Revista Direito em Debate

Revista do Departamento de Ciências Jurídicas e Sociais da Unijuí
Editora Unijuí – Ano XXXI – n. 57 – jan./jun. 2022 – ISSN 2176-6622 – e12476

DO RECONHECIMENTO DA AUTODETERMINAÇÃO INFORMATIVA COMO DIREITO DA PERSONALIDADE E DO PRINCÍPIO DA SEGURANÇA

http://dx.doi.org/10.21527/2176-6622.2022.57.e12476

Submetido em: 29/6/2021
Aceito em: 22/9/2021

Dirceu Pereira Siqueira

Autor correspondente: Universidade Cesumar (UniCesumar) de Maringá. Av. Guedner, 1.610, Bloco 7 – Térreo – Zona 08. Jardim Aclimação. CEP 87050900 – Maringá/PR, Brasil. http://lattes.cnpq.br/3134794995883683. https://orcid.org/0000-0001-9073-7759. dpsiqueira@uol.com.br

Fausto Santos de Morais

Faculdade Meridional, Escola de Direito. Passo Fundo/RS, Brasil. http://lattes.cnpq.br/2028518764749733. https://orcid.org/0000-0002-4648-2418

Lucimara Plaza Tena

Universidade Cesumar (UniCesumar) de Maringá. Maringá/PR, Brasil. http://lattes.cnpq.br/0452242712842724. https://orcid.org/0000-0002-5448-3808

RESUMO

O objetivo deste artigo é o estudo da autodeterminação informativa e o seu reconhecimento material como direito da personalidade analisado sob o viés do princípio da segurança. O atual desenvolvimento tecnológico traz benefícios à coletividade, contudo se observa que o indivíduo se tornou o produto da Sociedade da Informação, e isso viola o princípio do livre-desenvolvimento da personalidade da pessoa natural, o que justifica a presente investigação. O método utilizado é o hipotético-dedutivo, e a hipótese testada é se o direito à autodeterminação informativa é suficiente para garantir o livre-desenvolvimento da personalidade em um contexto de sociedade instrumentalizada por dados. A metodologia concentra-se na revisão bibliográfica de doutrina, legislação, artigos científicos, consulta a *sites* de órgãos oficiais e notícias publicadas na mídia. Os resultados alcançados mostram que a autodeterminação informativa é um direito que, para concretização, exige elementos que lhe sustentem. A conclusão identifica que o princípio da segurança é um desses baluartes a ponto de se tornar a condição *sine qua non* para a efetivação do direito à autodeterminação informativa. O artigo apresenta sugestões para o fortalecimento dessa rede de apoio.

Palavras-chave: autodeterminação informativa; direitos da personalidade; Lei Geral de Proteção de Dados (LGPD); princípio da complementaridade; princípio da segurança.

RECOGNITION OF INFORMATIVE SELF-DETERMINATION AS THE RIGHT TO PERSONALITY AND THE SECURITY PRINCIPLE

ABSTRACT

The aim of this article is the study of informative self-determination and its material recognition as a right of the personality analyzed under the principle of security. The current technological development brings benefits to the community, however, it is observed that the individual has become the product of the Information Society, and this violates the principle of the free development of the personality of the natural person, which justifies the present investigation. The method used is the hypothetical-deductive, and the tested hypothesis is whether the right to informative self-determination is sufficient to guarantee the free development of the personality in a context of a society instrumented by data; the methodology focuses on the bibliographic review of doctrine, legislation, scientific articles, consultation with official agency websites and news published in the media. The results achieved show that informative self-determination is a right that requires concrete elements to support it. The conclusion identifies that the principle of security is one of these bastions to the point of becoming the sine qua non condition for the realization of the right to informative self-determination. The article presents suggestions for strengthening this support network.

Keywords: informative self-determination; rights of the personality; General Data Protection Law (LGPD); complementarity principle; principle of security.

1 INTRODUÇÃO

O cenário da abordagem deste estudo está inserido no contexto da pandemia da Covid-19. O momento excepcional exigiu que, para a proteção da vida e da saúde, outros direitos, como livre-mercado, liberdade de locomoção e privacidade, fossem relativizados. Populações foram enclausuradas em suas casas. Uma nova forma de educação e trabalho remoto via internet se desenvolveu, e muitas atividades migraram já em definitivo para o ambiente *on-line*. Modelos de negócios que não tinham no seu perfil a inovação ou o potencial para tal, precisaram se adaptar para sobreviver e, infelizmente, muitos não resistiram. O ano de 2020 foi incomum e marcado pelo medo generalizado. Apesar da confiança nas vacinas, o terror em relação à doença persistiu em 2021. O que o futuro reserva para 2022 não é possível imaginar. A esperança é que nenhuma outra variante traga ainda mais dor à sociedade mundial.

Sem dúvida a pandemia acelerou os processos de migração para o Universo Paralelo[1] e o volume[2] de dados em trânsito tornou-se intenso. Não faltaram tentativas de violação de privacidade do Poder Público para com os particulares e ataques *hackers* a entes privados e públicos, o que demonstrou a fragilidade dos sistemas de segurança de todos que circulam pelo mundo virtual. No mundo físico são instaladas fechaduras, cadeados, alarmes e cofres para que documentos se mantenham em segurança. No Universo Paralelo, no entanto, parece que as proteções disponíveis ainda não são suficientes para fazer frente à capacidade de ataques do submundo virtual. É uma nova era cheia de piratas em busca de dados e *bitcoins*: os mocinhos terão muito trabalho pelos próximos anos.

A Lei Geral de Proteção de Dados (LGPD) prevê fundamentos e princípios que a sustentam e direcionam seu eixo de proteção e hermenêutica. Para os fins deste estudo, os autores analisam o fundamento da autodeterminação informativa e o seu reconhecimento material como direito da personalidade em combinação com o princípio da segurança. Em razão da Sociedade da Informação vislumbra-se que o indivíduo é transformado em objeto, isto é, dados, para que informações sejam geradas. Tal conduta viola o princípio do livre-desenvolvimento da personalidade da pessoa natural, o que justifica a presente investigação. O método é o hipotético-dedutivo e a hipótese testada é se o direito à autodeterminação informativa é suficiente para garantir o livre-desenvolvimento da personalidade em um contexto de sociedade instrumentalizada por dados. A metodologia concentra-se na revisão bibliográfica de doutrina, legislação, artigos científicos, consulta a *sites* de órgãos oficiais e notícias publicadas na mídia, conduta escolhida em razão do rápido desenvolvimento tecnológico que exige constante acompanhamento das mudanças no cenário tecnológico.

Os resultados alcançados mostram que a autodeterminação informativa é um direito que, para concretização, exige elementos que o sustentem. A conclusão identifica que o princípio da segurança (presente na LGPD) é um desses baluartes a ponto de se tornar a condição *sine qua non* para a efetivação do direito à autodeterminação informativa, o qual é fundamental para a proteção do desenvolvimento da personalidade do indivíduo. Nesse sentido, o Direito tem papel fundamental de transformação social. Sabe-se que essas ações são difíceis de serem realizadas, seja por razões técnicas ou interesses diversos, mas, apesar disso, os autores sugerem algumas medidas que visam a auxiliar no objetivo mencionado.

O texto está dividido nos seguintes tópicos: 1 Introdução; 2 Autodeterminação informativa: um novo direito da personalidade; 3 Da autodeterminação informativa no contexto da Sociedade da Informação e o princípio da segurança; 3.1 Medidas para a efetivação do direito à autodeterminação informativa; 4 Demais princípios da LGPD que atuam em favor do livre-desenvolvimento da personalidade da pessoa natural; 5 Considerações finais; 6 Referências.

[1] Expressão utilizada pelos autores para mencionar as atividades que ocorrem no ambiente *on-line*.

[2] "1,7 MB de dados são criados a cada segundo por cada pessoa durante 2020; nos últimos dois anos foram criados [...] 90% dos dados mundiais; 2,5 quintilhões de bytes de dados são produzidos por humanos todos os dias; 463 exabytes de dados serão gerados a cada dia por humanos a partir de 2025; até o final de 2020, 44 zetabytes formarão todo o universo digital" (BULAO, 2021).

2 AUTODETERMINAÇÃO INFORMATIVA: UM NOVO DIREITO DA PERSONALIDADE

A autodeterminação informativa está na LGPD (BRASIL, 2018) como um de seus fundamentos. Há, contudo, um movimento jurídico que se tornou proeminente em 2020 com a edição da MP 954/20 (BRASIL, 2020b) e posterior propositura da ADI 6387 (BRASIL, 2020c), que pretendia elevar a autodeterminação informativa à categoria de direito fundamental.

Os direitos da personalidade são ilimitados. Isso significa que o rol elencado no Código Civil, artigos 11 ao 21 (BRASIL, 2002), é apenas exemplificativo. Os autores demonstram, neste artigo, que, embora não haja o reconhecimento formal da autodeterminação informativa como um direito da personalidade, é possível atribuir a ela tal condição, tendo em vista as suas características e a urgente necessidade de proteção jurídica da personalidade humana. Os riscos causados à pessoa podem ser irreversíveis em um ambiente de Sociedade da Informação. O perfil da Sociedade 4.0 acelera as relações humanas e exige rápido movimento e adaptação do capital aos mais diversos nichos de mercado que nascem e desaparecem. O Direito, nessa 4ª Revolução Industrial, precisará adaptar-se aos movimentos da sociedade e do *Universo Paralelo* para continuar entregando justiça.

O reconhecimento da autodeterminação informativa como um direito da personalidade e, quiçá, fundamental, justifica-se pela potência dos prejuízos a serem causados ao ser humano e, ainda, ao seu patrimônio. Cueva (1999)adverte que

> [...] el peligro potencial y real al que nos enfrentamos radica, por una parte, en el volumen de información, a menudo aparentemente irrelevante, que sobre nosotros se maneja. Por la otra, en la posibilidad cierta de obtener – mediante el tratamiento de esos datos – nuevos elementos informativos que nos afectan. En tercer lugar, en que tales procedimientos permiten lograr el conocimiento de aspectos de nuestra vida que, además de personales, merecen ya el calificativo de íntimos. Por último, existe el riesgo de que, a partir de ese cúmulo informativo, se elaboren o construyan perfiles de nuestra personalidad en función de los cuales se tomen decisiones sobre nuestros derechos y expectativas, por ejemplo, a la hora de conseguir una vivienda en alquiler, obtener un crédito bancario o una simple tarjeta de crédito o aspirar a un puesto de trabajo (p. 38).

Não está em jogo apenas, como menciona Cueva (1999), a intimidade do indivíduo, mas a sua própria identidade como pessoa humana, e "[...], la libertad que nos pertenece constitutivamente." (p. 38). Sem a efetividade do direito à autodeterminação informativa será difícil mudar essa realidade. Primeiro, o indivíduo não sabe onde estão armazenados ou como estão sendo usados seus dados (isso já é uma realidade nos dias atuais), em seguida, a vigilância e a manipulação sob seus desejos são intensificadas, e, por fim, sem que tenha consciência ou qualquer controle, sua subjetividade é raptada por essa grande Matrix (THE MATRIX, 1999). De pessoa é transformado em mais valia do capital e, uma vez destituído de humanidade para requerer direitos, é encarcerado nas Guantánamos da modernidade (SANTOS, 2007, p. 76).

É verdade que o referido direito não se realiza facilmente, uma vez que está ligado ao princípio da segurança, que aqui, neste artigo, é entendido como segurança tecnológica para os dados disponibilizados ao controlador e que o mantém sob sua guarda. Ao Direito cabe o papel de vetor de transformação social. Não é possível apenas aguardar que as empresas se organizem a partir de uma autorregulação regulada ou de *compliance*, sob pena de comprometer, inclusive, o movimento da Sociedade 5.0 (OLIVEIRA, 2019)[3] que já está em andamento. É preciso que o Estado normatize as relações e que isso seja compreendido pelas organizações como um dever a ser realizado e não como uma opção para atender aos interesses dos acionistas.

[3] O conceito de Sociedade 5.0, Sociedade da Imaginação ou Sociedade Super-inteligente, nasceu no Japão. "É uma sociedade centrada nos humanos que equilibra o progresso económico [sic] com a resolução de problemas sociais através de um sistema que integra de forma eficaz o ciberespaço e o espaço físico" Gabinete do Governo do Japão. OLIVEIRA, Helena. A Sociedade 5.0 E a co-criação do futuro. 17 jan. 2019. *VER – Valores, Ética e Responsabilidade.* Disponível em: https://www.ver.pt/a-sociedade-5-0-e-a-co-criacao-do-futuro/. Acesso em: 12 nov. 2020.

3 DA AUTODETERMINAÇÃO INFORMATIVA NO CONTEXTO DA SOCIEDADE DA INFORMAÇÃO E O PRINCÍPIO DA SEGURANÇA

O escopo da LGPD, conforme estabelece o artigo 1º (BRASIL, 2018), é proteger os direitos fundamentais de liberdade, privacidade e o livre-desenvolvimento da personalidade da pessoa natural. Para a Lei, *dado pessoal* (artigo 5º, I) são as informações capazes de identificar o indivíduo a quem elas estão relacionadas. Klee e Pereira Neto (2019) explicam que a proteção ao dado pessoal tem por objeto "[...] (1) o direito à intimidade e (2) o direito à identidade pessoal. Enquanto o primeiro importa na autodeterminação informativa, o segundo visa a impedir que a identidade pessoal seja alterada por informações inexatas ou incompletas." (p. 14). Em outros termos, que uma personalidade virtual/imaterial, paralela à real/material, seja criada e se torne mais verdadeira que essa, tanto para ele quanto para terceiros, gerando danos à sua vida em todas as esferas.

A Lei 13.709/18 menciona, no artigo 2º (BRASIL, 2018), que a disciplina da proteção de dados pessoais se estabelece sob sete fundamentos, quais sejam: respeito à privacidade; autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre-iniciativa, a livre-concorrência e a defesa do consumidor; e os direitos humanos, o livre-desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Embora todos os fundamentos sejam relevantes, o presente estudo elegeu para análise o relativo à *autodeterminação informativa,* entendendo que o seu cumprimento depende fortemente da garantia da observância do princípio da segurança.

O direito à autodeterminação informativa prevê que seja possível ao dono dos dados conhecer quais as informações que se têm a seu respeito, retificar dados equivocados, atualizar e cancelar os inadequados. Esse direito enfrenta uma dificuldade para a sua concretização, pois,

1) se os dados estiverem em posse de um único detentor é possível acesso aos mesmos, de início, a partir de mera solicitação ou *habeas data*, se for necessário;
2) os dados podem ter sido coletados de diversas fontes, estruturadas ou não, e um perfil de personalidade construído e inserido em grupos segmentados para a geração de informação para os mais diversos fins, como campanhas publicitárias mercadológicas ou políticas, a exemplo do caso das eleições norte-americanas de 2016, que envolveu a Cambridge Analytica (HU, 2020). O indivíduo é o alvo a ser atingido;
3) os dados pessoais, ou com potencial para formar informações particulares, podem ser *hackeados* e comercializados na *deep web*. Uma vez sob o domínio de terceiros desconhecidos, como localizá-los?

O reconhecimento do direito à autodeterminação informativa, como direito da personalidade, quer evitar que em algum momento o indivíduo não saiba mais quem é: se João ou Maria ou se o reflexo de um avatar do *Universo Paralelo*; que necessite perguntar: "Ei Google, onde estou?", "Ei Google, quem sou eu?" ou "Ei Google, que roupa devo usar?" Por enquanto, ainda não é sabido se existe uma ferramenta semelhante ao "Ei Google...", mas, se nada for feito é provável que o desenvolvimento da personalidade de gerações de humanos esteja comprometido. Pelo Universo Paralelo estão espalhados pedaços dos indivíduos, que, ao serem unidos como em um mosaico (MADRID CONESA, 1984; SIQUEIRA; MORAIS; TENA, 2021), traçam perfis de personalidades que dizem muito de cada um deles e, inevitavelmente, carregam a força para produzirem danos. Esses fractais de dados são insumos que alimentam diversos modelos de negócios que prosperam na opacidade de algoritmos discriminatórios.

Para, todavia, que o direito à autodeterminação informativa seja levado a sério, é imperativo que se observe o princípio da segurança. A LGPD (BRASIL, 2018) faz menção a ele em alguns artigos, os quais abrangem ampla gama de medidas relativas à segurança que se deve dispensar quando se lida com dados pessoais. O artigo 6º, VII, dispõe que a segurança é a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". No que se refere aos sistemas utilizados para o tratamento de dados pessoais, o artigo 49 determina que "[...] devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos" na própria lei e nas demais normas regulamentares.

O artigo 47 menciona: "agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento, obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término." (BRASIL, 2018). A Lei também determina (artigo 46) que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito." (BRASIL, 2018). A exigência da norma (BRASIL, 2018) é que essas medidas indicadas no *caput* sejam "[...] observadas desde a fase de concepção do produto ou do serviço até a sua execução." (§2º, artigo 46). Vale dizer que procedimentos de melhoria contínua a serem usados por aqueles que manuseiam dados pessoais (PESTANA, 2019), incluem o dever de atenção para a adoção de tecnologias de segurança equiparadas e com capacidade de deter tentativas externas de violação a bancos de dados privados ou públicos.

A ideia central desse princípio é manter sempre os dados que estão sendo tratados da pessoa física em ambiente seguro. Por esse motivo, deve-se optar pelo uso de tecnologias de segurança em consonância com os riscos trazidos pelas inovações. Para pessoas jurídicas recomenda-se a adoção de procedimentos de melhoria contínua para garantir a segurança (PESTANA, 2019).

A conclusão extraída dos artigos demonstra que se aqueles que utilizam dados pessoais adotarem o que dispõe a LGPD, certamente não apenas o direito à autodeterminação informativa teria oportunidade de ser efetivado, como outros também gozariam de maior proteção, como o da privacidade. Logo, embora a realização desse novo direito seja complexa, não é impossível.

A autodeterminação informativa possui algumas peculiaridades conexas ao princípio da segurança, observe:

a) por envolver questões tecnológicas, nem sempre aqueles que se utilizam de dados, apesar da boa-fé, têm competência técnica suficiente para lidar com as ameaças que surgem aos seus bancos de dados. O princípio da necessidade (artigo 6º, III) da LGPD limita o tratamento ao mínimo necessário para a finalidade proposta e, em situações de vazamentos, o prejuízo ao proprietário dos danos pode ser menor;

b) decisões técnicas relativas à segurança de dados devem se conectar ao sistema jurídico. O apoio normativo tem o condão de prevenir fatos jurídicos que colocam a autodeterminação informativa em risco;

c) transparência no uso dos dados com informações verdadeiras sobre tempo de guarda, descarte e, principalmente, o sistema de segurança utilizado, com as cautelas devidas para que isso não comprometa a proteção do mesmo ou segredos comerciais ou industriais;

d) ação coordenada da Autoridade Nacional de Proteção de Dados (ANPD) exigindo daqueles que se utilizam de dados responsabilidade técnica e jurídica quanto à segurança no manuseio, guarda e descarte;

e) políticas públicas de educação voltadas à segurança dos dados.

Do mesmo modo, infere-se que o princípio da segurança possui a característica da complementaridade, atributo pertinente aos direitos fundamentais que, "[...] para serem efetivados, dependem de outros." (FACHIN, 2019, p. 231). Por exemplo, "o exercício do direito fundamental de participação política pressupõe o direito fundamental de informação. Em outras palavras, a informação é imprescindível para o exercício de direitos políticos." (FACHIN, 2019, p. 231). Da mesma forma, em relação ao direito à autodeterminação informativa que, para ser efetivado, implica o direito à segurança. Nesse sentido, Francisco Balaguer Callejón explica que os direitos fundamentais assim o são "porque se apoiam uns nos outros; não são compartimentos estanques, mas se inter-relacionam mutuamente, de tal forma que o desfrute de um deles pressupõe o desfrute de outro." (1999, p. 37 *apud* FACHIN, 2019, p. 230).

Diante disso, como pensar em autodeterminação informativa se o indivíduo não tem qualquer segurança técnica de onde e com quem estão seus dados? Por outro lado, como garantir o livre-desenvolvimento da personalidade da pessoa natural se uma das consequências da falta de autodeterminação informativa é ter a sua consciência violada e não saber nem de onde veio o ataque/manipulação?

Comenta Cueva (1999) que "[...], si la protección de la información personal ante los peligros derivados de su tratamiento automatizado es un bien jurídico valioso por sí mismo, también posee una dimensión instrumental en la medida en que sirve para garantizar otros derechos" (p. 47). Dados perdidos ou hackeados colocam em colapso todo o ecossistema de proteção de dados que está além da LGPD.

Vive-se uma era abarrotada de informações. Se uma bomba estourar do outro lado do mundo, em segundos, com poucos *clicks*, sabe-se tudo o que aconteceu no local. No que se refere aos dados pessoais, da mesma forma: nossas informações estão espalhadas literalmente por todo o globo terrestre em *data centers*. É verdade que cada indivíduo é responsável por muitos dos dados que estão "soltos" no Universo Paralelo, não apenas porque aceitam compartilhá-los em troca de acessos às plataformas, mas porque, ao se comportarem como se objetos fossem, compartilham a si mesmos a partir das fotos no *Facebook*, *Instagram*, *Twitter*, aplicativos de relacionamento... normalmente sempre com acesso público liberado para aumentar o número de seguidores e curtidas. Boa parte da população coloca-se na rede como produto a ser degustado: se faz o marketing pessoal, pois, afinal, "quem não é visto não é lembrado", já dizia o ditado. A pergunta é: Quem lembrará de você ou quem você quer que se lembre de você? Talvez, porém, o que não se pergunte é: O que farão com essa recordação?

Ocorre que a busca em excesso da visibilidade cobra o seu preço, principalmente dos indivíduos pertencentes aos grupos vulneráveis. Cathy O'Neil, autora do livro "Armas de Destruição Matemática" (2016)[4], comenta que empresas criam algoritmos e, a partir dessa imensidão de dados captados, selecionam suas vítimas: conceder ou não crédito; ofertas de ensino duvidosas; vagas de emprego em condições abusivas direcionadas àqueles que não se encontram em condições de recusar. Esses são apenas alguns exemplos dos danos que o acesso irrestrito aos dados pessoais pode causar e que justifica a necessidade da criação de mecanismos para que o proprietário dos mesmos "[...] mantenga o recupere el poder de disposición y control sobre ellos." (CUEVA, 1999, p. 38).

Uma eficiência de 100% de controle sobre seus próprios dados, porém, jamais o indivíduo terá. É melhor aceitar tal verdade e agir a partir dela com políticas de prevenção, minimização dos riscos e consequências, bem como responsabilidades. Se os dados valem mais que ouro e são o novo petróleo (REGULATING..., 2017) ou o urânio da atualidade, nenhum modelo de negócio que os têm como insumos deles abrirão mão. Dessa forma, a regulamentação envolvendo a autodeterminação informativa deve considerar as especificidades relativas a esse direito, que, acoplado ao princípio da segurança, exige uma resposta tecnológica para sua elaboração.

3.1 Medidas para a efetivação do direito à autodeterminação informativa

Sem a pretensão de esgotar o tema, mas apenas como mera contribuição científica, o presente estudo detectou três medidas que contribuem para a realização do direito à autodeterminação informativa. Evidencia-se que o princípio da segurança está enraizado no conceito do referido direito, sendo elemento essencial a ser considerado quando da elaboração de estratégicas para alcançar a autodeterminação informativa. O tópico seguinte do estudo (4) apresentará os princípios da LGPD, mas com enfoque distinto do presente item. Seguem as medidas identificadas.

a) Políticas públicas de educação do uso consciente e responsável da (na) rede: cultura de proteção de dados

Neste tópico requer-se que sejam desenvolvidas políticas públicas educativas que conscientizem a população sobre o uso responsável da (na) internet e sobre as consequências do compartilhamento indiscriminado de dados e dos riscos que causam à vida do indivíduo em segmentos como: econômico, político, financeiro, educacional e acesso ao mercado de trabalho. Políticas públicas voltadas à proteção do meio ambiente, por exemplo, atingem todas as faixas etárias e prioritariamente as crianças. Visão semelhante

[4] 1) os autores utilizaram nas pesquisas a obra de Cathy O'Neill na versão em espanhol, a qual está inserida nas referências; 2) a autora se refere aos algoritmos como "armas de destruição matemáticas" (ADM). Para o presente estudo, optou-se pela utilização da sigla em inglês escolhida pela autora na versão original, qual seja, WMD (Weapons of Math Destruction); 3) "Algoritmos de Destruição em Massa: Como o Big Data aumenta a desigualdade e ameaça a democracia" - essa foi a tradução do título para o português (Brasil).

poderia ser adotada para o desenvolvimento de uma cultura de proteção de dados, compreendendo que tal ação é um exercício em favor do direito à autodeterminação informativa.

A proposta elaborada nesse tópico do estudo está de acordo com o posicionamento da Autoridade Nacional de Proteção de Dados (ANPD). Em 27 de janeiro de 2021, a ANPD publicou a Portaria 11, que descreve a Agenda Regulatória para o biênio 2021-2022, que "[...] é um instrumento de planejamento que agrega as ações regulatórias consideradas prioritárias e que serão objeto de estudo ou tratamento pela Autoridade durante sua vigência." (BRASIL, 2021).

A ANPD dispõe de autonomia técnica e decisória (artigo 55-B, LGPD) para fiscalizar e elaborar diretrizes e normas relacionadas à proteção de dados dos brasileiros (artigo 55-J e incisos, LGPD). Logo, espera-se que a ANPD crie políticas efetivas de privacidade e autodeterminação informativa, a fim de que aqueles que cedem seus dados para pesquisas ou desenvolvimento de ferramentas de Inteligência Artificial (IA) sejam protegidos.

Ainda, Waldemar Gonçalves, diretor-presidente da ANPD, afirma que a Autoridade promoverá "[...] a comunicação com a sociedade para a educação e disseminação de informações, de forma que todos possam entender os requisitos da Lei e os seus direitos individuais, promovendo a conscientização sobre a proteção de dados de indivíduos pelas organizações." (ANPD, 2021). Em outros termos, buscará o desenvolvimento de uma cultura de dados principalmente em relação às empresas que se utilizam deles. Em uma Sociedade da Informação os dados estão além de serem o novo petróleo. Ferramentas de IA, por exemplo, só funcionam se tiverem acesso a muitos dados. A última fase da agenda prevê a elaboração de documento orientando o público sobre as bases e hipóteses legais de aplicação da LGPD sobre temas diversos." (ANPD, 2021). Nesse ponto entra o papel fundamental das empresas que farão as suas propostas de autorregulação para a conformidade com a Lei.

Regras de boas práticas, *compliance* e uma cultura de dados também para empresas, mostram o papel transformador do direito para a realização da autodeterminação informativa, uma vez que acessa ferramentas que não se resumem apenas em "vigiar e punir". A partir do momento em que ambos os lados se preocupam com os dados e as informações que serão geradas a partir deles, dentro daquilo que a LGPD prevê, ter-se-á uma maior proteção ao livre desenvolvimento da personalidade do indivíduo. Estar consciente da importância dos dados implica estar atento à segurança dos mesmos, a fim de que seja possível o uso desse recurso valioso e indispensável à Sociedade da Informação.

b) Exigir do poder público e empresas responsabilidade em relação à segurança dos dados que mantêm nas suas bases

Investimentos em segurança e, por consequência, em privacidade, devem ser realizados e auditados com frequência para avaliação da higidez do programa adotado para tal finalidade. Em 22 de janeiro de 2021 o *Tecnoblog* noticiou um vazamento de dados que expôs o CPF de 220 milhões de brasileiros. Acredita-se que esse conjunto de dados estaria associado a uma base de dados que inclui, por exemplo, foto de rosto, endereço, telefone, *e-mail* e salário (VENTURA, 2021). A pergunta que se faz é: Qual/quais empresa(s) guardam em seus bancos de dados informações como as que vazaram? Medidas judiciais foram adotadas para verificar a origem do vazamento, mas, ainda que se identifique o responsável ou qual a base de dados que foi invadida, a verdade é que não há como reverter essa situação e o prejuízo ao usuário está instalado. O *site* do Serasa, por exemplo, descreve algumas sugestões de medidas que podem ser adotadas e que visam a diminuir os danos (SERASA, 2021).

É fundamental que a iniciativa privada e o poder público invistam na segurança dos dados que estão sob a sua tutela. Nesse sentido, é imprescindível que o Sistema Jurídico se abra ao Sistema Tecnológico e seja enriquecido por ele. A proteção efetiva à personalidade humana e à sua dignidade depende de investimentos robustos em tecnologia conectados ao Direito.

c) Auditoria nos algoritmos utilizados pelas iniciativa privada e poder público

O algoritmo, que tem por objetivo "solucionar problemas e auxiliar na tomada de decisões" (MENDES; MATTIUZZO, 2019, p. 40), é descrito como um conjunto de passos com vistas à resolução de um problema ou "uma sequência de etapas para resolver um problema ou realizar uma tarefa de forma automática, quer

ele tenha apenas uma dezena de linhas de programação ou milhões delas empilhadas em uma espécie de pergaminho virtual." (PIERRO, 2018). Para Thomas Cormen, "[...] o algoritmo computacional consiste em uma série de etapas para completar uma tarefa que é descrita de maneira precisa o bastante para que um computador possa realizá-la." (2013, p. 1 *apud* MENDES; MATTIUZZO, 2019, p. 40).

Na atual sociedade, movida por dados, é grande o desenvolvimento e o uso dos mais diversos algoritmos para a formação da informação, a fim de instrumentalizar a tomada da melhor decisão. Algoritmos podem produzir perfis de personalidade que vão desde os mais simples até os mais sofisticados, dependendo do que se quer investigar. No *site* do Serasa, por exemplo, está disponível o *score* do indivíduo, e, com base nele, o crédito pode ser concedido ou recusado. Nesse caso, o cidadão comum tem acesso à referida informação, o que nem sempre ocorre em outras plataformas que se utilizam dos dados pessoais ou com potencial para identificar a pessoa.

4 DEMAIS PRINCÍPIOS DA LGPD QUE ATUAM EM FAVOR DO LIVRE-DESENVOLVIMENTO DA PERSONALIDADE DA PESSOA NATURAL

Desde agosto de 2020 a LGPD está em vigor. Assim, espera-se que tanto o Poder Público quanto a iniciativa privada estejam em estruturação para se adequarem aos princípios previstos no artigo 6º da lei, que, logo no *caput,* determina que as atividades de tratamento de dados pessoais deverão primeiramente observar a boa-fé (BRASIL, 2018). Segue a exposição dos princípios e a análise, com a perspectiva da autodeterminação informativa e da relevância para o livre-desenvolvimento da personalidade da pessoa natural.

Finalidade: o tratamento dos dados deve ter propósitos legítimos, específicos, explícitos e serem informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Um cliente que compartilhou seus dados em uma farmácia, por exemplo, para obter desconto, conforme lhe foi informado, poderá confiar na finalidade informada? Note que se assim for, a princípio o laboratório fabricante do medicamento não poderá utilizar os dados do comprador para uma pesquisa de continuidade de produção do produto, uma vez que as informações foram fornecidas apenas à farmácia com um fim único, qual seja, obter desconto.

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. O controlador não pode se desviar do objetivo proposto, sob pena de descumprir o princípio estabelecido na norma e violar a autodeterminação informativa.

Necessidade: a LGPD limita o tratamento ao mínimo necessário para atingir sua finalidade. Os dados devem ser aqueles pertinentes, proporcionais e não excessivos em relação aos fins do tratamento de dados. Se o consumidor está apenas visitando uma loja, por exemplo, não há motivo para que lhe seja requerido acesso a dados pessoais que podem criar um perfil de sua personalidade.

Livre-acesso: ao titular é garantida a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Se esse princípio efetivamente for obedecido, certamente há forte possibilidade de o direito à autodeterminação informativa avançar em efetividade. Será que depois de anos que uma compra foi realizada a empresa ainda poderá manter arquivado os dados do comprador sob as populares promessas, por exemplo, de descontos futuros.

Qualidade dos dados: a Lei prevê que seja garantido aos titulares exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. As garantias estabelecidas pelo princípio em comunhão com o princípio da segurança favorecem o direito à autodeterminação informativa.

Transparência: a LGPD traz que deve ser garantido aos titulares o acesso a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. Será que o usuário do *Facebook* obteria facilmente a informação sobre quais dos seus dados estão armazenados pela plataforma?

O'Neil (2016) denuncia situações em que os sistemas podem interpretar equivocadamente os dados de uma pessoa e a incluírem em categorias incorretas (p. 118). No Brasil, a LGPD declara que o princípio da transparência deve ser observado a fim de permitir que o titular dos dados tenha acesso fácil à realização do

tratamento e aos respectivos agentes. E quando, porém, o tratamento ocorre à revelia do indivíduo? Ele pode ser excluído do mercado de trabalho, por exemplo, e desconhecer o motivo. Como corrigir tal imprecisão se não se sabe ao menos quais os dados que se têm? O'Neil (2016) comenta que

> No hay retroalimentación alguna que corrija el sistema. Un motor que analiza estadísticas no tiene forma alguna de aprender que acaba de enviar la llamada de un posible y valioso cliente al infierno de los sistemas de respuestas automáticas. Y, lo que es peor, los perdedores del universo no regulado de las calificaciones electrónicas cuentan con escasos recursos para presentar una queja, y aún menos para corregir un error en el sistema. En el reino de las ADM[5], ellos son los daños colaterales. Y puesto que este tenebroso sistema está ubicado en lejanas granjas de servidores, las víctimas casi nunca descubren el error." (p. 118).

Situações como a descrita por O'Neil (2016) ferem não apenas a autodeterminação informativa, mas o livre-desenvolvimento da personalidade, além de causar danos à sociedade, que terá de arcar com o ônus de vidas prejudicadas por sistemas mal calibrados e discriminatórios.

Segurança: menciona o dispositivo que a segurança prevê a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. As eleições brasileiras de 2020 passaram por um momento de tensão em razão do ataque *hacker* investido contra o Tribunal Superior Eleitoral (TSE). De qualquer forma, o presidente do Tribunal, ministro Luís Roberto Barroso (SZAFRAN, 2020), afirmou que as barreiras de segurança não foram rompidas e que, portanto, os resultados das eleições não estariam comprometidos. É certo que após tal ataque a segurança do TSE foi revista.

O *Future of Life Institute* delineou 23 diretrizes (PRINCÍPIOS DE ASILOMAR DE IA, 2017) a serem observadas por pesquisadores, cientistas e legisladores a fim de garantir o uso seguro, ético e benéfico de IA. Esses princípios nasceram de uma conferência em 2017, na Califórnia, quando pesquisadores se reuniram e debateram medidas que pudessem reduzir e controlar os riscos relacionados à IA (NAKAGAWA, 2020).

O princípio da segurança informa que "os sistemas IA devem ser seguros durante toda a sua vida operacional, e de forma verificável sempre que aplicável e viável." (PRINCÍPIOS DE ASILOMAR DE IA, 2017). Nesse contexto atual, de rápidas transformações, uma medida de segurança adotada para um período pode não ser suficiente para o seguinte. O sistema (qualquer que se utilize de dados) precisa estar seguro durante toda a sua vida operacional, assim como quando do momento do descarte de dados ou suspensão da utilização da ferramenta. O uso da IA tem trazido diversos benefícios a toda a humanidade e é importante que assim continue, mesmo porque a tendência é que o desenvolvimento tecnológico avance ainda mais. Sistemas enviesados trazem danos aos envolvidos que resultarão em responsabilidade civil.

Em 2020 o governo norte-americano de Donald Trump envolveu-se em uma polêmica com o *TikTok*. A empresa negou que atenderia às demandas do governo chinês por dados do povo norte-americano, uma vez que "[...] os dados são armazenados em servidores dos EUA e de Singapura, e não na China." (MOTA, 2020). Segundo o *TikTok*, "o armazenamento em nuvem que alugamos em Singapura é protegido por nossa própria criptografia e tecnologia, que é implementada por nossa equipe de segurança liderada pelos EUA." (MOTA, 2020). Outras empresas, a exemplo da *TikTok*, investem maciçamente contra invasores externos, mas as tentativas não cessam e a todo momento há um ou outro escândalo envolvendo dados pessoais.

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. A ANPD tem um papel relevante no sentido de orientar de maneira educativa. A prevenção exigirá das empresas programas de *compliance* com medidas duras de prevenção a riscos gerados pelo uso indevido ou desnecessários de dados em qualquer de suas fases, da captação ao descarte.

Não discriminação: a lei proíbe o tratamento para fins discriminatórios ilícitos ou abusivos, mas como controlar o algoritmo criado para o recrutamento de funcionários? Como garantir que ele é justo? O'Neil (2016), em seu livro, traz diversos exemplos da realidade norte-americana, do poder destruidor do algoritmo utilizado de maneira discriminatória. Para lidar com essa questão é necessário analisar a literatura sobre governança

[5] ADM (Armas de Destruição Matemática) ou WMD (Weapons of Math Destruction), como mencionado pela autora na versão original.

algorítmica. Como esse não é o foco do estudo, importa mencionar alguns princípios elaborados por duas entidades e que podem auxiliar o setor privado e o governo quando necessitarem lidar com algoritmos: A *Fairness, Accountability and Transparency in Machine Learning Organization* (FAT-ML) criou alguns princípios-chave, são eles: responsabilidade (*accountability*), explicabilidade (*explainability*), precisão, auditabilidade e justiça (*fairness*). A *Association for Computing Machinery* (Associação de Máquinas de Computação – ACM) vislumbrou os princípios da conscientização; acesso e reparação; proveniência dos dados; validação e experimentação. (MENDES; MATTIUZZO, 2019, p. 55).

Responsabilização e prestação de contas: a LGPD prevê que o agente demonstre ao titular dos dados que adota medidas eficientes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Os princípios descritos pela LGPD de fato oferecem uma proteção abrangente aos dados pessoais. Se observados pelas empresas e requeridos pelo poder público, certamente se estará diante de uma ampla proteção não apenas à autodeterminação informativa, mas, principalmente, ao livre-desenvolvimento da personalidade da pessoa.

5 CONSIDERAÇÕES FINAIS

O artigo analisou a importância do fundamento da autodeterminação informativa combinado com o princípio da segurança, ambos presentes na LGPD. Esse fundamento esteve em evidência no ano de 2020, principalmente por conta da MP 954/20, com a qual o Executivo pretendia que as teles compartilhassem com o IBGE alguns dos dados dos seus usuários. A MP não foi adiante, mas a ideia discutida na ADI 6387 (BRASIL, 2020c), proposta em razão da MP 954/20 (BRASIL, 2020b), de que a autodeterminação informativa deveria ser reconhecida como um direito fundamental, ganhou fôlego.

Ocorre que a autodeterminação informativa como princípio ou fundamento é um direito de difícil concretização. A atual Sociedade da Informação está tecnologicamente instrumentalizada e as informações circulam globalmente pela rede, a tal ponto que nem sempre é possível saber quem a ela teve acesso. Sendo assim, os autores consideram que a efetivação da autodeterminação informativa está umbilicalmente ligada ao princípio da segurança, também previsto na LGPD. É necessária a utilização de medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados, sua destruição, perdas, alterações, por exemplo, estejam eles onde estiverem.

Tendo em vista que os dados são considerados o novo petróleo da atualidade, é fato que diversas organizações criaram seus modelos de negócios tendo as informações/dados pessoais como insumos. Sendo assim, criar uma arquitetura de IA, por exemplo, que observe o princípio da segurança e que permita a fluidez da autodeterminação informativa, talvez prejudique os interesses dos acionistas, que não poderão utilizar os dados arbitrariamente ou despreocupadamente com relação a eventuais responsabilidades civis, penais ou administrativas. É em situações como a mencionada que se faz tão importante a presença do Estado, como agente transformador da sociedade e garantidor das regras do jogo (SUPIOT, 2007).

Ainda que a autodeterminação informativa por enquanto não tenha sido admitida formalmente como um direito fundamental, nada impede que seja reconhecida materialmente como um direito da personalidade, cujo rol previsto no Código Civil não é taxativo. Em termos de Sociedade 4.0, o crescimento tecnológico é muito rápido. A pandemia da Covid-19 no ano de 2020 acelerou esse desenvolvimento e o Direito ainda está se reestruturando para delinear os novos contornos jurídicos que se farão imprescindíveis.

Quando se trata, porém, do direito à autodeterminação informativa e princípio da segurança, não é admissível aguardar a boa-vontade das empresas para que se autorregulem ou criem programas de *compliance*. O Direito precisa caminhar ao lado do desenvolvimento tecnológico para estabelecer as normas que protegem o ser humano em aspectos tão valiosos como o livre-desenvolvimento da sua personalidade.

O uso indevido dos dados pessoais, sua captação irregular ou o compartilhamento pelo próprio proprietário de maneira irresponsável, normalmente por falta de conhecimento dos riscos envolvidos e dos prejuízos gerados, tem permitido às organizações pouco escrupulosas a criação de perfis de personalidade para manipulação de consciências para fins diversos, como consumo ou política. Tais ações ferem direitos

como o da intimidade, privacidade, liberdade e, principalmente, o livre-desenvolvimento da personalidade. Cathy O'Neil já denunciou como algoritmos são utilizados como armas matemáticas de destruição.

Observa-se, portanto, que ações precisam ser adotadas e os autores sugeriram três medidas em prol da proteção da personalidade humana. Não se trata de invadir o segredo de negócio das organizações ou tentar controlar o Estado, mas garantir que o ser humano continue no seu processo de desenvolvimento físico, intelectual, moral e emocional e não se torne um produto da Sociedade da Informação.

6 REFERÊNCIAS

ANPD. Com atuação da ANPD, Brasil ingressa em novo cenário de proteção de dados. *Gov.br.* Presidência da República. 28 jan. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/com-atuacao-da-anpd-brasil-ingressa-em-novo-cenario-de-protecao-de-dados. Acesso em: 31 jan. 2020.

BULAO, Jacquelyn. How much data is created every day in 2020? *TecJury.* 21 jan. 2021. Disponível em: https://techjury.net/blog/how-much-data-is-created-every-day/#gref. Acesso em: 27 jan. 2021.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. *Revista Direitos Sociais e Políticas Públicas – Unifafibe,* v. 8, n. 2, 2020.

BRASIL. *Lei n. 10.406, de 10 de janeiro de 2002.* Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 8 mar. 2020.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 12 nov. 2020.

BRASIL. *Exposição de Motivos da Medida Provisória nº 954, de 17 de abril de 2020.* EM nº 00151/2020 ME. Brasília, 15 de abril de 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Exm/Exm-MP-954-20.pdf. Acesso em: 12 jul. 2020.

BRASIL. *Medida Provisória nº 954, de 17 de abril de 2020.* Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020b. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_ATO2019-2022/2020/MPV/MPV954.HTM. Acesso em: 22 maio 2020.

BRASIL. Supremo Tribunal Federal. *ADI 6387/20 MC-REF/DF.* Conselho Federal da Ordem dos Advogados do Brasil (CFOAB). Rel. Min. Rosa Weber. 2020c. Disponível em: http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5895165. Acesso em: 22 fev. 2021.

BRASIL. Supremo Tribunal Federal. Processo n. 00905660820201000000 – *ADI 6387* – Ação Direta de Inconstitucionalidade. DF. Reqte: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Intimado: Presidência da República. Rel. Min. Rosa Weber. 2020d. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 22 fev. 2021.

BRASIL. *Portaria nº 11, de 27 de janeiro de 2021.* Presidência da República. Autoridade Nacional de Proteção de Dados – ANPD. Publicado em: 28 jan. 2021, ed. 19, seção 1, p.3. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 29 jan. 2021.

CUBIDES-CÁRDENAS, Jaime; NAVAS-CAMARGO, Fernanda; ORTIZ-TORRES, Diana; RICO, Antonio Fajardo. La libertad de expresión en Colombia: parámetros constitucionales y reglas jurisprudenciales. *Revista Direitos Sociais e Políticas Públicas – Unifafibe,* v. 8, n. 2, 2020.

CUEVA, Pablo Lucas Murillo de la. La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos (Nueva Época),* n. 104, abr./jun. 1999. Disponível em: file:///E:/%23%20MINHAS%20INFORMA%C3%87%C3%95ES%20%23/Downloads/Dialnet-LaConstruccionDelDerechoALaAutodeterminacionInform-27560%20(1).pdf. Acesso em: 1º fev. 2020.

FACHIN, Zulmar. *Curso de direito Constitucional.* 8. ed. rev. atual. São Paulo: Editora Verbatim, 2019.

FERMENTÃO, Cleide Aparecida Gomes Rodrigues; FERNANDES, Ana Elisa Silva. A resolução n. 125/2010 do CNJ como política pública de tratamento adequado aos conflitos nas relações familiares: em direção à proteção da dignidade da pessoa humana e a efetivação dos direitos da personalidade. *Revista Direitos Sociais e Políticas Públicas – Unifafibe,* v. 8, n. 2, 2020.

FERNÁNDEZ, Rosa Ana Alija. La necesidad de transversalizar los derechos humanos en las políticas públicas para hacer frente a las crisis: una aproximación desde el derecho internacional de los derechos humanos. *Revista Direitos Sociais e Políticas Públicas – Unifafibe,* v. 8, n. 2, 2020.

HU, Margaret. Cambridge Analytica's Black Box. *Big Data & Society,* July 2020. Disponível em: https://journals.sagepub.com/doi/10.1177/2053951720938091. Acesso em: 7 jan. 2020.

KLEE, Antonia Espíndola Longoni; PEREIRA NETO, Alexandre Nogueira. A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. *Cadernos Adenauer XX*, n. 3, 2019. Proteção de dados pessoais: privacidade versus avanço tecnológico Rio de Janeiro: Fundação Konrad Adenauer, out. 2019. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc=-7bdc8430-12-1f-b21564acd06e?version-1.0&t=1571685012573. Acesso em: 13 nov. 2020.

MADRID CONESA, Fulgenio. *Derecho a la intimidad, informática y Estado de Derecho.* Valencia: Universidad de Valencia, 1984.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público,* v. 16, n. 90, dez. 2019. ISSN 2236-1766. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 5 mar. 2021.

MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. Estudos preliminares sobre os princípios aplicados ao tratamento de dados pessoais na Lei nº 13.709/2018 – LGPD. ENCONTRO NACIONAL DE ENSINO, PESQUISA E EXTENSÃO, ENEPE, 2020. *Anais* [...]. Unoeste, 2020. p. 2.603-2.613. Disponível em: http://www.unoeste.br/Areas/Eventos/Content/documentos/EventosAnais/564/anais/Sociais%20Aplicadas/Direito.pdf#page=190. Acesso em: 8 mar. 2021.

MOTA, Renato. EUA censura documento que detalha riscos do TikTok à privacidade. *Olhar Digital,* 28 set. 2020. Disponível em: https://olhardigital.com.br/2020/09/28/noticias/eua-censura-documento-que-detalha-riscos-do-tiktok-a-privacidade/. Acesso em: 11 out. 2020.

NAKAGAWA. Liliane. Inteligência artificial: quais os riscos que a tecnologia pode gerar? Busca desenfreada por uma "superinteligência" pode tirar o ser humano do topo da cadeia alimentar. *Olhar Digital,* 19 set. 2020. Disponível em: https://olhardigital.com.br/2020/09/09/noticias/inteligencia-artificial-quais-os-riscos-que-a-tecnologia-pode-gerar/. Acesso em: 1º fev. 2021.

OLIVEIRA, Helena. A Sociedade 5.0 E a co-criação do futuro. 17 jan. 2019. *VER – Valores, Ética e Responsabilidade.* Disponível em: https://www.ver.pt/a-sociedade-5-0-e-a-co-criacao-do-futuro/. Acesso em: 12 nov. 2020.

O'NEIL, Cathy. *Armas de destrucción matemática*. Cómo el Big Data aumenta la desigualdad y amenaza la Democracia. Título original: Weapons of Math Destruction: How Big Data increases Inequality and Threatens Democracy. Trad. Violeta Arranz de la Torre. Editor digital: Orhi, 2016. Disponível em: https://ww2.lectulandia.com/book/armas-de-destruccion-matematica/.

PESTANA, Marcio. *Os princípios no tratamento de dados LGPD*. Conjur, 10 de julho de 2019. Disponível em: https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf. Acesso em: 14 ago. de 2020.

PIERRO, Bruno de. O mundo mediado por algoritmos. Sistemas lógicos que sustentam os programas de computador tem impacto crescente no cotidiano. *Revista Pesquisa Fapesp.* 28 maio 2018, ed. 266, abr. 2018. Disponível em: https://revistapesquisa.fapesp.br/o-mundo-mediado-por-algoritmos/. Acesso em: 2 nov. 2020.

PRINCÍPIOS de Asilomar de IA. *Future of Life Institute*. 6 fev. 2017. Disponível em: https://ierfh.org/principios-asilomar-de-ia/. Acesso em: 19 nov. 2020.

REGULATING the internet giants. The world's most valuable resource is no longer oil, but data. *The Economist.* May 5th 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 1 fev. 2020.

SANTINO, Renato. Após negar ataque, TSE tem bancos de dados expostos por hackers em dia de eleição. *Olhar Digital,* 15 nov. 2020. Disponível em: https://olhardigital.com.br/2020/11/15/noticias/apos-negar-ataque-tse-tem-bancos-de-dados-vazado-por-hackers/. Acesso em: 17 nov. 2020.

SANTOS, Boaventura de Sousa. Para além do pensamento abissal – das linhas globais a uma ecologia de saberes. *Novos Estudos 79,* nov. 2007.

SERASA. Meus dados vazaram na Dark Web. E agora? Disponível em: https://ajuda.serasa.com.br/hc/pt-br/articles/360047251951-Meus-dados-vazaram-na-Dark-Web-E-agora-. Acesso em: 1º fev. 2021.

SILVA, Juvêncio Borges; IZÁ, Adriana de Oliveira. A importância da participação popular na elaboração do orçamento e os limites estabelecidos pela lei de responsabilidade fiscal para a administração pública. *Revista Direitos Sociais e Políticas Públicas – Unifafibe,* v. 8, n. 2, 2020.

SIQUEIRA, Dirceu Pereira; LARA, Fernanda Corrêa Pavesi; SOUZA, Bruna Carolina de. Os direitos humanos e a proteção aos seus defensores: análise à luz da salvaguarda dos direitos de personalidade. *Revista Direitos Sociais e Políticas Públicas (Unifafibe),* v. 8, n. 3, p. 159-180, 2020. ISSN 2318-5732.

SIQUEIRA, Dirceu Pereira; ANDRECIOLI, Sabrina Medina. Direitos personalidade das mulheres sob a perspectiva da dignidade da pessoa humana como axioma justificante. *Revista Direitos Humanos e Democracia,* Ijuí: Editora Unijuí, v. 8, n. 15, p. 290-307, 2020.

SIQUEIRA, Dirceu Pereira; ALMEIDA, Fernando Rodrigues de. A impossibilidade de racionalidade dos direitos da personalidade sem um purismo metodológico: uma crítica a partir do debate entre Kelsen e Schmitt. *Revista de Brasileira de Direito (Imed),* v. 16, n. 1, p. 1-27, 2020.

SIQUEIRA, Dirceu Pereira; CASTRO, Lorenna Roberta Barbosa. Minoria feminina e constituições republicanas brasileiras: análise de 1891 a 1988 pela inclusão das mulheres. *Argumenta Journal Law – UENP*, Jacarezinho, v. 33, n. 1, p. 361-382, 2020.

SIQUEIRA, Dirceu Pereira; LARA, Fernanda Corrêa Pavesi. Quarta revolução industrial, inteligência artificial e a proteção do homem no direito brasileiro. *Revista Meritum,* Belo Horizonte: Fumec, v. 15, n. 4, p. 300-311, 2020.

SIQUEIRA, Dirceu Pereira; MORAIS, Fausto Santos de; TENA, Lucimara Plaza. Captação de dados pessoais pelo estado e o direito à privacidade em tempos de pandemia. *Revista Brasileira de Direitos Fundamentais & Justiça,* v. 14, n. 43, p. 407-425, 10 maio 2021.

SHIMABUKURO, Igor. Adoção de criptografia frearia luta contra abuso infantil, alega Facebook. *Olhar Digital,* 22 jan. 2021. Disponível em: https://olhardigital.com.br/2021/01/22/noticias/facebook-adocao-de-criptografia-frearia-luta-contra-exploracao-infantil/?utm_campaign=notificacao&utm_source=notificacao. Disponível em: 26 jan. 2021.

STORINI, Claudia; QUIZHPE-GUALÁN, Fausto César. Hacia otro fundamento de los derechos de la naturaliza. *Revista Direitos Sociais e Políticas Públicas – Unifafibe,* v. 8, n. 2, 2020.

SUPIOT, Alain. *Homo Juridicus:* ensaio sobre a função antropológica do direito. Trad. Maria Ermantina de almeida Prado Galvão. São Paulo: WMF Martins Fonte, 2007.

SZAFRAN, Vinicius. Barroso pede que Polícia Federal investigue ataque ao sistema do TSE. *Olhar Digital,* 17 nov. 2020. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/barroso-pede-que-policia-federal-investigue-ataque-ao-sistema-do-tse/110320. Acesso em: 20 nov. 2020.

THE MATRIX. Direção: Lana Wachowski; Lilly Wachowski. Elenco: Keanu Reeves, Laurence Fishburne, Carrie-Anne Moss. Distribuidor: Warner Bros. 1999. 136 min.

VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava. *Tecnoblog,* 22 jan. 2021. Disponível em: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/. Acesso em: 1º fev. 2020.

VIÑA, Jordi García. Aspectos laborales de empresas complejas en España. *Revista Direitos Sociais e Políticas Públicas – Unifafibe,* v. 8, n. 2, 2020.

ZEIFERT, Anna Paula Bagetti; CENCI, Daniel Rubens; MANCHINI, Alex. A justiça social e a agenda 2030: políticas de desenvolvimento para a construção de sociedades justas e inclusivas. *Revista Direitos Sociais e Políticas Públicas – Unifafibe,* v. 8, n. 2, 2020.