tecnologia vinculada às criptomoedas (não reconhecida pelos governos) hoje recebe a atenção dos grandes bancos e governos e tem potencialidade de oferecer maior equidade aos players e reduzir custos para os clientes, levando as transações a custarem centavos. Além da redução de custos, um dos maiores benefícios da tecnologia é a segurança contra fraudes, erros e ataques hackers. A reformulação que os bancos e o ecossistema de meios de pagamento irão sofrer é comparada àquela que a indústria de mídia sofreu com a chegada da Internet. Um dos maiores desafios na implantação desta tecnologia será o ganho de escala. O Brasil conta com mais de 45 milhões de indivíduos (cerca de 1/3 da população economicamente ativa com mais de dezesseis anos) que não possuem contas em instituições bancárias, seja por preferir pagamentos com dinheiro vivo, seja por trabalhar na economia informal (Locomotiva, 2019). Os impactos positivos potenciais da aplicação desta tecnologia são claros: menos burocracia, menores tempos de processamento, mais acesso a financiamentos e empréstimos. Um aspecto importante para garantir a segurança no uso de dados e informações sensíveis dos usuários é a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) prevista para o segundo semestre de 2020 (Huelsen et al, 2020).

Os valores morais que aqui serão testados serão a honestidade e a transparência. Há um risco claro de maior vigilância e controle do Estado e das empresas sobre as pessoas. É uma tecnologia que deverá reduzir burocracias, evitar retrabalhos e tirar intermediários, mas dependerá das vantagens oferecidas pelo Banco Central para que o cidadão saia do dinheiro em papel e da informalidade nas trocas, senão sofre-se o risco de criarmos mais barreiras para o indivíduo pobre e aumentarmos as diferenças sociais no país, entre aqueles que são conectados e aqueles que não são. A ética das diferenças já não é mais uma ética desejada para este século. Outro aspecto a ser considerado e que pode agravar o aumento da desigualdade é uma maior destruição de empregos do que criação de novos postos de trabalho, como relatam Graglia e Huelsen (2019).

4.5 Inteligência Artificial, criticidade ao lidar com robôs

A Inteligência Artificial (IA) corresponde a sistemas capazes de interpretar dados externos corretamente, aprender com esses dados e usá-los para alcançar objetivos e tarefas específicas de forma flexível e adaptável. Estes sistemas são classificados por três níveis de maturidade. A IA estreita corresponde a sistemas capazes de ter autonomia para atividades simples e específicas, como, por exemplo, sistemas de reconhecimento de voz e comunição básica. O segundo nível corresponde aos sistemas de IA geral, assim chamados quando os mesmos podem agir em diferentes áreas, como a comunicação por voz, a escrita ou atividades motoras. O terceiro nível diz respeito à super IA, onde as habilidades das máquinas estão muito desenvolvidas e começam a ter consciência própria. Este nível é o mais distante da realidade atual e, provavelmente, não será atingido tão cedo (Kaplan, Haenlein, 2019). Embora o uso de Inteligência Artificial seja amplo e já empregado nas mais diversas áreas, como saúde, inteligência militar, veículos autonômos, recrutamento de pessoas e mesmo avaliação judicial (Livingston, Risse, 2019), no Brasil o uso da tecnologia está ainda em crescimento. Os setores de maior aplicação de IA são o varejo, com os chatbots de atendimento, os bancos, com aplicações de análise de riscos e investimentos e o agronegócio, que utiliza soluções de IA associadas a aplicações de Internet das Coisas, envolvendo desde sistemas inteligentes de irrigação de água até georreferenciamento com uso de drones e processamento de imagens. No setor cultural, há casos de uso de aplicativos de IA que interagem com visitantes de museus da cidade de São Paulo, respondendo perguntas e possibilitando a interação dos visitantes com obras de arte (Graglia, Huelsen, 2019). Na área da educação, as inovações concentram-se sobretudo no campo do processamento de linguagem natural – PNL, em fala e texto e com aprendizagem colaborativa ligada a sistemas de gestão de aprendizagem. Estes sistemas de IA contribuem para uma aprendizagem

mais individualizada e podem ser aplicados sobretudo na aprendizagem ativa e suas implementações, como sala de aula invertida. O uso de IA na educação é promissor e inclui a possibilidade do estudo da ética (Vicari, 2017). É também incontestável a importância do uso da Inteligência Artificial na medicina, especialmente como apoio a diagnósticos e pesquisas clínicas. O país tem utilizado IA para previsão da disseminação de doenças, apoio no diagnóstico, desenvolvimento de novas drogas e vacinas, gestão de leitos hospitalares, detecção de aglomerações humanas e combate às fake news (Tunes, 2020).

A disseminação do uso de sistemas de Inteligência Artificial reaviva o debate sobre a ética, essencialmente em dois aspectos. O primeiro diz respeito a como nós, seres dotados de capacidade moral, devemos lidar com as máquinas, como devemos responder a elas. O segundo tem se mostrado o cerne das discussões atuais: como as máquinas devem agir diante de nós. Isto desconsiderando a polêmica questão da consciência que estas máquinas poderiam adquirir, hipoteticamente, na terceira fase de evolução e então se tornarem moralmente capazes de agir por si.

Quanto ao primeiro aspecto, chama a atenção o fato de muitas pessoas não reconhecerem que estão se comunicando com máquinas ou recebendo mensagens de máquinas, não se questionando se as indicações que estão recebendo fazem sentido ou são coerentes. Harari (2018) menciona o caso de um motorista que caiu em um precipício, pois a indicação do aplicativo de geolocalização, que se utilizava de IA, indicava um caminho que ignorava as interrupções geográficas. Máquinas inteligentes tem escolhido ou induzido as notícias que são lidas pelas pessoas, os produtos que são consumidos, os caminhos e rotas que são seguidos nos deslocamentos diários. Por um lado, a IA facilita o dia a dia; por outro lado, limita as escolhas, induz a erros, direciona pensamentos e serve também como instrumento para manipulação da opinião pública. O que será de um povo onde a liberdade, o livre-arbítrio, o respeito e o estímulo às escolhas são limitados? Carr (2008) já dizia que a Internet estava tornando a sociedade humana mais estúpida, mas a chegada de IA pode intensificar a preguiça de pensar e refletir, quando é necessário exatamente o contrário: pensar ainda mais, refletir ainda mais, para evitar o engano, a manipulação. É preciso rever valores e buscar a melhor maneira de agir diante das inovações tecnológicas e suas implicações.

Quanto ao aspecto das máquinas agirem de acordo com alguma ética, é claro que isto passa pela ação humana, em muitos aspectos. Um deles diz respeito a compreensão de como as máquinas aprendem. Há modelos de aprendizagem de máquina, chamados de machine learning, onde os algoritmos são parametrizados para identificar padrões (comportamentos, imagens etc.) e sugerir tendências ou ações. Por exemplo, a identificação de imagens por robôs na Internet usa estes modelos e quando um indivíduo escolhe as imagens no CAPTCHA1 de um site está ensinando os algoritmos a reconhecerem imagens verdadeiras. Há também a aprendizagem profunda, ou deep learning, onde a aprendizagem ocorre por camadas, numa estrutura similar a das redes neurais do cérebro humano. Massas de dados são usadas para alimentar diretamente o algoritmo de aprendizagem, sendo que os dados de saída de uma camada são os dados de entrada de outra. Este tipo de aprendizagem é usado para reconhecimento de voz, escrita e visão computacional. Há ainda a aprendizagem por reforço, que acontece quando é possível melhorar o desempenho da aprendizagem do algoritimo com base em dados passados, melhoroando-o constantemente (Livingston, Risse, 2019). Mas, independentemente do tipo de aprendizagem de máquina, quando trata-se de IA e valores morais, deve-se analisar a interferência dos humanos, seja nos códigos, no processo de parametrização que ocorre durante as fases de aprendizagem da inteligência artifical, na escolha das bases de dados ou na análise de eventuais vieses. No caso das bases de dados, é sabido que elas normalmente contém os registros históricos de processos e decisões humanas. Assim, capturam o que há de bom e ruim e podem esconder distorções: ações discriminatórias de raça, gênero, condição social, crença religiosa, opção sexual, filiação política e visão de mundo. As empresas de tecnologia e de dados têm buscado formas de tratar a questão ética envolvida no desenvovimento de seus produtos e serviços, incluindo a criação de códigos de ética e comitês de supervisão. Uma das ideias que compõe este debate é o estímulo e definição de políticas de inclusão e diversidade mesmo para áreas de programação e desenvolvimento de sistemas de inteligência artificial. A lógica reside na convicção de que equipes mais heterogêneas e representativas das diferenças existentes na sociedade são capazes de melhorar as reflexões do grupo à procura das escolhas corretas e, assim, garantir uma atuação mais ética para suas equipes e organizações. Entretanto, atualmente, as equipes de desenvolvimento de sistemas de IA são majoritariamente compostas por homens brancos, com formação acadêmica na área de exatas, especializados em tecnologias da informação e comunicação, programação de sistemas e ciência de dados. Outra questão relevante, no estágio atual do desenvolvimento desta tecnologia, e que envolve o uso de algoritmos de aprendizagem mais sofisticados, é que apesar da possibilidade de se controlar os dados de entrada e aferir a assertividade do sistema comparando-os, de alguma forma, com os resultados (dados de saída), os programadores não conseguem explicar facilmente como o sistema consegue aprender. Ou seja, pode-se conhecer as entradas e saídas do sistema, mas não se compreende muito bem como ocorrem os processos de aprendizagem. Este fenômeno é conhecido como caixa preta em IA. Assim, se alguma ação subverter os princípios éticos e morais, esta pode ser descartada, mas não tão facilmente compreendida. A questão aprofunda- se ainda mais

1 CAPTCHA (significa, Completely Automated Public Turing test to tell Computers and Humans Apart") é um teste automatizado para diferenciação entre computadores e humanos, utilizado como ferramenta anti-spam.

com a super IA, com a chamada consciência das máquinas que, segundo Livingston e Risse (2019), poderão ser tornar agentes morais.

De qualquer forma, as medidas de resguardo e proteção parecem estar ficando sob cuidado exclusivo das próprias empresas e das equipes de tecnologia envolvidas no desenvolvimento dos sistemas de IA, que acabam por se tornarem responsáveis por julgar o que é bom ou ruim ou o que é certo ou errado em termos dos resultados e ações das máquinas. Isto traz um grande risco, pois as empresas de tecnologia detém enorme poder econômico atualmente, sendo que as cinco maiores possuem o maior valor de mercado entre todas as empresas dos EUA, como exemplo, o que lhes torna mais relevantes economicamente do que muitos países do mundo. Certamente, também são parte interessada naquilo que se dispõem a controlar, ferindo o princípio da isenção. Os interesses passam a ser de quem tem o capital, as empresas de tecnologia. O debate sobre a questão ética cresce à medida que a própria tecnologia se desenvolve e as possibilidades de aplicação se multiplicam em diversos campos da ação humana. A IBM (Internacional Business Machines) anunciou que deixará de investir mundialmente no mercado de IA para reconhecimento facial. Outras gigantes de tecnologia, a Amazon e a Microsoft, adotaram medidas semelhantes. A questão do uso das imagens e monitoramento social é polêmica no Ocidente e já é debatida frente a questão da privacidade individual. O tema envolve a controvérsia entre aumentar o monitoramento e a segurança e restringir o direito de ir e vir, o direito à privacidade, e do risco destes sistemas serem usados para algum tipo de controle social pelos Estados ou por empresas.

5 Sistema Legislativo Brasileiro, lentidão, esperança nas empresas e nos cidadãos

Se a lei demora a existir, o que esperar de sua aplicação e fiscalização? Este é um dos maiores dilemas do sistema jurídico do país: a combinação entre a falta de marcos regulatórios definidos por legislação específica e a histórica dificuldade de fiscalizar e exigir o cumprimento das leis de uma forma abrangente e equânime. Do ponto de vista regulatório, o país conta somente com o Marco Regulatório da Internet, um documento que estabelece princípios, direitos e deveres para o uso da Internet no Brasil, que estimula a cidadania, educação, cultura e a liberdade de expressão e preza para que a Internet seja de livre acesso a todos os brasileiros (Brasil, 2014). Em agosto de 2020 entrará em vigor a LGPD (Lei Geral de Proteção de Dados), regulamentação bastante similar à Regulamentação Européia de Proteção de Dados criada em 2018. Em termos gerais, esta lei exige das empresas e organizações transparência no uso dos dados, não discriminação, segurança e prevenção de danos frente ao uso dos dados de seus clientes ou usuários (Brasil, 2018). O país discute, também, um projeto de Lei contra as fake News, por força de diversos escândalos envolvendo a propagação de mensagens de ódio e de desinformação em escala industrial, além de ataques contra a reputação de políticos, agentes públicos e instituições da Républica. Teme-se que a ânsia de regular estas práticas nefastas termine por colocar em risco alguns princípios que regeram até aqui o uso da Internet no Brasil, incluindo o direito de expressão e o direito à privacidade. Iniciou-se, também, um texto regulatório para o uso de IA, a partir de uma fase inicial de consulta pública: trata-se do Projeto de Lei 21/20, que estalelece princípios, direitos e deveres e instrumentos de governança e transparência (Câmara dos Deputados, 2020).

Se o Estado não consegue acompanhar a realidade e propiciar parâmetros éticos para o uso adequado destas tecnologias, resta a esperança de que as empresas de tecnologia, por iniciativa própria ou por pressões de clientes, anunciantes e usuários e da própria sociedade civil busquem um posionamento adequado em relação a questão ética. Por outro lado, há a possibilidade de desenvolvimento de sistemas, envolvendo IA e blockchain, que sirvam como mecanismos úteis dentro de processos de controle e validação, o que pode significar a possibilidade de contar com robôs para combater fake News, robôs que nos alertem de condutas inadequadas ou mesmo mecanismos mais rápidos de criação e aplicação de leis para os ambientes digitais (Huelsen, 2019).

6 Conclusões

Este artigo procurou demonstrar a urgência do debate sobre as questões éticas e a necessidade de maior reflexão em relação aos desafios dos valores morais frente às novas tecnologias. Os costumes transpassam as redes e a sociedade convive com dilemas morais diante das aceleradas mudanças trazidas pelas novas

tecnologias. Isto é vivido em todas as instâncias, das individuais às coletivas: indivíduos, grupos de amizade e familiares, organizações, empresas, universidades, escolas e o próprio Estado, que age de forma reativa à inovação, tardando a elaborar e aplicar leis. A pandemia da COVID-19 vem provocando reflexões, mas a sociedade brasileira enfrenta ainda questões do jogo político, como a ameaça trazida pelo uso massivo e mal intencionado de fake News, que choca por evidenciar movimentos de distanciamento da razão e do respeito comum, um recuo frente aos valores relevantes que estão sendo demandados nas interações dos indivíduos com cada uma das tecnologias avaliadas nesta pesquisa (internet, redes sociais, IoT, blockchain e IA): liberdade, respeito, busca da verdade, segurança não vigiada, cuidado na exposição das mazelas humanas, honestidade, espírito crítico. O quadro 1 resume os aspectos humanos em relação às tecnologias e arranjos tecnológicos, seus benefícios, setores impactados, valores esperados das pessoas e virtudes ou valores essenciais para o convívio entre os humanos e as tecnologias analisadas.

Quadro 1: Resumo das tecnologias e valores requeridos

Fonte: Os autores, 2020

Faz-se necessário cuidar para que as relações trazidas por estas tecnologias sejam produtivas, direcionar a atenção para que elas sejam capazes de ensinar, facilitar, permitir melhor aproveitamento

do tempo, otimizar recursos naturais, proteger o meio ambiente, unir as pessoas e potencializar os seres humanos. Se estas tecnologias estão, em parte, sendo usadas em sentido oposto, é sinal de que são necessários ajustes. Não usamos IA para pensar menos. Não queremos monitorar as lavouras com Internet das Coisas para degradar o planeta. Não queremos economizar distâncias através da Web para simplesmente ter uma rotina de trabalho ainda maior. Não queremos eliminar mais e mais postos de trabalho e acelerar o desemprego estrutural no país e o aumento da desigualdade. É preciso evitar o mau uso dos dados, violações ao direito de privacidade, ameaças à estabilidade democrática. Não podemos deixar só a cargo da moral do indivíduo o bem agir diante da tecnologia. Os desafios que estes mecanismos tecnológicos estão instigando dependem de uma efetiva participação do Estado, especialmente os poderes Legislativo e Judiciário, e das empresas de tecnologia.

REFERÊNCIAS

[1] Freitag, Barbara. Antigone itineraries. The question of morality. [M]. Campinas: Papiros, 2002.

[2] Bauman, Zygmunt. Life in fragments. On postmodern ethics. Alexandre Werneck translation [M]. 1. Ed. Rio de Janeiro: Zahar, 2011.

[3] Lipovetsky, Gilles. The post-moralistic society. The twilight of duty and the painless ethics of the new democratic times [M]. São Paulo: Manole, 2009.

[4] Morin, Edgar. The method 6 Ethic [M]. Porto Alegre: Meridional Sulina, 2005.

[5] Bauman, Zygmunt. Postmodern ethics. João Rezende Costa translation. 6. Ed. [M]. São Paulo: Paulus, 2013.

[6] Bauman, Zygmunt. Moral Blindness. In: . DONSKIS, Leonidas.

The loss of sensitivity in liquid modernity. Carlos Alberto Medeiros translation. 1. Ed. Rio de Janeiro: Zahar, 2014, p. 41-46, 52-56, 59-62, 68-88, 118-132,137-144

[7] Castells, Manuel. The network society [M]. São Paulo: Paz e Terra, 2006.

[8] Santaella, Lucia. A ecologia pluralista das mídias locativas. In: Dossiê ABCiber. [J]. Revista Famecos. n. 37, p. 20-24, 2008

[9] Lemos, André. Cyberculture: technology and social life in contemporary culture [M]. 7 ed. Porto Alegre: Sulina, 2015.

[10] Lévy, Pierre. Cyberculture. [M]. São Paulo: Editora 34, 2010.

[11] Graglia, Marcelo, Huelsen, Patricia, Cacciari, Paulo. Hacking attacks and noise generated on networks. In: Santaella, Lucia. (org). Cacofonia nas redes. [M]. p. 157- 181. São Paulo: Educ, 2018.

[12] Wright, Alex. Exploring a 'deep web' that Google can't grasp. In New York Times, 23.09.2009 [J].

[13] Beckett, Andy. The darkside of the internet. In: The Guardian, 2009. [J]

[14] Rheingold, Howard. Virtual Community. [M]. Lisboa: Gradiva, 1996.

[15] Bauman, Zygmunt. Community, the search for security in today's world. Plínio Dentzien translation. [M]. 1. Ed. Rio de Janeiro: Zahar, 2004.

[16] Bakshy, Eytan, Messing, Salomon, Adamic, Lada. Exposure to ideologically diverse news and opinion on Facebook. In Science [J]. 2015, 348 (6239)

[17] Huelsen, Patricia. The code of ethics or the ethics of codes? In: Santaella, Lucia. (org). Artificial Intelligence and Social Netwoks. p. 89-100. [M]. São Paulo: Educ, 2019.

[18] Huelsen, Patricia. Cartographies of morals and ethics for the dilemmas of cyberspace. Doctoral thesis. Programa de Tecnologia da Inteligência e Design Digital (TIDD). [M]. Pontifical Catholic University of São Paulo, 2018

[19] Castells, Manuel. Network of indignation and hope. Social movements in the internet age. [M]. Rio de Janeiro: Zahar, 2013.

[20] Negri, Antonio. Multitude, the democracy of the crowd, 2016. [N]. Viewed in 20 Jul 2019 (in Portuguese)

[21] Lazzareschi, Noêmia, Graglia, Marcelo, Huelsen, Patricia. The forms of resistance of workers in the context of industry 4.0 and artificial intelligence. In : Revista Argumentum (in prelo) [J]. 2020.

[22] Graglia, Marcelo. Fake News: aesthetics and design. 21/06/2020. In: Sociotramas. [J]

[23] Patel, Keyur, Patel, Sunil. M. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application e Future Challenges. In: International Journal of Engineering Science and Computing. [J]. mai, 2016 (6)5

[24] Oliveira, Marcos de. The scientific and technological steps that made the great world wide web. In: Revista Fapesp. [J]. 2011 (2)

[25] Teleco. IoT Statistics. [R]. jul 2020.

[26] Foucault, Michael. Whatch and punish [M]. Petrópolis: Vozes, 1987.

[27] Formigone Filho, José R., Braga, Alexandre M., Leal, Rodrigo. Blockchain, an overview. CNPQ whitepaper. [J].

[28] Holotiuk, Friedrich, Pisani, Francesco, Moorman, Jürgen. The Impact of Blockchain Technology on Business Models in the Payments Industry, in: Proceedings of 13th International Conference on Wirtschaftsinformatik (WI 2017), St. Gallen [J]. 2017: 912-926

[29] Locomotiva, 2019. One in 3 Brazilians, does not have a bank account. In: Institute Locomotiva [R]. 24.09.219.

[30] Huelsen et al. Blockchain: impacts on payment methods and their disruptive potential. In: Santaella, Lucia. (org). Blockchain Expansions in Society [M]. p.? (in prelo). São Paulo: Educ, 2018.

[31] Graglia, Marcelo, Huelsen, Patricia. The sixth wave of innovation: artificial intelligence and the impact on work. In Risus [J]. 2020 11 (1): 3-17.

[32] Kaplan, Andreas, Haenlein, Michael Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence, In: Elsevier Business

Horizons [J] 2019 (62): 15—25

[33] Livingston, Steven, Risse, Mathias. The Future Impact of Artificial Intelligence on Humans and Human Rights. In: Ethics and International Affairs. [J], 2019 (33)2:141-158

[34] Graglia, Marcelo, Huelsen, Patricia. New technologies and the use of Artificial Intelligence in museums: attractiveness, registration, preservation and dissemination of memory. In: Tictions of cities. 1ed.Rio de Janeiro: Gramma Editora (in prelo), 2020.

[35] Vicari, Rosa Maria. AI Trends in Education - 2017-2013. In: CNI (Confederação Nacional da Indústria) [R]. 2018.

[36] Tunes, Suzel. Artificial intelligence against Covid-19. In: Revista Fapesp. 14/04/2020. [J].

[37] Harari, Yuval Noah. 21 lessons for the century. [M] São Paulo: Companhia das Letras, 2018.

[38] Carr, Nicholas. Is google making us stupid? In: The Atlantic. [J] jul-aug, 2008.

[39] Brasil. Lei n. 12965 de 23 de abril de 2014. [L].

[40] Brasil. Lei n. 13.709, 14 de agosto de 2018. [L].

[41] Chamber of Deputies, Brasil, 2020.