

**BIG DATA, PROTEÇÃO DE DADOS E TRANSPARÊNCIA: DESAFIOS PARA A
CONSOLIDAÇÃO DA CONFIANÇA E GARANTIA DOS DIREITOS DO
CIDADÃO***

*BIG DATA AND DATA PROTECTION AND TRANSPARENCY: THE CHALLENGE OF
BUILDING TRUST AND GUARANTEEING CITIZENS' RIGHTS*

Juliano Napoleão de Barros¹

Resumo: A coleta e correlação de dados tornam possíveis descobertas e predições não intuitivas sobre o mundo e, especialmente, sobre a sociedade. O processo decisório decorrente das correlações de dados não é transparente. De tal opacidade, emergem dúvidas razoáveis sobre a correção e justiça das decisões tomadas pelas máquinas. Este artigo tem como objetivo investigar os desafios para consolidação da confiança e a garantia dos direitos do cidadão no contexto do Big Data, com destaque para a exigência de maior transparência. A pesquisa se insere na vertente jurídico-sociológica, sendo investigação de tipo jurídico interpretativo, com a adoção de técnica bibliográfica e do procedimento de análise de conteúdo. Os resultados da pesquisa apontam para o reconhecimento da imprescindibilidade e insuficiência dos instrumentos normativos que regulamentam o tratamento de dados, haja vista a complexidade das transformações tecnológicas, políticas e sociais experimentadas pelo mundo contemporâneo.

Palavras-chave: Big Data; Inteligência Artificial; Proteção de dados pessoais; Ética de Dados; Lei Geral de Proteção de Dados (LGPD).

Abstract: Data collection and correlation make possible unintuitive discoveries and predictions about the world, and especially about society. The decision process arising from data correlations is not transparent. From such opacity, reasonable doubts arise about the correctness and fairness of the decisions made by the machines. This article aims to investigate the challenge of building trust and guaranteeing citizens' rights in the context of Big Data, as well as analyzing the need for greater transparency. The research, from a legal-sociological perspective, adopted the bibliographic technique and the procedure of content analysis. The research results point to the recognition of the indispensability and insufficiency of the normative instruments that regulate the data treatment in face of the complexity of the technological, political and social transformations experienced by the contemporary world.

Keywords: Big Data; Artificial Intelligence; Data Ethics; Data Protection; Brazil's New General Data Protection Law.

* Texto submetido em 12/12/2019 e aprovado para publicação em 13/08/2020.

¹ Mestre e Doutor em Direito pela UFMG. Professor de Filosofia do Direito, Direitos Humanos e Metodologia da Pesquisa Científica da graduação e da pós-graduação em Direito do UniSALESIANO/Lins. ORCID: <https://orcid.org/0000-0002-0831-2661>.

INTRODUÇÃO

No passado, o valor dos dados era definido pela sua captura e utilização em uma finalidade concreta. Em um futuro cada vez mais presente, com o Big Data, a atribuição de valor aos dados ultrapassa o momento da coleta, sendo definida pela sua utilização para múltiplos propósitos, mediante a combinação de diferentes fontes de dados. Na metáfora proposta por Viktor Mayer-Schönberger e Yann Padova (2016, p. 320), cada conjunto de dados coletados pode ser descrito como uma peça de um quebra-cabeça. Em si, possui valor limitado. Contudo, quando combinada com outras peças para completar uma imagem, torna-se verdadeiramente preciosa.

É que na interação entre diferentes fontes de dados, novos padrões são identificados. Este movimento reconfigura, dramaticamente, os métodos de construção do conhecimento científico. Se, antes, os dados eram utilizados apenas para comprovar ou refutar uma hipótese pré-formulada, agora, da correlação entre os dados, emergem novas hipóteses e novas perspectivas de interpretação da realidade, não mais protagonizadas por seres humanos. Análises protagonizadas por inteligências artificiais com habilidades de aprendizagem autônoma (*machine learning*) podem identificar padrões que jamais seriam encontradas pela observação humana. (MENEZES NETO; MORAIS, 2018, p. 188).

O armazenamento e análise de grande quantidade de dados já é aspecto central do mundo contemporâneo. Embora não haja consenso sobre a exata delimitação conceitual de Big Data, é possível reconhecer como principais atributos deste fenômeno: a velocidade, a variedade e o volume de dados coletados, armazenados e analisados. (CIACCIO; GIORGI, 2016, p. 5). A coleta e correlação de dados tornam possíveis descobertas e previsões não intuitivas sobre o mundo e, especialmente, sobre a sociedade. Pela aplicação de algoritmos complexos à gigantesca quantidade de dados armazenados, são formados padrões capazes de antecipar acontecimentos globais e comportamentos sociais, das mudanças climáticas aos comportamentos de consumidores em determinado segmento de mercado.

O big data pode ser utilizado para ajudar a resolver ou gerenciar problemas mundiais críticos, levar a novos avanços científicos e avanços na saúde humana, fornecer informações e análises em tempo real sobre amplas áreas da vida, conectar os sistemas naturais do planeta para monitoramento e recuperação ambiental, intensificar significativamente o uso e a eficiência de recursos e aprimorar a tomada

de decisões e as operações diárias da sociedade. (GARRETT, 2013, p. 2, tradução nossa).²

Esses resultados são obtidos por meio do constante avanço tecnológico e do decorrente aumento da velocidade de processamento dos veículos de informação, da variedade e do volume de dados disponíveis para análise. Quanto maior a velocidade de processamento, a variedade e o volume de dados, mais complexas e valiosas são as descobertas e as previsões na economia digital.

Não se trata de um arranjo democrático. Embora muitos dados estejam disponíveis em diferentes plataformas, apenas os atores que concentram o domínio da maior velocidade de processamento e, notadamente, da maior variedade e volume de dados, são capazes de desenvolver a capacidade analítica necessária para atribuir efetivo sentido e valor aos dados.

O valor dos dados, enquanto ativos na economia digital, somente pode ser mensurado a partir das ligações estabelecidas entre imensos montantes de informação coletada. O mesmo acontece com o impacto da coleta e análise dos dados nos direitos fundamentais. A privacidade sofre severos ataques. A reunião de dados provenientes de fontes diversas viabiliza formas surpreendentes de definição de perfis e rastreamento de pessoas. Destacam-se, para além, a manipulação do usuário e sua indução ao consumo de produtos, serviços e experiências correlacionados ao perfil que lhe é atribuído e a decorrente violação à liberdade de escolha; a discriminação e arbitrariedade em processos seletivos; a listagem de indivíduos para finalidades distintas; e a mitigação da livre concorrência e da livre iniciativa, tendo em vista as barreiras de entrada impostas às pequenas empresas pelas grandes companhias que possuem acesso às informações advindas da análise de grandes volumes de dados. Se percebidos isoladamente, os dados aparentam ser de pouco valor e inofensivos. Mas a reunião massiva desses elementos intensifica a riqueza e o poder das grandes empresas digitais (ZANATTA, ABRAMOVAY, 2019, pp. 423-431) e as decorrentes ameaças e violações aos direitos fundamentais.

A partir de tal premissa, cogita-se que as normas jurídicas atinentes à regulamentação do tratamento de dados são indispensáveis, embora ainda não se revelem aptas para assegurar, satisfatoriamente, a tutela dos direitos fundamentais no contexto do Big Data, haja vista sua complexidade e opacidade. Frente a esta hipótese, este artigo tem como

² “Big data could be used to help solve or manage critical global problems, lead to new scientific breakthroughs and advances in human health, provide real-time information and analysis on wide areas of life, wire up the planet’s natural systems for monitoring and environmental remediation, greatly improve efficiency and resource use, and enhance the decision-making and daily operations of society”. (GARRETT, 2013, p. 2).

objetivo geral contribuir com as investigações sobre os desafios para consolidação da confiança e a garantia dos direitos do cidadão no contexto do Big Data. Para tanto, assume, como objetivos específicos, a pretensão de reconhecer e difundir a importância da Ética de Dados, em especial dos princípios da confiança e da transparência e investigar os desafios para a tutela dos direitos fundamentais diante das ameaças e violações advindas do tratamento de dados, sob a perspectiva dos instrumentos normativos de proteção de dados pessoais, nominalmente, do Regulamento Geral Sobre a Proteção de Dados (GDPR) (UNIÃO EUROPEIA, 2016) e da Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018).

A pesquisa se insere na vertente jurídico-sociológica, sendo investigação de tipo jurídico interpretativo, com a adoção de técnica bibliográfica e do procedimento de análise de conteúdo. A divulgação dos resultados da pesquisa realizada se divide em quatro seções.

Esta primeira, constituída pela introdução teórico-metodológica, apresenta considerações sobre a temática investigada e as opções e procedimentos metodológicos adotados.

A segunda seção ocupa-se das discussões sobre a Ética de Dados e o anseio por transparência e confiança, a partir do entendimento de que não se pode ignorar a responsabilidade ética própria à atuação de plataformas artificiais que assumem, progressivamente, o protagonismo de processos de tomada de decisão que afetam intensa e amplamente a vida dos seres humanos.

Em seguida, na terceira seção, a edição da lei de proteção de dados brasileira e a influência extracontinental do regulamento europeu são abordadas para fomentar a análise dos desafios à tutela dos direitos fundamentais impactados pelo tratamento de dados.

Finalmente, a quarta seção dedica-se às conclusões disponibilizadas pela investigação. Os resultados da pesquisa apontam para o reconhecimento da imprescindibilidade e insuficiência dos instrumentos normativos que regulamentam o tratamento de dados, haja vista a complexidade das transformações tecnológicas, políticas e sociais experimentadas pelo mundo contemporâneo.

1. ÉTICA DE DADOS E A BUSCA POR TRANSPARÊNCIA E CONFIANÇA

O uso massivo de dados pode ser precursor de práticas abusivas e discriminatórias, com graves consequências para a sociedade em longo prazo. (WACHTER; MITTELSTADT, 2019, p. 82). O processo decisório decorrente das correlações de dados não é transparente.

Os algoritmos utilizados para tanto permanecem muitas vezes em sigilo, inacessíveis para o público, exceto nas raras ocasiões em que informações são vazadas ou delatadas por alguém. (PASQUALE, 2015, p. 4). De tal opacidade, emergem dúvidas razoáveis sobre a correção e justiça das decisões tomadas pelas máquinas, tendo em vista os riscos de configuração de diferentes tipos de danos – morais, econômicos, sociais e até mesmo físicos. (CIACCIO; GIORGI, 2016, p. 11 e 12).

Em um cenário em que as máquinas são programadas para aprender sozinhas (*machine learning*), a tecnologia precisa coexistir com o reconhecimento normativo de princípios e valores fundamentais. (DIGNUM, 2018, p. 1). Quando plataformas artificiais assumem, progressivamente, o protagonismo de processos de tomada de decisão, não se pode ignorar as consequências de seus comportamentos.

Como denunciado por O’neill (2016), o aprendizado de máquinas é vulnerável a pontos cegos e à perspectiva de programação. Seus modelos preditivos podem reproduzir preconceitos e outros padrões deturpados, maquiados pela impressão de uma suposta neutralidade. Em decorrência, é imprescindível o mapeamento dos vieses nas máquinas e a concepção e implementação de mecanismos de *fairness* (promoção da justiça e de tratamento equitativo) e *accountability* (promoção da responsabilização e prestação de contas de quem realiza o tratamento de dados).

Neste intuito, uma ética de dados, calcada nos princípios da transparência e da confiança, é primordial para a compreensão dos desafios existentes e sua resolução justificável. (DONEDA; MENDES; SOUZA, 2018 p. 10). Isso contribuiria para a progressiva superação das contradições que perpassam o desenvolvimento dos sistemas de inteligência artificial e(m) sua interação com a promoção da dignidade humana e da sustentabilidade socioambiental.

O propósito de se consolidar a confiança dos cidadãos nos serviços da sociedade da informação, exige o incremento da transparência quanto ao funcionamento das tecnologias de Big Data. E isso exige a democratização do conhecimento tecnológico. Ainda que parte das tecnologias apenas possa ser utilizada corretamente por *experts* (BACHLECHNER; FORS; SEARS, 2018, p. 12), políticas públicas de inclusão digital e iniciativas sociais de divulgação científica devem promover o acesso ao conhecimento tecnológico pois, no contexto do Big Data, o caráter indispensável desse conhecimento se revela progressivamente na vida pessoal e profissional da população. (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2019, p. 43).

Transparência e *accountability* são, simultaneamente, objetivos necessários e de difícil obtenção. Em termos gerais, a população desconhece o modo pelo qual as informações podem ser aglutinadas e interpretadas. (MENEZES NETO; MORAIS; BEZERRA, 2018, p. 191). Como descreve Frank Pasquale (2015, p.3), os sistemas de dados atuais se assemelham às caixas pretas de trens e aviões: seu funcionamento é misterioso, pode-se observar suas entradas e saídas, mas não se pode dizer como uma deriva a outra.

Daí, os complexos padrões derivados dos dados disponibilizados diariamente pelas pessoas são desconhecidos pelos indivíduos e, provavelmente, ultrapassam as informações que elas originalmente concordariam em ceder. (ZANATTA; ABRAMOVAY, 2019, p. 431). Por conseguinte, a população também ignora a abrangência e intensidade dos riscos relacionados à coleta dos dados.

Os dados disponibilizados permitem que os indivíduos sejam influenciados em suas decisões, emoções e comportamentos em diferentes dimensões de sua vida. (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2019, p. 47-48). Cada pessoa é apresentada a um mundo único, customizado a partir dos dados por ela disponibilizados. (PASQUALE, 2015, p. 60). Isso significa dizer que a pessoa é privada de vários outros mundos, que são ocultados, uma vez que não correspondem ao que os algoritmos pretendem estimular ao sujeito do perfil definido pela correlação dos dados.

Não sem razão, a presença em destaque nos mecanismos de busca como o Google Search, é tão cobiçada pelas empresas. (PASQUALE, 2015, p. 60-61). Nesse contexto, os problemas éticos que envolvem dados pessoais não atingem apenas a privacidade dos indivíduos, mas, de modo mais amplo, a autonomia e poder econômico de pessoas físicas e jurídicas. (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2019, p. 43).

Ocorre que a democratização do conhecimento tecnológico se apresenta como tarefa de difícil realização, haja vista a complexidade das tecnologias, procedimentos e dos discursos que os descrevem. Grande parte da população não compreende plenamente o funcionamento dos aparelhos, programas e aplicativos com os quais interage. Do mesmo modo, persiste a incompreensão diante da especificidade da linguagem técnica pertinente, que se configura como barreira à inclusão dos indivíduos no debate público sobre tecnologia. Ademais, há barreiras tecnológicas. Muitos dispositivos e softwares não são projetados para serem transparentes: as tecnologias de transparência e *accountability*, ainda não estão maduras. (BACHLECHNER; FORNS; SEARS, 2018, p. 8).

Além disso, a democratização do conhecimento tecnológico, bem como a promoção de transparência e confiança, nem sempre se mostram presentes na motivação e no agir das grandes empresas que detêm o controle das tecnologias de informação.

[Serviços de busca] fizeram incursões muito profundas na esfera da influência cultural, econômica e política que antes era dominada por redes de transmissão, estações de rádio e jornais. Mas seu domínio é tão completo e sua tecnologia tão complexa que elas escaparam das pressões por transparência e *accountability* que mantinham a mídia tradicional responsável perante o público. (PASQUALE, 2015, p. 61, tradução nossa)³.

Identificar a responsabilidade ética de tais empresas nas análises de dados promovidas é muitas vezes inviável, pois, a análise de dados se relaciona com o input do algoritmo ou com o método estatístico utilizado, os quais com frequência estão protegidos por sigilo empresarial. (DONEDA; MENDES; SOUZA; ANDRADE, 2018, p. 6). A divulgação dessas informações para indivíduos e autoridades não é benquista pelas companhias, pelo risco de exposição de seus segredos empresariais. Desta maneira, estas possuem poucos motivos para promoverem a transparência. (WACHTER; MITTELSTADT, 2019, p. 11).⁴

Esta é uma das razões pelas quais a intervenção estatal e as inovações legislativas direcionadas à regulamentação da proteção de dados pessoais se revelam indispensáveis para a garantia dos direitos fundamentais frente às rápidas e intensas transformações experimentadas pela sociedade a partir do avanço das tecnologias do Big Data e da inteligência artificial. Estado e sociedade civil devem protagonizar os esforços de promoção da ética de dados, em contraposição aos interesses corporativos que não forem compatíveis com este propósito.

2. A IMPRESCINDIBILIDADE E INSUFICIÊNCIA DA TUTELA DOS DIREITOS FUNDAMENTAIS NO CONTEXTO DO BIG DATA

2.1 A edição da lei de proteção de dados brasileira e a influência extracontinental do regulamento europeu

³ “[...] have made very deep inroads indeed into the sphere of cultural, economic, and political influence that was once dominated by broadcast networks, radio stations, and newspapers. But their dominance is so complete, and their technology so complex, that they have escaped pressures for transparency and accountability that kept traditional media answerable to the public”. (PASQUALE, 2015, p. 61).

⁴ Há ainda outros problemas éticos, como a maior preocupação empresarial com a proteção de seus dados do que com os de seus usuários e a ausência de um treinamento necessário por parte dos desenvolvedores de tecnologia para criptografar dados e garantir a sua segurança. (BACHLECHNER; FORS; SEARS, 2018, p. 10).

Importante marco para a disseminação de leis de proteção da privacidade e de dados pessoais no mundo, o Regulamento Geral Sobre a Proteção de Dados (GDPR) pretende reforçar e unificar a proteção de dados pessoais na União Europeia. O GDPR substituiu, assim, a antiga Diretiva 95/46 CE, de 1995. Aprovado pelo Conselho Europeu em abril de 2016, o regulamento tornou-se executável a partir de 25 de maio de 2018. (UNIÃO EUROPEIA, 2016).

Com a edição do GDPR, as empresas que coletam e tratam dados do público europeu se viram obrigadas a ajustar suas políticas de privacidade. Ademais, a inovação europeia influenciou outras nações, que também editaram normas com a pretensão de assegurar a proteção de dados pessoais.

Exemplo desta influência extracontinental do GDPR foi a edição, no Brasil, da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD). Parte-se da premissa, conforme disposto no Art. 2º da lei, de que a proteção de dados tem, como fundamentos, o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão; a inviolabilidade da intimidade, da honra e da imagem; a inovação e o desenvolvimento econômico e tecnológico; a livre iniciativa, concorrência e a defesa do consumidor; os direitos humanos, a liberdade, a dignidade da pessoa humana e a cidadania. (BRASIL, 2018).

A criação de leis de regulamentação do tratamento de dados pessoais configura-se como um passo decisivo e imprescindível para a garantia de direitos fundamentais em um espaço global influenciado pelo fenômeno do Big Data. Em meio aos avanços tecnológicos constantes, à globalização e à emergência de novos centros de poder não estatais, persistem obstáculos à efetividade de tais regulamentos, especialmente no que concerne à proteção dos direitos fundamentais impactados pelo tratamento de dados.

2.2 Para além da privacidade: desafios à tutela dos direitos fundamentais impactados pelo tratamento de dados

Muitas vezes, os juristas que participam do debate sobre as políticas de regulamentação de dados restringem o seu foco às ameaças ao direito de privacidade e ignoram a indivisibilidade dos direitos fundamentais. Como defendem Menezes Neto, Morais e Bezerra (2018, p. 196) é preciso superar a “ideia de que informações pessoais e

comunicações privadas dizem respeito apenas às violações da privacidade”. Não se pode ignorar as sistemáticas violações à dignidade humana decorrentes do tratamento de dados.

Desta feita, a partir da crítica sociológica de Zygmunt Bauman (2014), o tratamento de dados pode ser percebido como um dos principais mecanismos de difusão da vigilância no mundo contemporâneo, viabilizando a definição de perfis que podem motivar limitações às liberdades individuais, notadamente, no que se refere à mobilidade. Pelo tratamento de dados, é possível dividir as pessoas em categorias distintas, identificar os párias e decidir, por exemplo, quem pode ou não atravessar determinada fronteira. A vigilância ganha no Big Data um significado mais amplo, os dados coletados permitem o monitoramento instantâneo e ininterrupto de indivíduos e organizações em escala global, com maior precisão de rastreamento e visualização. (LOTT; CIANCONI, 2018, p. 120-121).⁵

É preciso ter em mente que políticas de privacidade das empresas de tecnologia costumam privilegiar mais a proteção aos interesses delas mesmas do que aos de seus clientes. Diante da necessidade imediata do serviço, os usuários muitas vezes renunciam seus direitos assinando termos de consentimento cujo conteúdo ignoram ou não conseguem compreender.

Os termos de serviço do site se identificam menos com “políticas de privacidade” e mais com contratos que renunciam aos seus direitos ao proprietário do serviço. Se você os ler com atenção, encontrará uma ampla proteção para as empresas e pouco recurso para o consumidor. As pessoas clicam mecanicamente em "Eu concordo" quando confrontadas com contratos de "termos de serviço", cientes de que não há chance de que eles possam modificar os termos⁶. (PASQUALE, 2015, p. 143-144, tradução nossa).

Assim, exige-se dos cidadãos a reiterada expressão de um falso consentimento, que, na realidade, configura-se como renúncia de direitos fundamentais. Não há escolha: a renúncia é condição para que se viva no mundo contemporâneo: sem ela, não é possível fazer transações financeiras eletrônicas, enviar e-mails, postar em redes sociais, navegar na internet, localizar endereços em aplicativos de geolocalização, dentre outros.

Ademais, a constante presença de decisões protagonizadas por algoritmos na vida cotidiana das pessoas – por exemplo, na seleção de candidatos em um processo seletivo, ou na concepção e implementação de uma política pública – não é acompanhada pela

⁵ Do mesmo modo, dificulta-se a garantia do direito ao esquecimento – pois os dados podem ser armazenados e disponibilizados indefinidamente. (GARRETT, 2013, p. 9).

⁶ “Website terms of service are less “privacy policies” than contracts surrendering your rights to the owner of the service. If you read them carefully, you’ll find capacious protection for companies, and little recourse for the consumer. People mechanically click “I agree” when confronted with “terms of service” agreements, fully aware that there’s no chance they can modify the terms”. (PASQUALE, 2015, p. 143-144).

transparência dos procedimentos que alicerçam a tomada de decisão pelas máquinas. No caso de uma máquina que realiza processos seletivos a partir de uma grande base de dados, por exemplo, não é possível saber se a máquina irá discriminar uma pessoa ou coletivo por conta de suas deduções. (BACHLECHNER; FORNS; SEARS, 2018, p. 8).

A análise algorítmica dos dados coletados pode estabelecer padrões a partir de correlações que não possuem ligação lógica na perspectiva da mente humana. (ALVES, 2018, p. 7-10). Isso dificulta a fundamentação e transparência das decisões tomadas a partir dos dados, indispensáveis, uma vez que as correlações encontradas podem afetar substancialmente a vida das pessoas, ainda que não exista nenhum motivo racionalmente defensável para impor um prejuízo, ou mesmo um benefício a alguém.

Desde concessões de benefícios somente para indivíduos caracterizados como “de interesse comercial”, até a impossibilidade de utilizar meios de transporte aéreo, os seres humanos sofrem, cotidianamente, as consequências de sistemas que coletam e, acima de tudo, categorizam informações com critérios que não passam por qualquer tipo de controle democrático. (NETOMENEZES NETO; MORAIS; BEZERRA, 2018, p. 196).

Essa situação é observada nas denominadas técnicas de *black box* adotadas por agências de crédito. Ainda que reguladas, tais empresas utilizam algoritmos que analisam o perfil de seus clientes, a fim de determinar o risco que o empréstimo impõe para a empresa. As conclusões dos algoritmos decorrem de processos que não podem ser totalmente compreendidos – e, conseqüentemente – contestados ou auditados. (PASQUALE, 2015, p. 25). Como os sistemas de informação estão envoltos em segredos, é difícil fiscalizar ou recorrer dos resultados apurados. Assim, são cotidianamente geradas pontuações de crédito arbitrárias, havendo a possibilidade de grupos historicamente subordinados serem prejudicados. (CITRON; PASQUALE, 2014, p. 5).⁷

Outra incongruência da regulamentação estatal do tratamento de dados é o seu impacto negativo no que diz respeito à livre concorrência e à livre iniciativa. Ao contrário do que se poderia supor, majoritariamente, são as pequenas empresas que se veem obrigadas a se sujeitar às normas regulamentadoras, não as grandes corporações. (BEALES III; MURIS, 2019, p. 41). É que as últimas possuem maiores recursos para pesquisas e condição financeira

⁷ Tanto o GDPR quanto a LGPD asseguram o direito à transparência e à explicação. Este último pode ser compreendido como o direito que cada pessoa possui de receber informações suficientes e inteligíveis sobre a lógica e os critérios utilizados no tratamento de seus dados. (MONTEIRO, 2018, p. 4). Seja no contexto europeu, seja no brasileiro, o direito à explicação encontra restrições, como o respeito ao direito de manutenção dos segredos industriais das empresas responsáveis pelo tratamento de dados.⁷ Vale frisar que, neste ponto, o regulamento europeu é mais restritivo – não inclui, por exemplo, o direito à explicação relativa ao uso de dados anonimizados. (MONTEIRO, 2018, p. 14).

para pagar eventuais multas decorrentes de violações às normas estipuladas. Assim, possuem o privilégio de promover uma análise de custo-benefício: podem decidir se o lucro e seus demais interesses são contemplados pela opção de se cumprir a legislação ou se, ao contrário, o descumprimento das normas e o pagamento das multas aplicáveis se revela mais atrativo. Dessa maneira, indiretamente, os regulamentos de proteção de dados pessoais podem contribuir para a exclusão de pequenas empresas de tecnologia do mercado.

A assimetria de forças no contexto do Big Data é tão intensa que muitas companhias pequenas e start-ups não visam competir com as gigantes digitais. O objetivo de grande parte dessas empresas é serem adquiridas pelas grandes companhias. A tendência dos mercados digitais é a de que maiores entidades tendem a atrair mais capital simplesmente porque são vistas como “grandes demais para falir” e “grandes demais para serem presas”. Assim, há uma dinâmica de intensa e veloz concentração de riquezas e poder. (PASQUALE, 2015, p. 141).

Em suma, com o avanço e generalização da aplicação de tecnologias de Big Data e inteligência artificial, o tratamento de dados demanda rigorosa regulamentação não somente por impactar na privacidade dos indivíduos, mas por configurar-se enquanto ameaça à isonomia e à dignidade. As inovações legislativas correspondem a importante contribuição. Porém, inevitavelmente insuficiente, haja vista a complexidade das transformações tecnológicas, políticas e sociais experimentadas pelo mundo contemporâneo.

3. CONCLUSÃO

Diariamente, são muitos os dados produzidos pelas pessoas nas interações estabelecidas com os diferentes dispositivos e tecnologias. Concomitantemente, é imenso o volume de informações criadas por sistemas de inteligência artificial. A quantidade e variedade de dados armazenados de modo cada vez mais ágil pelas tecnologias de Big Data são gigantescas, e a complexidade dos sistemas evolui rapidamente.

A análise algorítmica dos dados coletados disponibiliza previsões advindas de métodos e correlações incompreensíveis para o ser humano. A aplicação de algoritmos complexos ao enorme volume de dados armazenados, permite a descrição precisa de perfis e até mesmo a antecipação de tendências de consumo, eventos naturais e comportamentos sociais.

Esse é um contexto marcado pelo protagonismo das grandes empresas de tecnologia, que armazenam o maior volume e variedade de dados e possuem maior velocidade de processamento. De modo isolado, os dados não aparentam possuir valor, nem configurar riscos para os cidadãos. Contudo, o controle massivo de dados e das informações provenientes de sua análise por algoritmos intensifica a concentração de capitais e poder pelas grandes companhias digitais e, concomitantemente, inflige severas ameaças e violações aos direitos fundamentais.

Em decorrência de tal concentração de poder, tais empresas disseminam fortes influências nas esferas social, cultural, política e econômica. Pela conjugação da abrangência de seu domínio e da complexidade própria ao funcionamento de seus modelos de negócio, são insuficientes as pressões por transparência e *accountability*.

Em grande parte, persiste o desconhecimento da população sobre o que as máquinas estão realizando e quais são as ameaças e violações a direitos fundamentais daí decorrentes. A exigência de consentimento não é suficiente: mesmo que exista a escolha de se disponibilizar ou não dados pessoais – o que nem sempre ocorre – não há transparência sobre como se dá e quais são as consequências do tratamento de tais dados.

Dito de outro modo, os indivíduos não estão cientes das implicações e dos riscos que emanam do tratamento de dados. O contexto do Big Data é complexo e não intuitivo. Assim, mesmo que as pessoas compreendam que seus dados serão coletados, não há clareza sobre quais são as consequências de suas escolhas. Diante de tal lacuna de informação, pode-se cogitar que o consentimento expresso é viciado.

São necessários, portanto, esforços direcionados à democratização do conhecimento tecnológico, tarefa de difícil realização. As tecnologias são complexas, assim como são os discursos que descrevem seu funcionamento e suas repercussões para a vida pessoal e social. Ademais, tal democratização muitas vezes se revela contrária aos interesses das grandes empresas de tecnologia, o que reforça a imprescindibilidade do fortalecimento de iniciativas da sociedade civil e da intervenção estatal na promoção da transparência e da confiança no contexto do Big Data.

Os direitos fundamentais são indivisíveis e interdependentes, desta feita, as violações decorrentes do tratamento de dados não se limitam ao direito à privacidade. No mundo contemporâneo, intensifica-se o fenômeno da vigilância, a definição de perfis, o rastreamento de pessoas e as possíveis restrições a seus direitos civis e políticos. Além disso, os algoritmos promovem práticas empresariais que manipulam seus usuários, pela indução ao

consumo de produtos, serviços e experiências selecionadas a partir da identificação de um perfil arbitrariamente atribuído a cada pessoa, o que evidentemente restringe a liberdade de escolha. Reitera-se o destaque também às discriminações que podem se dar em processos seletivos conduzidos por inteligências artificiais, bem como a mitigação da livre concorrência e da livre iniciativa decorrentes das barreiras de entrada impostas às pequenas empresas de tecnologia frente à impossibilidade de concorrer com as gigantes do mercado.

A edição do GDPR pela União Europeia e da LGPD pelo Brasil representam importante esforço de superação das assimetrias de poder próprias à era do Big Data. Entretanto, seria ingênuo cogitar da suficiência da regulamentação estatal em um período em que o poder político e econômico das nações se vê ofuscado pela expansão global das grandes corporações.

Considerada a complexidade e velocidade das transformações tecnológicas, políticas e sociais experimentadas no mundo contemporâneo, os instrumentos normativos de regulamentação do tratamento de dados são imprescindíveis e insuficientes. De modo ambivalente, as tecnologias de Big Data e inteligência artificial revelam, juntamente com suas contribuições para o avanço científico e social, ameaças aos direitos fundamentais e à dignidade humana. É necessário, portanto, que o constante aprimoramento da regulação do Big Data e a busca por efetividade da intervenção estatal sejam acompanhados do progressivo engajamento da sociedade civil na exigência de democratização do conhecimento tecnológico e de transparência no tratamento dos dados.

REFERÊNCIAS

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information. **The Aspen Institute**: Congressional Program, Cambridge, Massachusetts, p. 43-48, maio 2019. Disponível em: <https://assets.aspeninstitute.org/content/uploads/2019/06/MIT-Conference-Report.pdf>.

Acesso em: 29 ago. 2019.

ALVES, Paulo M. M. R. O Impacto de Big Data na Atividade de Inteligência. **Revista Brasileira de Inteligência**: ABIN, Brasília, n. 13, dez. 2018. Disponível em: http://www.abin.gov.br/conteudo/uploads/2018/12/RBI-13_artigo-2_O-IMPACTO-DE-BIG-DATA-NA-ATIVIDADE-DE-INTELIG%C3%8ANCIA.pdf. Acesso em: 28 ago. 2019.

BACHLECHNER, Daniel; FORS, Karolina La; SEARS, Alan M. The Role of Privacy-Preserving Technologies in the Age of Big Data. **13th Pre-ICIS Workshop on Information Security and Privacy**, São Francisco, 13 dez. 2018. Disponível em: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=wisp2018>. Acesso em: 30 ago. 2019.

BAUMAN, Zygmunt. **Vigilância líquida**. Rio de Janeiro: Zahar, 2014.

BEALES III, J. Howard; MURIS, Timothy J. Privacy and Consumer Control. **The Aspen Institute**: Congressional Program, Cambridge, Massachusetts, p. 37-42, maio 2019. Disponível em: <https://assets.aspeninstitute.org/content/uploads/2019/06/MIT-Conference-Report.pdf>. Acesso em: 29 ago. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Poder Legislativo, Brasília, DF, 15 ago. 2018. Seção 1, p. 59.

CIACCIO, Agostino Di; GIORGI, Giovanni Maria. Statistics in The Big Data Era. **Rivista Italiana di Economia Demografia e Statistica**, Roma, v. LXX, n. 4, p. 5-23, out./dez. 2016. Disponível em: https://www.researchgate.net/publication/316739091_Statistics_in_the_big_data_era/link/591189cf458515bbcb9172e3/download. Acesso em: 30 ago. 2019.

CITRON, Danielle K.; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. **Washington Law Review**, Washington, DC, v. 89, n. 1, p. 1-33, mar. 2014. Disponível em: https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1611&context=faculty_scholarship. Acesso em: 6 ago. 2020.

DIGNUM, Virginia. Ethics in artificial intelligence: introduction to the special issue. **Springer Science + Business Media B.V**: Ethics and Information Technology, Online, 13 fev. 2018. DOI <https://doi.org/10.1007/s10676-018-9450-z>. Disponível em: <https://link.springer.com/content/pdf/10.1007%2Fs10676-018-9450-z.pdf>. Acesso em: 30 ago. 2019.

DONEDA, Danilo Cesar Maganhoto; MENDES, Laura Schertel; SOUZA, Carlos Affonso Pereira de; ANDRADE, Norberto Nuno Gomes de. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 23, p. 1-17, out./dez. 2018. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8257/pdf>. Acesso em: 27 ago. 2019.

GARRETT, Banning. Big Data Is Changing Your World... More than You Know. **Atlantic Council**: Brent Scowcroft Center on International Security, Washington, DC, p. 1-12, 2013. Disponível em: https://www.atlanticcouncil.org/images/publications/Big_Data_is_Changing_Your_World.pdf. Acesso em: 2 set. 2019.

LOTT, Yuri Monnerat; CIANCONI, Regina de Barros. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da Ciência da Informação no Brasil. **Perspectivas em Ciência da Informação**, Belo Horizonte, ano 2018, v. 23, n. 4, p. 117-132, out./dez. 2018. Disponível em: https://www.researchgate.net/profile/Regina_Cianconi2/publication/330837473_Vigilancia_e_privacidade_no_contexto_do_big_data_e_dados_pessoais_analise_da_producao_da_Ciencia_da_Informacao_no_Brasil/links/5c564f10458515a4c7539780/Vigilancia-e-privacidade-no

contexto-do-big-data-e-dados-pessoais-analise-da-producao-da-Ciencia-da-Informacao-no-Brasil.pdf. Acesso em: 27 ago. 2019.

MAYER-SCHÖNBERGER, Viktor; PADOVA, Yann. Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation. **The Columbia Science & Technology Law Review**, Columbia, Nova York, v. XVII, p. 315-335, Primavera 2016. Disponível em: <http://informationaccountability.org/wp-content/uploads/SchonbergerPadova.pdf>. Acesso em: 30 ago. 2019.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?. **Instituto Igarapé**: Artigo Estratégico 39, Rio de Janeiro, dez. 2018. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protacao-de-Dados-no-Brasil.pdf>. Acesso em: 28 ago. 2019.

MENEZES NETO, Elias Jacob de Menezes; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, n. 3, p. 184-198, dez. 2018. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4840/3636>. Acesso em: 27 ago. 2019.

O'NEILL, Cathy. **Weapons of math destruction**: How Big Data Increases Inequality and Threatens Democracy. NY: Brodway Books, 2016.

PASQUALE, Frank. **The Black Box Society**: The Secret Algorithms That Control Money and Information. Cambridge, Massachusetts: Harvard University Press, 2015. Disponível em: https://doc.lagout.org/science/0_Computer%20Science/2_Algorithms/The%20Black%20Box%20Society_%20The%20Secret%20Algorithms%20that%20Control%20Money%20and%20Information%20%5BPasquale%202015-01-05%5D.pdf. Acesso em: 5 ago. 2020.

WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Rethinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, Nova York, v. 2019, ed. 2, p. 1-130, 2019. Disponível em: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3248829. Acesso em: 2 set. 2019.

ZANATTA, Rafael A. F.; ABRAMOVAY, Ricardo. Dados, vícios e concorrência: repensando o jogo das economias digitais. **Estudos Avançados**, São Paulo, v. 33, n. 96, p. 421-446, ago. 2019. DOI <http://dx.doi.org/10.1590/s0103-4014.2019.3396.0021>. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142019000200421&lng=en&nrm=iso. Acesso em: 27 ago. 2019.