UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Joelma da Silva Machado de França

DADOS PESSOAIS SOB VIGILÂNCIA: REPERCUSSÕES DO CASO CAMBRIDGE ANALYTICA X FACEBOOK

Santa Maria, RS
2021

Joelma da Silva Machado de França

DADOS PESSOAIS SOB VIGILÂNCIA: REPERCUSSÕES DO CASO CAMBRIDGE ANALYTICA X FACEBOOK

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Direito, na área de concentração Direitos Emergentes na Sociedade Global, com ênfase na Linha de Pesquisa Direitos na Sociedade em Rede: atores, fatores e processos na mundialização da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Direito**.

Orientadora: Prof.ª Dr.ª Valéria Ribas do Nascimento

Santa Maria, RS
2021

da Silva Machado de França, Joelma
DADOS PESSOAIS SOB VIGILÂNCIA: REPERCUSSÕES DO CASO CAMBRIDGE ANALYTICA X FACEBOOK / Joelma da Silva Machado de França.- 2021.
121 p.; 30 cm

Orientador: Valéria Ribas do Nascimento
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Ciências Sociais e Humanas, Programa de Pós-Graduação em Direito, RS, 2021

1. Direito à proteção de dados 2. Vigilância 3. Internet das coisas 4. Poder 5. Cambridge Analytica I. Ribas do Nascimento, Valéria II. Título.

Sistema de geração automática de ficha catalográfica da UFSM. Dados fornecidos pelo autor(a). Sob supervisão da Direção da Divisão de Processos Técnicos da Biblioteca Central. Bibliotecária responsável Paula Schoenfeldt Patta CRB 10/1728.

Declaro, JOELMA DA SILVA MACHADO DE FRANçA, para os devidos fins e sob as penas da lei, que a pesquisa constante neste trabalho de conclusão de curso (Dissertação) foi por mim elaborada e que as informações necessárias objeto de consulta em literatura e outras fontes estão devidamente referenciadas. Declaro, ainda, que este trabalho ou parte dele não foi apresentado anteriormente para obtenção de qualquer outro grau acadêmico, estando ciente de que a inveracidade da presente declaração poderá resultar na anulação da titulação pela Universidade, entre outras consequências legais.

Joelma da Silva Machado de França

DADOS PESSOAIS SOB VIGILÂNCIA: REPERCUSSÕES DO CASO CAMBRIDGE ANALYTICA X FACEBOOK

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Direito, na área de concentração Direitos Emergentes na Sociedade Global da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Direito**.

Aprovado em 25 de fevereiro de 2021:

Prof.ª Dr.ª Valéria Ribas do Nascimento (UFSM)
(Orientadora/Presidente)

Prof. Dr. Rafael Santos de Oliveira (UFSM)

Prof.ª Dr.ª Rosângela Angelin (URI)

Santa Maria, RS
2021

AGRADECIMENTOS

A gratidão é um sentimento que não posso deixar de expressar às pessoas que tornaram possíveis não somente a conclusão desse trabalho, mas de um sonho aqui representado, regado há muito tempo. E nesse tempo em que se manifesta essa realização tão significativa, não só para a minha vida, mas para todos aqueles que persistem diante dos obstáculos, eu quero agradecer.

A Jesus Cristo, que mesmo sendo todo poderoso, se revelou a mim, e continua dia após dia a me sustentar. Sem ti, nada posso, em ti, faço proezas.

Ao meu amor eterno, meu esposo Jorge, por ser incansável em expressar seu amor por mim, por compartilhar a vida comigo, pelo apoio e incentivo incondicionais, por acreditar comigo.

Às minhas amadas e maravilhosas filhas, meus tesouros, Cecília e Celena, por me amarem mesmo em face da minha ausência, necessária para vencer essa etapa e avançar para as seguintes. Vocês e o papai são os principais motivos da minha dedicação.

À minha incrível mãe Delma, mulher preciosa, pelo cuidado constante, por não medir esforços para me ajudar, pelo exemplo de vida, por plantar esse sonho em mim.

À minha linda irmã Joceane, minha amiga mais que especial, por me encorajar, por compartilhar suas experiências acadêmicas comigo, por toda a ajuda.

Ao meu pai Joel e aos demais familiares e amigos que torceram por mim.

Às minhas amigas Amanda Prado e Simone Messina, bem como aos casais de amigos Ari e Ieda Dessotti e Ronaldo e Fabia Silva, por se empenharem de forma a tornarem essa trajetória mais leve.

À minha estimada orientadora, Prof.ª Valéria Ribas do Nascimento, pela compreensão, pela paciência, por compartilhar comigo seus conhecimentos, seus livros, sua sala de aula, pelos ensinamentos no desenvolvimento deste trabalho e para a vida profissional.

A todos os docentes do Programa de Pós-Graduação em Direito (PPGD/UFSM), pelos valiosos ensinamentos e por contribuírem significativamente para a ampliação dos meus horizontes acadêmicos.

À Prof.ª Carolina Salbego Lisowski, minha orientadora da Monografia, exemplo de comprometimento profissional na sala de aula, na gestão pública e na gestão privada, por me inspirar a seguir essa carreira, minha sempre mestra por quem teço grande admiração.

As colegas Vanessa Muller e Andreia Momolli, a veterana Célia Albino, aos colegas do extinto grupo de estudos do CNPQ, CCULTIS, Centro de Culturas Jurídicas Comparadas, Internacionalização do Direito e Sistemas de Justiça, então coordenado pela versada Prof.ª Jânia Maria Lopes Saldanha, aos colegas do grupo de estudos do CNPQ, NDC, Núcleo de Direito Constitucional, coordenado pela minha orientadora Prof.ª Valéria Ribas do Nascimento, pelo companheirismo, pelos compartilhamentos, pelo incentivo, pelo suporte.

A todos os colegas do Programa de Pós-Graduação em Direito (PPGD/UFSM), pela ímpar oportunidade de convivência, debates e contribuições durante os dois anos de convívio.

À Universidade Federal de Santa Maria (UFSM), que tanto eu sonhei em integrar, pela grandiosa oportunidade, pela acolhida, pela exemplar atuação no ensino público e gratuito e na luta pelo fortalecimento e preservação do direito à educação.

À Faculdade Palotina (FAPAS), pela formação que me proporcionou, de maneira a me possibilizar sustentação teórica para ingressar no Curso de Especialização em Gestão Pública Municipal da UFSM, onde obtive êxito em adquirir maiores conhecimentos em Direito Público, área que tanto aprecio, bem como para o progresso desse trabalho.

Aos professores Rafael Santos de Oliveira, de quem tive o privilégio de ser aluna, e Rosângela Angelin, pela presteza em terem aceitado o convite para compor a banca de qualificação e defesa e pelas engrandecedoras contribuições ao meu trabalho.

Por fim, a todos os demais que, de alguma forma, contribuíram para que eu viesse a concluir essa trajetória, muito obrigada mesmo.

RESUMO

DADOS PESSOAIS SOB VIGILÂNCIA: REPERCUSSÕES DO CASO CAMBRIDGE ANALYTICA X FACEBOOK

AUTORA: Joelma da Silva Machado de França
ORIENTADORA: Valéria Ribas do Nascimento

Não é mais possível conceber sociedade, política e democracia ignorando os riscos iminentes acerca da extinção do direito à privacidade, nesse tempo, ressignificado no direito à proteção de dados. A expansão da vigilância aplicada no cotidiano dos cidadãos, sobretudo, em face do advento da internet das coisas, obrigou o direito a ter um novo olhar sobre categorias como identidade, personalidade, no que toca a imbricação da esfera digital com a esfera real, onde os dados pessoais atingiram um elevado valor de mercado. Tal realidade é também evidenciada pela nova lei de proteção de dados no Brasil (Lei 13.709/2018). O caso *Cambridge Analytica X Facebook* clarifica acerca das formas como tal negócio informacional opera, onde se pretendeu a manipulação de humanos por meio da operação de algoritmos. Assim, certos atores públicos e privados, agem em afronta à dignidade da pessoa humana, com práticas antidemocráticas que se reinventam em face do aparato tecnológico, sendo que não é possível saber na totalidade de que forma tal poder se manifestará no futuro. O presente trabalho tem como objetivo principal analisar em que medida a vigilância operada pelo aparato tecnológico de alcance global conseguirá ou não exercer algum tipo de controle sobre a sociedade global, tendo por base o caso *Cambridge Analytica* X *Facebook* (2016). A metodologia empregada nesta pesquisa constitui-se pelo método dedutivo. O método de procedimento escolhido para a pesquisa foi o estudo de caso. Relativamente às técnicas de escrita, foi feito uso de resumos e fichamentos. A teoria de base adotada conjuga autores como Zygmunt Bauman, Stefano Rodotà e Bruno Ricardo Bioni em diálogo com outros autores. A imbricação da vigilância com o aparato tecnológico tem viabilizado a construção de um sistema global que opera a manipulação de poucos sobre a multidão de seres humanos.

Palavras-chave: Direito à proteção de dados. Vigilância. Internet das coisas. Poder. Cambridge Analytica.

ABSTRACT

PERSONAL DATA UNDER SURVEILLANCE: REPERCUSSIONS OF THE CASE CAMBRIDGE ANALYTICA X FACEBOOK

AUTHOR: Joelma da Silva Machado de França
ADVISOR: Valéria Ribas do Nascimento

It is no longer possible to conceive society, politics and democracy ignoring the imminent risks of the extinction of the right to privacy, at that time, remeaning in the right to data protection. The expansion of surveillance applied in the daily life of citizens, especially in the face of the advent of the Internet of Things, forced the right to have a new look at categories such as identity, personality, about the imbrication of the digital sphere with the real sphere, where personal data have reached a high market value. This reality is also evidenced by the new data protection law in Brazil (Law 13.709/2018). The Cambridge Analytica X Facebook case clarifies the ways in which such an informational business operates, where human manipulation was intended through the operation of algorithms. Thus, certain public and private actors act in affront to the dignity of the human person, with undemocratic practices that reinvent themselves in the face of the technological device, and it is not possible to know in its entirety how this power will manifest itself in the future. The main objective of this work is to analyze the extent to which surveillance operated through the technological device had achieved or did not exert control over global society. For this we take as a basis the case Cambridge Analytica X Facebook (2016). The methodology used in this research is constituted by the deductive method. The procedure method chosen for the research was the case study. Regarding writing techniques, abstracts and records were used. The basic theory adopted combines authors such as Zygmunt Bauman, Stefano Rodotà and Bruno Ricardo Bioni in dialogue with other authors. The imbrication of surveillance with the technological device has enabled the construction of a global system that operates the manipulation of few on the multitude of human beings.

Keywords: Right to data protection. Surveillance. Internet of Things. Power. Cambridge Analytica.

LISTA DE ABREVIATURAS E SIGLAS

ADC	Associação pelos Direitos Civis
ANDP	Autoridade Nacional de Proteção de Dados
CA	Cambridge Analytica
CADH	Convenção Americana de Direitos Humanos
CEDH	Conferência Euroamericana de Direitos Humanos
CEJIL	Centro pela Justiça e o Direito Internacional
CELS	Centro de Estudos Legais e Sociais
DUDH	Declaração Universal dos Direitos Humanos
EUA	Estados Unidos da América
FSNL	Frente Sandinista de Liberación Nacional
FTC	Comissão Federal do Comércio
LGPD	Lei Geral de Proteção de Dados
OC	Opinião Consultiva
OEA	Organização dos Estados Americanos
OIT	Organização Internacional do Trabalho
ONG	Organização Não Governamental
ONU	Organização das Nações Unidas
OUA	Organização da Unidade Africana
PIDCP	Pacto Internacional de Direitos Civis e Políticos
PIDESC	Pacto Internacional de Direitos Econômicos, Sociais e Culturais
RGPD	Regulamento Geral de Proteção de Dados
TEDH	Tribunal Europeu de Direitos Humanos
TICS	Tecnologias de Informação e Comunicação
UE	União Europeia
UFSM	Universidade Federal de Santa Maria

SUMÁRIO

1 INTRODUÇÃO

O campo da proteção de dados é um dos temas mais desafiadores a serem enfrentados na contemporaneidade, na medida em que os dados pessoais se tornaram elementos basilares da economia global, e a capacidade de controle dos titulares sobre estes se encontra ameaçada, sobretudo, em face da assimetria de poder que caracteriza o negócio informacional. Nesse sentido, a vigilância possibilitada pelo aparato tecnológico favorece o empoderamento de atores públicos e privados que possam exercer controle sobre ferramentas apropriadas para operacionalizar a exploração de dados.

Tal quadro é agravado, ao se considerar que a conectividade se tornou indispensável no cotidiano dos indivíduos e, portanto, o uso de aparelhos aptos para vigilância também. Assim, processos que visam perscrutar os aspectos mais íntimos da vida da pessoa são operados com opacidade, em movimentos que, parecem apontar para a extinção do direito à proteção de dados. Nessa conjuntura, cidadãos são tratados cada vez mais como suspeitos e, valores como democracia, direitos humanos e direitos fundamentais são afrontados frente ao avanço de novas práticas totalitárias, motivadas, especialmente pelas lógicas mercadológica e política.

Nesse sentido, o escândalo *Cambridge Analytica X Facebook* manifesta acerca de como a ausência de leis eficazes que regulamentem a coleta de *Big Data* e, portanto, viabilizem a efetiva proteção de dados pessoais, possibilitam que atores públicos e privados sejam empoderados a ponto de conhecerem profundamente a respeito de populações. E, então de posse de tal conhecimento, implementem práticas de manipulação humana, por meio da aplicabilidade das análises computacionais preditivas. Assim, indivíduos têm seu livre arbítrio violado, ao serem conduzidos a uma realidade imposta por algoritmos, sendo uma forma de poder ampla e, até então, de execução suavizada.

Logo, trata-se de uma abrangente e impactante mudança no âmbito social, onde a vigilância sofisticada pela tecnologia passou a desconhecer quaisquer tipos de fronteiras e a desafiar quaisquer limitações, suscitando uma série de questões jurídicas, políticas, sociais e morais. Vale notar, quanto à impossibilidade de conhecer acerca dos efeitos decorrentes desse contexto na totalidade, no entanto, é seguro afirmar que a imbricação da tecnologia de vigilância com as

lógicas de mercado informacional e política parecem apontar para uma sociedade futura inevitavelmente transparente no que toca ao conhecimento de terceiros acerca de sua privacidade. Portanto, trata-se de um novo tipo de vulnerabilidade[1] humana.

Aliás, tal transparência de indivíduos mostra-se indispensável para a implementação e manutenção de tendências tecnológicas, entre elas, a internet 5 G, a internet das coisas (OIT) e a inteligência artificial (AI). Mas, ainda que a proteção de dados se apresente como uma meta difícil de ser alcançada, não é por essa razão que direitos que garantam a dignidade da pessoa humana, enquanto valor supremo, devam ser rechaçados, ao contrário, em tempos de tecnologias e violações de alcance global, tais direitos adquirem elevada relevância e necessidade máxima de proteção.

Diante dessa nova economia, baseada na informação e sustentada pelo acesso a dados, que reflete visões discriminatórias antigas e estruturais, no que tange ao papel do direito frente à regulamentação de leis que garantam a proteção de dados pessoais, indaga-se: qual o potencial que a vigilância operada por meio do aparato tecnológico demonstra ter para exercer controle sobre a sociedade global, tomando por base o caso *Cambridge Analytica X Facebook* (2016)?

Para responder ao questionamento, objetiva-se analisar em que medida a vigilância operada pelo aparato tecnológico de alcance global conseguirá ou não exercer algum tipo de controle sobre a sociedade global, tendo por base o caso *Cambridge Analytica X Facebook* (2016).

Com relação aos objetivos específicos, busca-se compreender como a vigilância é exercida pelo advento das TICS em um contexto Pós Panóptico, de modo a afrontar o direito à proteção de dados e consequentemente os demais direitos humanos e fundamentais. Também, verificar acerca da influência do paradigma tecnológico e informacional na trajetória percorrida pelo direito à privacidade ao ponto de tal direito ser ressignificado no direito à proteção de dados. Ademais, pretende-se analisar as reflexões que atravessam o direito à

[1] A vulnerabilidade é uma palavra de origem latina, *vulnus,* cujo sentido semântico significa machucado ou ferida, que pode ser compreendida enquanto a potencialidade de o sujeito, então identificado como vulnerável, ser ou estar suscetível a sofrer danos. Dessa forma, compreendemos que a assimetria característica do mercado informacional agrava a condição vulnerável do cidadão, já que para fazer parte da sociedade informacional, deve necessariamente aceitar fornecer seus dados pessoais, podendo ser machucado pela má utilização dos mesmos, sendo que a potência da suposta ferida não pode ser prevista. (BIONI, 2020, p. 155-156).

proteção de dados no Brasil em face do advento da Nova Lei de Proteção de dados (Lei nº 13.709/2018), bem como investigar quanto à ocorrência de uma revitalização da ideia de vigilância frente à inserção da internet das coisas (OIT) e identificar de que forma um “novo” estado de exceção está se materializando na era digital global. Por fim, busca-se investigar o caso *Cambridge Analytica X Facebook* (2016) e compreender se o mesmo pode ser considerado um indicativo de que a vigilância operada por meio do aparato tecnológico aponta para a extinção do direito à proteção de dados em nível global.

Para responder ao problema de pesquisa e abranger o objetivo principal e os objetivos específicos, a metodologia científica empregada neste estudo constitui-se pela abordagem dedutiva. Nesse sentido, utiliza-se do enfoque dedutivo que consiste na argumentação que tornam explícitas conclusões particulares contidas em premissas estabelecidas anteriormente. A técnica desta argumentação consiste em construir estruturas lógicas através da relação entre as premissas e a conclusão. Assim, admitindo-se as premissas, devem-se admitir também as conclusões, pois o conteúdo principal da conclusão já estava, pelo menos, implicitamente, expresso nas premissas (CERVO, 1983).

O método de procedimento escolhido para a pesquisa foi o estudo de caso. Para Yin (2009), o estudo de caso é o método ideal quando o pesquisador não tem controle dos fatos e quando o foco da pesquisa está inserido em um contexto real, o que é demonstrado pela temática abordada (a necessidade da efetiva proteção de dados pessoais em face da vigilância *on-line*). Assim, o estudo de caso, por sua vez, explora profundamente um programa, um evento, uma atividade, um processo ou um ou mais indivíduos. Para esta dissertação, busca-se aprofundar conhecimentos sobre o caso *Cambridge Analytica X Facebook* (2016).

A técnica de pesquisa empregada como ferramenta ao estudo do tema foi pesquisa bibliográfica, através de meios audiovisuais como documentários, além de publicações como livros, artigos científicos, sites e portais institucionais e de notícias. Técnicas de escrita como a elaboração de resumos e fichamentos também foram desenvolvidas durante esse período.

A teoria de base adotada agrega as contribuições teóricas e jurídicas de autores que abordam acerca de como o surgimento do paradigma informacional impacta o direito à proteção de dados pessoais, tais como Zygmunt Bauman, no que se refere ao estabelecimento das bases estruturais para a compreensão

acerca da expansão da vigilância na contemporaneidade, Stefano Rodotà, quanto ao estudo da contribuição do direito à proteção de dados pessoais para uma cidadania futura no contexto da sociedade de vigilância, e Bruno Ricardo Bioni, autor que trabalha de maneira mais específica o panorama da produção jurídica brasileira relacionada à proteção de dados pessoais.

Sustentada por essa teoria de base e em conformidade com a metodologia escolhida, essa pesquisa foi estruturada em três unidades, sendo que a primeira unidade dedica-se a introdução do tema exposto. A segunda unidade, intitulada "Vigilância Pós Panóptico: Liquidez como afronta ao direito fundamental à proteção de dados pessoais e o consequente enfraquecimento dos demais direitos humanos e fundamentais", conta com três subdivisões, quais sejam: 2.1) À privacidade ressignificada no direito à proteção de dados pessoais em tempos de vigilância líquida; 2.2) Reflexões do direito fundamental à proteção de dados pessoais no Brasil com o advento da Nova Lei de Proteção de dados (Lei 13.709/2018). ;

No que toca a terceira unidade, cujo título é: "O poder da vigilância e a aplicabilidade das análises computacionais preditivas", conta com duas subdivisões, estando assim dispostas: 3.1) A revitalização da ideia de vigilância em face da inserção da internet das coisas (OIT); 3.2) A manifestação de um "novo" estado de exceção na era digital global; 3.3) O direito fundamental à proteção de dados rumo à extinção? Perspectivas tendo em vista o caso *Cambridge Analytica X Facebook.*

A presente pesquisa em Direito realizada na área das Ciências Sociais e Humanas do Programa de Pós Graduação em Direito da Universidade Federal de Santa Maria (UFSM), no âmbito dos estudos realizados pelo grupo de pesquisa Núcleo de Direito Constitucional (NDC), adequa-se perfeitamente à linha de pesquisa Direitos da Sociedade em Rede: atores, fatores e processos na mundialização, pois a vigilância suscitada pelo aparato tecnológico que alimenta o negócio informacional avança em detrimento do direito à proteção de dados, na medida em que a rede de atores que exerce controle sobre tais tecnologias, tem como principal objetivo, realizar manipulação sobre humanos, fato que aponta para retrocessos que impactam o ideal democrático em escala global.

Salienta-se que o interesse pessoal pelo tema surge da trajetória da pesquisadora, que desde o TCC da graduação se dedica à investigação científica

na perspectiva da defesa do bem-estar comum acima de quaisquer interesses pessoais, por acreditar ser essa a premissa para uma sociedade mais justa e a própria razão do Estado Democrático de Direito. Tal intento foi reforçado na oportunidade da especialização e novamente se manifesta nessa pesquisa, ainda que sob novos horizontes, entrelaçando os trabalhos realizados.

Vale notar que as violações aos direitos humanos e fundamentais parecem ser potencializadas em face do paradigma informacional global, de forma a trazer significativos retrocessos no que toca as históricas conquistas obtidas norteadas pelo ideal democrático, todavia, de formas suavizadas e opacas. Logo, trata-se de uma nova expressão de controle sobre indivíduos extremamente poderosa, sendo que a assimetria de poder que caracteriza o negócio informacional, inclusive por abarcar uma rede de atores em seus processos, atinge para além dos tradicionais limites nacionais.

Tais práticas de vigilância, em consonância com as tendências tecnológicas futuras, que são alimentadas por dados, em longo prazo, aparentam demostrar ter capacidade para ocasionar um estado de submissão pleno dos indivíduos em nível global, após tê-los tornados transparentes e hipervulneráveis. Dessa forma, a supressão do direito à proteção de dados pessoais, em favor do controle de dados por atores públicos e privados que possam exercer domínio sobre o aparato tecnológico, apresenta-se como uma provável realidade. Portanto, do ponto de vista científico, o tratamento jurídico do tema oportunizado por essa pesquisa é indispensável, em especial porque a matéria que abarca a regulamentação do direito à proteção de dados é nova no Brasil, tendo em vista que a legislação acerca do tema entrou em vigor somente no ano de 2020.

2 VIGILÂNCIA PÓS PANÓPTICO: LIQUIDEZ COMO AFRONTA AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS E O CONSEQUENTE ENFRAQUECIMENTO DOS DEMAIS DIREITOS HUMANOS E FUNDAMENTAIS

A visibilidade é uma armadilha.
(FOUCAULT, 2013, p. 166)

O paradigma informacional viabilizado pelo advento tecnológico e disseminado nos processos sociais consiste em uma tendência global inafastável, sendo um dos mais impactantes fenômenos que caracterizam a cultura contemporânea**.** Assim, o tempo presente encontra-se imerso em expectativas quanto às investidas tecnológicas do futuro como jamais houvera em outro período da história**.** Nesse viés, a forma como a vigilância tem operado com maior sofisticação na sociedade, sendo especialmente favorecida nessa conjuntura, tem sido objeto de análise da doutrina hodierna.

Nesse enquadramento, é possível afirmar que se vive absorto em uma cultura da vigilância, onde o movimento da vida passou a ser monitorado, acompanhado e observado com maior alcance e eficácia, conforme será estudado neste primeiro capítulo. Tal realidade relaciona-se com o surgimento da internet na metade do século XX e final da década de 1960, tendo o fato ocorrido no contexto militar norte americano, cujo intuito fora construir uma comunicação resistente a falhas e ataques por meio de uma rede de computadores interconectados (MAGRANI, 2018, p. 61).

Ao longo do tempo, em face das inovações tecnológicas inerentes aos mecanismos presentes na internet, seus usos foram potencializados, com destaque para a grande interatividade disponibilizada em suas plataformas, culminando na revolução digital que veio a atravessar a sociedade com profundas mudanças. Os efeitos decorrentes dessas alterações ainda estão longe de serem plenamente descortinados, no entanto, impera uma inevitável dificuldade em se apartar o cotidiano da internet. (LEONARDI, 2011, p. 28).

Uma vez que tais processos se encontram em pleno movimento, de forma concomitante, implicam em soluções para antigos problemas e criam novos, como o concernente a dificuldade em torno da regulamentação que diz respeito ao tráfego, à coleta e ao tratamento de dados informáticos no cenário mundial. Pois, tal conjuntura oportunizou que empreendedores viessem a preencher as lacunas

existentes nas plataformas digitais antes dos governos, o que resultou na estruturação de novos tipos de monopólios, verdadeiros impérios globais dedicados à modificação de comportamento humano (LANIER, 2018, p. 35).

Nesse sentido, em que pese a facilidade de circulação da informação em escala global, a sua efetiva proteção se encontra na dependência de uma situação externa favorável à convergência das regras internacionais acerca da proteção de dados pessoais. No entanto, ainda não é possível afirmar até que ponto o direito terá condições de se fazer valer de forma efetiva, para além do seu habitat original, o território estatal. Assim, cogita-se que garantir a preservação do direito fundamental à proteção de dados pessoais em uma sociedade hiperconectada seja um desafio imenso tanto quanto necessário (DONEDA, 2006, p. 310).

Por isso, é seguro afirmar que o cenário exposto aponta para um movimento intenso de aprofundamento quanto ao (des)controle relativo ao acesso por terceiros aos bancos de dados informáticos em âmbito global, uma vez que, mesmo os maiores esforços governamentais em propor regulamentações para a questão, via de regra, têm se mostrado insuficientes para garantir que o ciberespaço perdeu suas características originais, ou seja, de ser um ambiente hostil e de cometimento de abusos e violações (LEONARDI, 2011, p. 222).

Dito isto, assume especial relevância a clarificação quanto à posição de destaque que o direito fundamental à proteção de dados pessoais ocupa em relação à defesa de outros direitos humanos e basilares, como é o caso do direito à liberdade. Pois, tal direito se encontra profundamente prejudicado diante da possibilidade de julgamento de uma pessoa física em função dos arranjos realizados por sistemas de tratamento de dados proveniente de fontes públicas ou privadas, por vezes, de forma intrusa e imposta. Tal fato é ilustrado no que se referem às análises praticadas pelas agências de avaliação de crédito, por exemplo.

Nessa conjuntura, Bauman (2013) teoriza que a vigilância se apresenta de forma onipresente, em estado líquido e perturbador na modernidade, ou seja, em plena expansão. As justificativas para tanto se amparam, ora na necessidade de mais segurança impulsionada pelos governos, especialmente após a tragédia do 11 de setembro de 2001 ocorrida nos Estados Unidos, ora pelo anseio da sociedade moderna em expressar-se e consequentemente expor-se por meio das plataformas digitais, e não menos, devido à conveniência de se responder aos

mais diversos processos sociais disponibilizados por meio de acessos virtuais (BAUMAN, 2013, p. 9).

Destarte, o dispositivo Panóptico de Bentham mostra-se enquanto a figura basilar ensejadora dessa composição social, trata-se da ilustração que apresenta um projeto arquitetural que privilegia um ponto de observação único. Assim, da torre central do Panóptico vê-se tudo, no entanto, sem nunca ser visto. Portanto, uma referência do poder totalitário, de comando e controle centralizado que impelia a uma produção comportamental específica de quem estivesse sendo observado. Todavia, tal comportamento poderia ser deixado de lado a partir do momento que o indivíduo estivesse fora desse lugar físico (FOUCAULT, 2013, p. 165).

Logo, tal descrição comporta um paralelo com uma tendência contemporânea evidenciada pela possibilidade de controle social beneficiada pelas novas tecnologias de vigilância. Segundo a constatação cunhada por Bauman (2013), a descrição desse fenômeno faz referência à vigilância líquida. Todavia, o autor explica que enquanto o Panóptico descreve uma arquitetura permanente em dado local, a vigilância líquida ilustra a respeito de um mundo Pós Panóptico, onde as formas de controle apresentam diferentes faces, que não têm uma conexão óbvia com o prisioneiro, sendo que não há lugar para se escapar da observação (BAUMAN, 2013, p. 12).

A partir do exposto é possível afirmar que, na medida em que os avanços tecnológicos referentes à informação e a comunicação voltados para o contexto da vigilância se intensificam e se aperfeiçoam, por vezes, problematizam tentativas de limitações éticas ou jurídicas no campo social. Tal conjuntura enseja alterações substantivas em face desse direito, que também pode ser pensado pelos termos “vida privada”, “intimidade”, “sigilo”, entre outros, uma vez que tanto a doutrina estrangeira como a brasileira não apresentam um único padrão de nomenclatura. (LEONARDI, 2011, p.46).

A Constituição Federal Brasileira de 1988 declara invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. (Brasil, CF, 1988, art. 5º, X). De mesmo modo, o Código Civil de 2002 declara que a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a

esta norma. (BRASIL, CC, 2002, art.21). No entanto, tais diplomas legais não oferecem conceituação objetiva para as expressões privacidade[2], intimidade e vida privada.

Assim, se pretende, na sequência desse estudo, discorrer de maneira mais específica relativamente às mutações que o paradigma informacional impõe ao direito fundamental à privacidade, de maneira a trazer-lhe um novo significado no direito à proteção de dados pessoais. Para tanto, na próxima seção, ampliaremos essa discussão através da abordagem da privacidade ressignificada no direito à proteção dos dados pessoais.

2.1 A PRIVACIDADE RESSIGNIFICADA NO DIREITO À PROTEÇÃO DE DADOS PESSOAIS EM TEMPOS DE VIGILÂNCIA LÍQUIDA

A potencialização do uso das novas tecnologias de informação e comunicação (TICs) na contemporaneidade veio a repercutir, sobretudo na relativização dos significados e das práticas tradicionais atribuídas aos conceitos de tempo e espaço, sendo que o tempo passou a um estado de aceleração e o espaço não está mais limitado pelas fronteiras geográficas, fora realocado em uma nova perspectiva e estrutura denominada ciberespaço (LEONARDI, 2011, p. 126).

Diante de tantas inovações tecnológicas irrompendo no cenário da vida social, o modelo de tratamento dos direitos fundamentais até então utilizado, deixou de responder eficientemente à nova realidade, especialmente nos contornos atinentes à privacidade. Tema que sofreu inúmeras releituras e

[2] No entanto, existem correntes doutrinárias que diferem tais conceitos, sendo o termo direito à intimidade considerado enquanto uma tipificação dos chamados “direitos da personalidade”, podendo ser conceituado como o direito da pessoa excluir do conhecimento de terceiros tudo aquilo a que ela se relaciona. Nesse sentido, a intimidade diz respeito ao âmbito do que é exclusivo, referente ao que alguém reserva para si, sendo afastado qualquer tipo de repercussão social, nem sequer ao alcance de sua vida privada. Enquanto a vida privada, por mais isolada que possa ser, sempre se caracteriza pelo viver entre outros, seja em família, no trabalho ou no lazer em comum, por exemplo. Ainda, o direito à intimidade pode ser entendido enquanto um direito amplo que comporta diferentes variações, destacando-se o chamado direito ao segredo ou sigilo, que se refere aos fatos específicos que não convêm ser divulgados, seja por razões pessoais, profissionais ou comerciais. Nesse sentido, a Constituição Federal de 1988 estabelece que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei penal estabelecer para fins de investigação criminal ou instrução processual penal. Além disso, o Código Penal estabelece em seu art. 151 o crime de violação de correspondência, o qual é uma forma de violação do direito ao segredo.

mutações ao longo do tempo, em sua maioria, ditadas pela sofisticação do aparato tecnológico. Assim, novas tensões e conflitos de ordem jurídica emergem a espera de solução, pois em decorrência desses fatos recentes, os campos jurídicos também se encontram profundamente transformados (SOMBRA, 2020).

Indispensável, então, que se compreenda a respeito do surgimento dos direitos humanos, cogita-se que mesmo antes de qualquer declaração escrita, jurídica ou política dos direitos comuns ao ser humano, já existiam manifestações destes datadas ainda da Antiguidade. Nesse sentido, é possível afirmar que tais direitos sempre foram precedidos por profundas justificações, tanto de origem ética, moral, religiosa, política, filosófica para a sua exigibilidade e, que a matéria permanentemente se encontra em busca por evolução. As principais teses acerca da origem do tema remontam ao jusnaturalismo[3] e ao positivismo[4], de onde derivaram posições filosóficas diversas (GORCZEVSKI, 2016. p. 55).

[3] É possível afirmar que o jusnaturalismo foi à tese que deu origem e que mais influenciou os direitos humanos. Trata-se de uma fundamentação que compreende que os direitos são anteriores ao Estado, sendo que a humanidade já os possuía no estado de natureza. Entre outros posicionamentos que derivam dessa tese principal, encontra-se a tradição judaico-cristã, sendo que introduziu uma concepção filosófica humanista que reivindicava a liberdade e a igualdade da pessoa humana como algo anterior ao Estado, de forma que este só existe para protegê-los. Assim, entre as várias teses provenientes do jusnaturalismo, destaca-se o jusnaturalismo teológico, que busca fundamento na existência de um ser superior. (GORCZEVSKI, 2016, p. 60). Nesse viés, o cristianismo aprofunda a ideia judia do ser humano criado à semelhança de Deus, e daí a igualdade entre todos os homens. Ocorre que tal ideia, oriunda da Torá, sendo o livro sagrado judeu, sofreu uma variedade de tentativas de alterações em seu sentido original. Pois, após a manifestação de Jesus Cristo, que suscitou uma elevada expansão no número de cristãos, tal fé passou a ser considerada uma ameaça para o império romano, cuja religião adotava a adoração a vários deuses, o que era contrário à ideia judaica de um Deus único e soberano. Então, após as tentativas fracassadas de eliminar os cristãos, o que incluía atirá-los aos leões no Coliseu para divertimento das multidões, Constantino, o imperador romano na época, deu início a Igreja Católica Apostólica Romana, em 323 D.C. no Concílio de Nicéia. No entanto, a nova igreja tratou de abarcar práticas judaicas e romanas ao mesmo tempo, de forma a tentar adaptar a fé judaica com os costumes romanos. Contudo, trata-se de práticas de fé e de cultura totalmente distintas, sendo que não é possível conceber o cristianismo nessa estrutura. Portanto, o cristianismo original apresenta um fundamento de injustiça a quaisquer lesões aos direitos humanos, pois compreende que Deus está presente em cada ser humano, de forma que nem um humano é superior ao outro. (JUS, 2020).

[4] A tese positivista surge como uma reação contra o idealismo que prevalecia na primeira metade do século XIX, com a pretensão de submeter toda e qualquer possibilidade de verdade ao experimento prático. Como seus antecedentes abarca o pragmatismo de Maquiavel, o método experimental de Bacon, o materialismo de Hobbes e o ceticismo de Kant. Foi iniciado por Augusto Comte entre 1798 e 1857. O positivismo jurídico busca “cientificar” o direito, com rigor e exatidão que o aproximem do método matemático. Dessa forma, o positivismo jurídico designa uma concepção de direito como sistema e normas de conduta e de estrutura, postas por seres humanos como ato de vontade, sistema que está constituído, ainda que não exclusivamente, por normas gerais e abstratas, coerentes, ou reduzíveis a coerência e de caráter coercitivo. Para o positivismo os direitos humanos não possuem em si valor intrínseco ou razões morais, apenas positividade. Então, o recurso utilizado para dar consistência a esses direitos foi a sua formalização, que teve como consequência a constitucionalização dos direitos humanos. Tal fundamentação promoveu

O viés jusnaturalista teológico, fundado na existência de valores objetivos e universais, ensina que o cristianismo**,** a primeira religião com pretensões de universalidade, recolhe e aprofunda o princípio judeu datado da Antiguidade do ser humano criado à imagem e semelhança de Deus, daí a igualdade entre todos os homens. Tal princípio, inerente ao cristianismo, aliado ao princípio da fraternidade, que proclama e exalta a dignidade suprema do homem, como filho de Deus, portador de valores eternos e irmão de todos, portanto, sem quaisquer distinções, representou uma afronta ao modelo de sociedade existente na época (GORCZEVSKI, 2016, p. 71).

Afinal, a fé cristã, a partir dos ensinamentos contidos na Bíblia, em Romanos, capítulo 2, versículo 11, sustentava e ainda sustenta que não existem diferenças entre senhores e escravos, o que significava a necessidade de alteração do status quo existente com reflexos, sobretudo, na moral e na economia. As coisas materiais são vistas sob um prisma secundário e a simples existência humana passa a ser o ponto culminante da criação, tendo importância suprema no universo. Dessa forma, o cristianismo manifesta fundamento na defesa dos direitos humanos, ao defender que nenhum homem é superior aos demais, o que contribui para o desenvolvimento e reconhecimento dos direitos do homem, tanto na ordem estatal como na sociedade até os dias atuais.

A doutrina positivista, por sua vez, compreende por direito o que está escrito, expresso pela vontade do poder por meio do direito constitucional de um Estado ou de um órgão que represente os Estados. Resultado de um processo histórico, que abarca as ideias de Hobbes, entre outros filósofos desse período, e o surgimento da Escola da Exegese, onde se buscou fundamentar um direito natural racionalista, motivado pela vontade de estabelecer uma ordem jurídica com caráter universal válida para todos os homens e para todos os tempos, sendo que tais tentativas restaram em princípios fundamentais do direito que vigoram até o tempo presente (GORCZEVSKI, 2016, p. 96).

---

grandes mudanças nos direitos humanos, a exemplo da Declaração Universal dos Direitos Humanos, da abolição da escravatura, da igualdade de direitos civis e políticos da mulher, entre outras. No entanto, o fato de tais direitos ficarem ao arbítrio da vontade do Estado, parece uma perspectiva que deixa em aberto uma porta para a atuação de regimes totalitários em qualquer forma. (GORCZEVSKI, 2016, p. 93 a 97).

Nesse sentido, a doutrina majoritária costuma apresentar uma classificação a respeito dos direitos humanos, onde os direitos humanos propriamente ditos são os considerados inerentes à condição humana, que guardam relação com os documentos de ordem internacional, sendo posicionamentos jurídicos e políticos que reconhecem direitos e liberdades ao ser humano, independente de sua vinculação à determinada Constituição, o que revela o seu caráter supranacional. Enquanto os direitos fundamentais são direitos humanos reconhecidos e positivados pelo direito Constitucional de um Estado (SARLET, 2015, p. 41).

Em relação às antigas formas de proteção à pessoa, a literatura jurídica também apresenta menções, seja no direito grego ou no romano, que podem ser compreendidas como antecedentes a partir dos quais veio a se desenvolver os direitos fundamentais e, mais precisamente os direitos da personalidade, a saber, o direito da pessoa ser o seu próprio fim. No entanto, a proteção da pessoa, especialmente no campo privado, foi inicialmente assimilada com dificuldade, os códigos civis que seguiram o código de Napoleão por mais de um século foram extremamente tímidos nesse aspecto, assim como grande parte da doutrina (DONEDA, 2006, p. 73).

Isto posto, compreende-se que a origem histórica do conceito de intimidade relaciona-se estreitamente com a luta contra o feudalismo e o consequente surgimento do Estado Liberal e da burguesia, a partir do século XVIII, sendo definido à época como “o direito de ser deixado em paz”. Trata-se de uma aspiração dessa classe social com um forte componente individualista, que culminou na ampliação da possibilidade de isolamento frente às condições sociais e econômicas que conduziram ao desenvolvimento dos núcleos urbanos. Dado isso, as novas formas de divisão do trabalho separaram o lugar em que se mora, a casa privada do estabelecimento em que se trabalha (PÉREZ LUÑO, 1984).

Assim, enquanto um privilégio da classe burguesa, como refere Pérez Luño (1984, p. 328): “O direito à vida privada aparece como um direito à solidão, à reserva, ao isolamento”. Nessa acepção, pode-se afirmar que o início do acesso à intimidade remete a possibilidade de dispor-se de condições de vida financeiramente favoráveis para manter o isolamento, realidade que, evidentemente, não contemplava a população mais humilde da época e que, portanto, encontrava-se à margem das expectativas quanto ao alcance a esse direito.

Como direito de faceta liberal, se evidencia o aspecto originário negativo do direito à privacidade, sendo que o cidadão se contentava com o fato de o Estado não interferir em seu direito de liberdade, em face ao absolutismo monárquico vigente na época. No entanto, o Estado social veio a consolidar a dimensão positiva dos direitos, cujo direito à privacidade passou a ter uma faceta positiva que se manifestará, a partir do direito de acesso, retificação e cancelamento dos dados. Tal perspectiva é fundamental, uma vez que as informações passaram a ser armazenadas por longo tempo, constituindo essencial que o cidadão possa acessá-las, modificá-las ou até mesmo cancelá-las (LIMBERGER, 2016, p. 50).

Cumpre salientar que o ordenamento jurídico reconhece que o artigo de Warren e Brandeis*, "The Right to Privacy"* publicado em 1890 na revista *Harvard Law Review,* inaugurou o debate moderno acerca da privacidade, ao trazer a compreensão de que a privacidade passa a ser entendida como uma proteção em si mesma, uma forma de tutela da própria pessoa humana, independente do direito à propriedade. O direito de ser deixado em paz, da expressão inglesa "*the right to be let alone*", se destaca em face da difusão generalizada da imprensa e seu potencial para interferir na vida privada. Assim, a modernidade suscita um rompimento, sobretudo, do ponto de vista jurídico do direito à privacidade com o direito à propriedade (LEONARDI, 2011, p. 52).

Em vista disso, pode-se afirmar que a contemporaneidade ainda ocasiona diferentes formas de acesso ao direito à intimidade que podem ser ilustradas pelas desigualdades perceptíveis na distribuição de rendas, implicando em possibilidades de acesso a moradia extremamente contraditórias, a exemplo da proliferação de luxuosos condomínios fechados, ao mesmo tempo em que subsistem moradias miseráveis compartilhadas por muitos indivíduos nos aglomerados urbanos presentes na atualidade.

Há que se ressalvar ainda, no tocante à proteção dos direitos humanos, que embora existam várias manifestações relevantes, entre estas a Magna Carta em 1215, o *Bill of Rights* em 1689, a Declaração Norte Americana de Independência de 1778 e a Declaração Francesa de 1789, o marco histórico principal do processo da internacionalização dos direitos humanos se inicia em 1946 quando o Conselho Econômico e Social da ONU, constituiu uma Comissão de Direitos Humanos incumbida de elaborar uma Declaração de Direitos Humanos que, após alguns ajustes, fora aprovada em 1948 (GORCZEVSKI, 2016, p. 156).

Em referência a esse período mais recente da história, constata-se que com o término da segunda guerra mundial e, consequentemente, com os impactos frente às atrocidades humanitárias nela cometidas, surge à visão de proteção internacional dos direitos humanos. Devido acontecimento fora facilitado pela liberdade de imprensa, bem como pelo desenvolvimento de modernos meios de comunicação, resultando em uma desacomodação no conceito clássico de soberania estatal, até então tido como um poder ilimitado, para dar lugar a um mínimo ético comum universal (GERVASONI, 2017, p. 178).

Nessa acepção, destaca-se a seguir o artigo 12 da Declaração Universal de Direitos Humanos (DUDH), dispositivo que trata da privacidade, sendo esse pertencente aos direitos civis e políticos, embasados pelos princípios da igualdade e da fraternidade:

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da Lei. (ASSEMBLEIA GERAL DA ONU, 1948).

Dessa forma, a necessidade de plena realização do direito fundamental à privacidade, enquanto um direito de caráter humano e universal, sendo alvo de resguardo internacional, resta fundamentado. Contudo, dada a competência para fazer recomendações atribuída a DUDH, portanto, não sendo um documento juridicamente vinculante, nada se pode afirmar acerca de punições aos Estados que violarem tal direito.

Nessa perspectiva, constata-se que a partir dos anos setenta, surgiram inúmeros instrumentos nacionais e internacionais, destaca-se a OCDE (Organização para a Cooperação e Desenvolvimento Econômico) e o Conselho da Europa que adotaram em 1981 instrumentos nessa área. Em 2000, a Carta de Direitos fundamentais da União Europeia reconheceu a proteção de dados como um direito autônomo, estabelecendo a distinção entre o convencional direito de respeito à vida privada e familiar e o direito a proteção de dados pessoais (RODOTÁ, 2008, p. 16).

Portanto, a natureza do direito à privacidade se revela tanto por ser um direito humano resguardado pela Organização Nacional das Nações Unidas, como em seu atributo de ser um direito fundamental positivado e protegido pelas

Constituições dos Estados Democráticos de Direito. Assim, em que pesem os reposicionamentos, as mutações e as ressignificações que vieram a comportar no decorrer da história, especialmente favorecido pelo advento das novas TICs, foi redefinido no direito à proteção de dados pessoais na contemporaneidade.

Ainda no que concerne a adoção das novas TICs, cumpre destacar o impacto que estas vieram a causar ao alterarem a noção clássica de privacidade, anteriormente peculiar às relações familiares e a exclusão do conhecimento alheio sobre a intimidade da pessoa. Assim, passa-se a levar em consideração, sobretudo, um poder de controle que a pessoa deve ter sobre suas informações pessoais, dadas as ameaças decorrentes da globalização e da sociedade informacional que passam a ter uma relação muito significativa com a privacidade.

Nesse viés, Rodotà (2008, p. 15) ensina que a privacidade pode ser compreendida como "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular". Além disso, o desastre ocorrido em onze de setembro de 2001 inaugura uma nova concepção no tocante ao direito à privacidade, onde esta é considerada um obstáculo à segurança, sendo, por vezes, superada por legislações de emergência, deixando de ser tratada na prática enquanto um direito fundamental (RODOTÀ, 2008, p. 14).

Tal constatação é demonstrada, particularmente pelas decisões na Europa sobre a transferência de dados pessoais de passageiros de linhas aéreas a outros países. Isso, desde a entrada em vigor do "*General Data Protection Regulation* Nº 2016/679", ou Regulamento Geral de Proteção de dados pessoais (RGPD), que regula o armazenamento e o processamento de dados pessoais de indivíduos, bem como de informações pertencentes a empresas e demais organizações que se utilizarem dos serviços de aviação.

Para fins de segurança nacional, a diretiva tem por escopo evitar os ataques terroristas como os que ocorreram na França[5] sendo que essa legislação prevê que as companhias aéreas repassem aos países membros do bloco o registro dos dados dos passageiros que partiram ou chegaram à Europa para oportuno rastreamento. Quanto ao seu alcance, essa legislação veio a repercutir

[5] GLOBO. G1, 2015. Disponível em: <http://g1.globo.com/mundo/noticia/2016/07/franca-foi-alvo-de-multiplos-ataques-desde-janeiro-de-2015.html>. Acesso em: jan. 2019.

para além da Europa, ao influenciar outros países quanto a necessidade de tais medidas de prevenção ao terror, inclusive possibilitando a troca de informações entre países, a depender do reconhecimento do Conselho Europeu acerca da credibilidade das informações por eles fornecidas (SOMBRA, 2020).

Como regra geral, a transferência de dados pessoais a um país fora da União Europeia só pode ocorrer após a Comissão Europeia ter decidido que tal país apresenta um nível adequado de proteção de informações, conhecido como decisão de adequação. No entanto, o Brasil ainda não se beneficia de uma decisão de adequação proferida pela Comissão Europeia relacionada à transferência de dados nos termos do RGPD, ao contrário da Argentina que foi o primeiro Estado latino-americano a receber o juízo positivo de adequação pela União Europeia de sua normativa aos padrões europeus (DONEDA, 2006, p. 343).

Nesse contexto, importante salientar que, no Brasil, a Agência Nacional de Aviação Civil já havia editado em 2012, a Resolução nº 255 que regula o compartilhamento de dados pessoais de passageiros e tripulantes para fins migratórios e de segurança nacional, tendo definido dois conceitos relacionados ao compartilhamento de dados pessoais sendo Informações Antecipadas sobre Passageiros e Registro de Identificação de Passageiros (ANAC, 2014).

De acordo com a Resolução nº 255, as empresas brasileiras e estrangeiras que exploram serviço de transporte aéreo público, com exceção das empresas de táxi aéreo, devem disponibilizar, por meio de mensagem eletrônica segura, as informações disponíveis sobre passageiros e tripulantes a bordo de suas aeronaves em voos internacionais com destino, origem ou trânsito pelo território nacional, devendo fazer constar em seus contratos de transporte a informação de que os dados de reserva dos passageiros serão disponibilizados às autoridades de controle migratório (Polícia Federal), aduaneiro (Receita Federal), sanitário (Anvisa) e agropecuário (Vigiagro).

Recentemente, a ANAC submeteu à Consulta Pública nº 10/2020 a proposta de revisão da Resolução nº 255 que tem por objetivo estabelecer a padronização de informações de passageiros a órgãos de segurança pública, de dados de reserva e registro de viagens para a avaliação de risco relacionado à segurança da aviação civil contra atos de interferência ilícita em voos domésticos. A proposta submetida é também do interesse da Agência Nacional de Vigilância Sanitária (Anvisa) no que diz respeito aos aspectos de controle epidemiológico.

Para tanto, as contribuições foram encaminhadas à Agência por meio de formulário eletrônico próprio, disponibilizado em seu endereço eletrônico, até 3 de junho de 2020 (ANAC, 2014).

Tal Consulta Pública resultou na aprovação da revisão da Resolução nº255, de modo que foi definido prazo de 6 meses para a entrada em vigor da norma. Contudo, considerando o volume e especificidades dos voos domésticos, foi estabelecido um período de implementação assistida de seis meses, posterior a entrada em vigor da norma, durante o qual os entes regulados ficarão isentos de penalidades administrativas, não sendo, portanto, emitidos autos de infração no período indicado para possíveis inconformidades verificadas. Uma vez que, para a correta coleta e envio dos dados, além do desenvolvimento de canal de recepção de forma segura das informações, deve o operador aéreo ter condições de incorporar devidamente os novos procedimentos a sua rotina (ANAC, 2020).[6]

Uma vez que o volume de dados tratados pelas companhias aéreas é gigantesco, o que se justifica pela amplitude de suas atividades, é possível afirmar que a realidade evidenciada pelos rumos que a legislação em torno da aviação tem tomado, clarifica o fato de que se vive em uma conjuntura que afeta nossa autonomia e consequentemente o direito de desenvolver plenamente nossa personalidade, de modo a se facilitar que os outros se apropriem de certa forma de nosso ser. Assim, percebe-se que se trata de um processo de normalização da transparência do eu, onde o critério de segurança pública se converte em exclusivo critério de referência (LIMBERGER, 2016, p. 62-63).

Logo, o sistema de proteção de dados pessoais passa a ser cada vez mais percebido pelo critério da multifuncionalidade, por vezes, pela pressão exercida pelas agências institucionais no plano doméstico e internacional. Assim, dados coletados para um propósito específico por determinada agência são disponibilizados para propósitos diversos para agências diferentes. Tal é a liquidez que caracteriza a vigilância e reflete o quão transparentes encontram-se os cidadãos, sendo que os órgãos públicos ou privados que operam essa vigilância não estão submetidos a controles eficazes, nem sob o aspecto político, nem sob o aspecto legal (RODOTÀ, 2008, p. 15).

---

[6] GOVERNO. BR, 2020. Disponível em: <https://www.anac.gov.br/participacao-social/consultas publicas/consultas/2020/10/cp-10-2020-rac.pdf> Acesso em: 11 fev. 2020.

Nesse sentido, faz-se oportuno considerar o posicionamento relativo à proteção de dados pessoais acerca da experiência da União Europeia. A propósito, importa enfatizar que a base desses dispositivos remetem à dignidade da pessoa humana, conforme o art. 1º. da Carta dos Direitos Fundamentais do bloco elaborada no ano 2000: “Dignidade do ser humano. A dignidade do ser humano é inviolável. Deve ser respeitada e protegida”. Tal normativa passou a ter força jurídica e vinculativa com o Tratado de Lisboa em 2009, onde os Estados membros são obrigados a respeitar a Carta quando aplicam a legislação europeia (RODOTÁ, 2008, p. 295).

Interessante ressaltar que um dos pontos mais relevantes acerca da experiência europeia em proteger os dados pessoais consiste na adoção de uma autoridade administrativa independente responsável pela proteção desses. Tal posicionamento não se limita ao território europeu, sendo identificado também em outros países como Estados Unidos, Argentina e Taiwan. Nessa senda, indispensável mencionar o pioneirismo alemão, que criou em 1970, a primeira Lei de Proteção de Dados Pessoais do mundo no Estado de Hesse, cujo impulsionou a criação da primeira Lei Federal de Proteção de Dados Pessoais em 1979, em um momento identificado pelo avanço do desenvolvimento tecnológico (BURKERT, 2000 apud FORTES, 2016, p. 154).

Reforçando o pioneirismo alemão, em 1983, em consequência de um histórico julgamento no Tribunal Constitucional Federal do caso envolvendo a Lei do Censo, que determinava o recenseamento geral da população, portanto, objetivava a coleta de dados para confrontar com os existentes no registro civil para repassar a autoridade pública, houve o reconhecimento do direito fundamental à autodeterminação informativa sobre os dados de caráter pessoal. Trata-se de um marco para a proteção jurídica dos dados pessoais, uma vez que os indivíduos passaram a ter o direito de determinar se desejam tornar públicas informações a seu respeito, bem como a quem cedê-las e em que ocasião (LIMBERGER, 2016, p. 51).

O mesmo Tribunal, por ensejo da expansão das TICs, veio a atualizar o direito à autodeterminação informativa a partir do novo direito fundamental à garantia de confidencialidade e integridade dos sistemas técnico-informacionais no ano de 2008. Nesse sentido, embora a decisão tenha sido restrita à atuação do poder público, é amplamente reconhecido o impacto que de igual forma pode

causar no setor privado. Tal posicionamento ilustra acerca da aludida migração das relações e da condução da vida na sociedade informacional para o ambiente virtual (LIMBERGER, 2016, p. 52).

A seguir, passa-se a notabilizar algumas disposições de origem europeia a respeito da proteção dos dados pessoais:

> Artigo 8º:
> Proteção de dados pessoais:
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
> 3. O cumprimento destas regras fica sujeito à fiscalização por parte de uma autoridade independente (CARTA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPÉIA, 2000).

Tal proteção fora reforçada posteriormente no Tratado que propôs a criação de uma Constituição com jurisdição nos países membros da União Europeia, que traz no artigo I-51, capitulado na seção “Vida democrática da União” a previsão deste instituto legal. Ainda, a Carta Constitucional europeia também apresenta essa previsão legal no artigo II – 68, capitulado na seção das “Liberdades” (UNIÃO EUROPEIA, 2004).

Ademais, a Diretiva 95/46/CE prevê derrogações específicas do tema, ao instituir regras de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como a livre circulação desses dados no continente europeu. Por conseguinte, a mesma destaca a necessidade dos sistemas de tratamento de dados respeitarem as liberdades e os direitos fundamentais, singularmente considerados, de modo a assegurarem a proteção à vida privada, assim como contribuir para o progresso econômico e social dos indivíduos. (PARLAMENTO EUROPEU E CONSELHO, 2014).

A respeito do entendimento relativamente ao conceito atribuído aos dados pessoais, oportuno lembrar que sua parte inicial consta no artigo 2º, “a” da Diretiva 95/46/CE do Conselho da Europa, cujo teor do dispositivo embasou para além das normativas daquele bloco, o desenvolvimento de leis e edificações doutrinárias acerca do tema em variadas partes do mundo (SILVA, 2019, p. 347). Os dados pessoais compreendem, segundo tal dispositivo:

> [...] qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa). É considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social. (UNIÃO EUROPÉIA, 1995).

Nesse viés, esse importante instrumento jurídico também apresenta a definição acerca do tratamento de dados pessoais, sendo:

> [...] qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição. (PARLAMENTO EUROPEU E CONSELHO, 2014).

A Diretiva considerou ainda a definição relativamente ao consentimento da pessoa em causa enquanto “qualquer manifestação da vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento.” (PARLAMENTO EUROPEU E CONSELHO, 2014).

Analisando esses instrumentos jurídicos, pode-se afirmar que o modelo regulatório europeu prevê: que todas as pessoas têm direito à proteção de dados de caráter pessoal que lhes digam respeito; que esses dados devem ser objeto de um tratamento leal, para fins específicos, desde que se disponha do consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei; e que o cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

As normativas europeias refletem que a proteção de dados na contemporaneidade torna-se um valor em si mesma, ao sintetizar as prerrogativas da pessoa, contribui para a construção da cidadania condizente com a vivência da sociedade informacional. Logo, é possível afirmar que as novas TICs no que tange as diversas possibilidades de intercâmbio de dados entre indivíduos, organizações e governos acabam por transformar o contexto sobre o qual incidem as normas europeias de proteção de dados, bem como buscam a garantia do direito à privacidade (FORTES, 2016, p. 169).

Fato é que frequentemente surgem novos acontecimentos atinentes ao espaço virtual com desdobramentos no espaço real, que vêm a ensejar a possibilidade de reconhecimento de novos direitos, aos quais os operadores do direito necessitam estar aptos para apresentarem soluções diante da realidade de um direito em trânsito na contemporaneidade. É o caso da discussão teórica que afirma ser a autodeterminação informativa um novo direito ou faceta do direito à privacidade, que embora novo, já apresenta uma evolução condizente com a positivação do reconhecimento do direito à proteção de dados pessoais, de forma autônoma (LIMBERGER, 2016, p. 52).

Assim, diante desse direito em trânsito, notabiliza-se também o caso do que alguns autores denominam de “direito ao esquecimento” e “direito a extimidade”. Nesse sentido, o direito ao esquecimento vem a conferir a possibilidade de um usuário apagar seus dados e suas informações pessoais na internet, enquanto o direito a extimidade seria a maneira como algumas questões relativas à intimidade são oferecidas ao público, desse modo, a intimidade deixa de ser íntima, todavia, ela não se torna pública e sim “extima”, ou seja, revela-se com a perspectiva de que aquele conteúdo que foi aberto seja visto dentro de certo controle (NASCIMENTO, 2017, p. 283).

Com efeito, a privacidade ressignificada no direito à proteção de dados pessoais, assume posição de destaque na proteção da pessoa humana, sendo que o real interesse em sua tutela reside na dignidade da pessoa humana, finalmente uma forma de tutela da própria pessoa. Tais inovações convergem na busca por uma esfera privada garantidora de que a pessoa não passe a ser submetida a formas de controle social, que finalmente venham a desembocar em restrições as liberdades, anulando-se a individualidade, cerceando-se a autonomia privada e inviabilizando-se o livre desenvolvimento da personalidade (DONEDA, 2006, p. 142).

Portanto, a relativização evidenciada pela sociedade informacional acerca da exploração de seus dados acarreta, sobretudo, em ameaças permanentes aos direitos de liberdade por parte de entes públicos ou privados, e o fio condutor para tanto reside em um caminho que aponta para a institucionalização da supressão do exercício do direito à privacidade, bem como da tutela dos dados pessoais. Essa reflexão importa na medida em que a vigilância líquida tem potencial para

violar direitos civis, políticos, econômicos, sociais e culturais, atingindo a um número ilimitado de indivíduos, além de instituições públicas e privadas.

Nesse sentido, a identificação de indivíduos a partir de dados pessoais, fornecidos de maneira espontânea, imposta ou coletados por meios diversos, sendo posteriormente direcionados a entes públicos ou privados, culmina na problemática de estes indivíduos virem a ser representados e julgados de acordo com o conteúdo destes dados e não conforme aquilo que realmente são. Tal fato pode significar perda de autonomia, de individualidade e, por fim, de liberdade, a exemplo dos dados poderem ser examinados no julgamento de uma concessão de um plano de saúde ou seleção para um emprego, além de tantas outras hipóteses de maneiras indevidas (DONEDA, 2006, p. 2).

Portanto, as demandas que moldam o perfil da privacidade, antes ditadas nos moldes da propriedade, atualmente estão condicionadas pelo paradigma informacional e não mais pelos casos clássicos de violação à privacidade. Assim, notabiliza-se uma tendência paradoxal ilustrada por um movimento de exteriorização da intimidade, suscitando a ocorrência de um deslocamento do direito à privacidade, do âmbito do direito de personalidade ao campo do direito patrimonial, uma vez que, pessoas recebem valores patrimoniais relevantes em troca da exposição de sua intimidade (LIMBERGER, 2016, p. 61).

Haja vista que o fluxo de informações no meio informático só faz crescer incessantemente, de forma proporcional aumenta o número de oportunidades de os indivíduos realizarem escolhas que podem influir em suas esferas privadas, inclusive quanto a preferências realizadas na esfera virtual com desdobramentos na esfera da vida real. Importa que a proteção de dados pessoais para além da privacidade, tutela também a pessoa, classes e grupos sociais contra as mais diversas violações, a exemplo da ocorrência de discriminações e do controle indevido praticado por determinados atores (SILVEIRA, 2020, p. 60).

O tema da proteção do direito à privacidade ressignificado na proteção dos dados pessoais na conjuntura hodierna, em face do fenômeno informático assinala que os principais riscos que afrontam sua proteção enquanto direito fundamental, residem no poder operado pela vigilância líquida. O poder que busca normalizar um processo global de transparência dos indivíduos perante determinadas organizações, que podem ser de natureza pública ou privada, mas que convergem quanto ao objetivo de conhecer tudo quanto é possível do ser, a fim de se

alcançar especialmente proveito econômico ou político, por meio da manipulação destes (DIAS, 2020, p. 539).

No que tange a essência do valor resguardado no direito à proteção de dados pessoais, é toda a inserção da pessoa na sociedade que deve ser considerada, sendo a proteção devida a esse direito condição para a igualdade e fruição dos demais direitos humanos e fundamentais. Portanto, a tutela relativamente aos dados pessoais se apresenta como o meio necessário para a concretização de um conjunto de valores fundamentais que devem acompanhar a pessoa em qualquer momento da vida. Afinal, em uma relação democrática inexistem posições de supremacia ou privilégio que possam justificar o menosprezo à dignidade (RODOTÀ, 2008, p. 291).

A seguir, será abordado acerca das repercussões do direito à proteção de dados pessoais no cenário brasileiro, em face aos desdobramentos de ordem social e jurídicas presentes diante do fenômeno manifesto pela conexão entre a necessidade de proteção de dados pessoais e as possibilidades de vigilância sofisticadas pelas novas TICs. Considere-se que tais inovações costumam ser oferecidas sob o argumento de que são um modo de capturar, controlar e, até mesmo, eliminar incertezas inerentes à condição humana. Todavia, o qual faculta um ambiente, sobretudo, de vulnerabilidades do ser humano derivadas das interconexões da esfera real com a esfera virtual.

2.2 REFLEXÕES DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS NO BRASIL COM O ADVENTO DA NOVA LEI DE PROTEÇÃO DE DADOS (Lei 13.709/2018)

Ao tratar das repercussões do direito fundamental à proteção de dados pessoais com o advento da nova Lei de Proteção de dados no Brasil (Lei nº 13.709/2018), este capítulo desenvolve um recorte ao priorizar aspectos materiais vinculados ao tema específico desta dissertação, em detrimento de outros aspectos procedimentais, como também de outras temáticas abordadas pela novel legislação. Vale salientar, que a LGPD tem origem na esteira da promulgação da RGPD pela União Europeia, que já debatia o tema da proteção de dados enquanto um direito fundamental há mais de 20 anos.

Nesse enquadramento, é fato que a realidade hodierna expressa um novo ciclo de desenvolvimento econômico assinalado pelo avanço do paradigma informacional que tem impulsionado a sociedade da informação, fomentando assim a consolidação de um novo mercado de geração de valor. Nesse sentido, a principal ferramenta de trabalho advém da gigantesca abundância de dados gerados mediante a utilização dos recursos da rede[7] em escala mundial.

A valoração atribuída aos dados pessoais disponibilizados pelo uso da internet, diante do fato de que tal fornecimento, por parte dos cidadãos, parece ter se tornado um requisito indispensável para a sua efetiva participação no meio social, em troca de serviços, se deve a viabilidade que a vigilância, em torno dos mesmos, oportuniza para a formulação de perfis individuais ou de grupos sociais. Tal categorização é especialmente proveitosa, tanto para análises de mercado, como para objetivos políticos, a exemplo do direcionamento de campanhas eleitorais, conforme se evidencia no caso *Cambridge Analytica X Facebook.*

Tal cenário amplia nas agendas sociais e políticas, em escala global, a imprescindibilidade de se estabelecer ferramentas jurídicas que regulem a coleta, o uso, o armazenamento, o tratamento e a proteção dos dados pessoais com eficácia. Na busca por apresentar respostas nesse contexto em que a vigilância *on-line* e a economia se entrelaçam, recentemente passou a vigorar no Brasil a nova Lei de Proteção de Dados. Trata-se de uma lei específica com o escopo de regular a proteção de dados de maneira ampla.

A relevância da LGPD vem sendo reforçada em face da atual pandemia causada pelo Coronavírus que veio a acometer a saúde de parte significativa da humanidade, de modo a impactar histórica e negativamente a economia global. Tal cenário revelou ainda mais acerca das vulnerabilidades presentes nos sistemas de bancos de dados informáticos de órgãos públicos e instituições privadas. A crise em curso trouxe maiores desafios à implementação da LGPD, sobretudo, quanto a sua vigência, sob o argumento de que sua aplicação poderia agravar ainda mais a situação do setor empresarial, que não poderia arcar com as possíveis sanções administrativas previstas na norma (CHICARONI; SERRAGLIO; DA SILVA, 2020).

[7] Compreendemos rede enquanto uma ou mais estruturas comunicativas no âmbito da vida social que viabilizam a interação entre diferentes atores sociais, de forma a impulsionar os valores e interesses destes. Manuel Castells (2016, p.53).

Portanto, os caminhos para a efetivação da LGPD restaram permeados por tentativas políticas de adiamento no período que antecedeu a sua entrada em vigor. Fato é que a norma foi promulgada em 14 de agosto de 2018 prevendo um difícil processo de adaptação dos empresários e dos próprios entes públicos, na ocasião o Legislativo estabeleceu um prazo considerado bastante dilatado de vacância, sendo de 12 meses. E, novamente em julho de 2019 o Congresso aprovou a prorrogação do início da vigência por mais 12 meses (DIAS, 2020).

Além disso, sobrevieram outras medidas de adiamento da vigência da LGPD, a exemplo do Projeto de Lei nº 1.179/2020, que dispunha sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado, posteriormente editado sob o nº 14.010/2020, sendo que, de acordo com a sua previsão, somente a vigência dos artigos da LGPD relacionados à aplicação de sanções administrativas seriam adiados (DIAS, 2020).

Além destes, integram este rol, a Medida Provisória nº 959/2020 que buscava prorrogar mais uma vez a *vacatio legis* da LGDP para 03 de maio de 2021, com exceção da aplicação de sanções administrativas às violações da lei, que só passariam a vigorar em agosto de 2021. Tal medida, contudo, foi convergida na lei nº14. 058/2020, cujo instaurou a principal norma no Brasil objetivando tutelar os direitos dos titulares dos dados, a chamada Lei Geral de Proteção de dados[8].

Tendo em vista que a relevância da entrada em vigor da LGPD foi elevada em face do enfrentamento à crise causada pela pandemia, vale pontuar que o Governo Federal (2019-2023) concedeu um valor para custeio das despesas da população mais vulnerável por meio do denominado Auxílio Emergencial. Trata-se de um programa de benefício financeiro destinado aos trabalhadores informais, microempreendedores individuais, autônomos e desempregados, tendo por escopo fornecer proteção de caráter emergencial. Ocorre que o cadastramento para a obtenção do benefício fora disponibilizado por meio do envio dos dados pessoais dos solicitantes para um aplicativo do governo intitulado Caixa Tem. [9]

[8] BRASIL. Lei n° 14058. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L14058.htm)>. Acesso em: 08 de mai. 2019.

[9] BRASIL. Lei n° 13982. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13982.htm>. Acesso em: 10 de jun. 2019.

Dessa forma, a aprovação para o recebimento do benefício dependeu de um cruzamento de dados operado pela agência governamental acerca de cada possível beneficiário, a fim de se definir a aptidão ou não dos mesmos para tanto. Nesse viés, a construção da identidade fica entregue por completo aos algoritmos, sendo que o direito à autodeterminação informativa, por vezes, se torna inoperante face à identidade esculpida mediante procedimentos automáticos. Tal nova abstração produz um esvaziamento do humano, de modo que é oportuno afirmar acerca da existência de uma singular antropologia virtual (LIMBERGER, 2016, p. 63).

Fato é que o processo responsável pelo cruzamento desses dados foi atravessado por significativas imprecisões, a exemplo da negativa do valor do benefício, sob a alegação de que o solicitante não preenchia os requisitos estabelecidos pelo Ministério da Cidadania, por estar eleito, ou até mesmo por estar morto, entre outros posicionamentos do órgão público que se demostraram inverídicos quando embasaram a negativa ou mesmo a concessão indevida. Assim, enquanto milhares de pessoas que cumpriam os requisitos para a aprovação não o obtiveram de imediato, outros milhares que não cumpriam esses requisitos por não estarem vulneráveis inclusive servidores públicos, foram contempladas.[10]

Nesse contexto, equívocos quanto aos dados apresentados pelo Governo vieram a ser manifestos pelos titulares dos dados, pelo menos, perante a mídia, uma vez que a agência governamental não disponibilizou um canal de atendimento destinado a resolver tais questões de forma célere. Todavia, vale notar que tal possibilidade poderia ter sido viabilizada de imediato por meio do cruzamento dos dados analisados com as informações obtidas em outros bancos de dados governamentais, como os da Receita Federal e da Justiça Eleitoral que, mais tarde, comprovaram a incompatibilidade.

Cumpre salientar que o princípio da dignidade da pessoa humana, expresso no artigo 1º, III da Constituição da República Federativa do Brasil constitui-se basilar na ordem constitucional, sendo fundamento e vetor interpretativo dos demais direitos fundamentais (BRASIL, 1988). Portanto, a dignidade de tais

[10] GLOBO. G1, 2020. Disponível em: < https://g1.globo.com/economia/noticia/2020/05/05/auxilio-emergencial-saiba-quais-sao-os-principais-erros-de-cadastro-que-podem-provocar-demora-na-analise-do-beneficio.ghtml>. Acesso em: 20 set. 2019.

cidadãos resta significativamente maculada diante da incompatibilidade de dados evidenciada pelo sistema governamental, somado ao fato de que o AE não apresentava formas de contestação acerca das decisões negativadas externadas compatíveis com a urgência de sua natureza.

Para a persecução desse propósito, no entanto, o próprio Governo Federal posteriormente firmou um acordo de cooperação técnica com a Defensoria Pública da União para solucionar o caso das pessoas que foram injustiçadas por meio administrativo, intentando impedir posteriores processos pela via judicial. Logo, é possível afirmar, diante do ocorrido, que tal ação por parte do ente público remete a uma racionalidade instrumental de modo que o primado da eficácia, em nome da razão técnica, acaba por esvaziar o conteúdo concreto, pois a necessidade emergencial das pessoas vulneráveis foi irremediavelmente prejudicada (DIÁRIO OFICIAL DA UNIÃO, 2020).

Deste modo, é possível afirmar que a alternativa apresentada pelo Governo Federal brasileiro no que toca ao Programa do AE, a depender de um cruzamento de dados inicialmente considerado apto somente pelo veredito do Ministério da Cidadania, manifesta acerca da problemática que abarca a proteção de dados pessoais no Brasil que carecia de um marco regulatório condizente com tais enfrentamentos. Afinal, não somente os possíveis danos afeitos à dignidade da pessoa humana, mas também o avanço tecnológico e as pressões do mercado internacional corroboravam tal necessidade (RIANELLI, 2020).

Nesse viés, importa enfatizar que o reconhecimento do direito fundamental à privacidade consta expresso na CF de 1988, compreendendo a proteção da vida privada e da intimidade, além da honra e imagem.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, 1988).

A positivação constitucional do direito à privacidade no Brasil tem origem na doutrina e jurisprudência alemã, segundo a teoria das esferas ou círculos concêntricos, cujas esferas da vida privada comportam o grau de interferência que o indivíduo vem a suportar com relação à terceiros. Nessa perspectiva, leva-se em

consideração o grau de reserva do menor para o maior, sendo que, no círculo exterior se encontra à privacidade; no intermediário, a intimidade; e, no interior desta, o sigilo. Assim, a tutela legal se intensifica, à medida que se adentra no interior da última esfera, ou seja, quanto mais interno dentro das esferas estiver o comportamento, mais intensa deverá ser a proteção jurídica. (LIMBERGER, 2016, p. 53).

Nessa acepção, a Constituição protege alguns outros aspectos específicos relacionados à privacidade, sendo que o artigo 5º, inciso XI proíbe a invasão de domicílio, enquanto o artigo 5º, inciso XII garante a inviolabilidade de dados, referindo-se à interceptação de correspondências e comunicações telefônicas. Além disso, estabelece a figura do *Habeas Data*, regulamentada pela Lei 9507/97, como remédio constitucional previsto no artigo 5º, inciso LXXII, que estipula uma modalidade destinada à proteção dos dados pessoais, por meio do direito de acesso e de retificação das informações constantes de registros ou bancos de dados de entidades governamentais ou de caráter público (BRASIL, 1988).

Assim sendo, o *Habeas Data* configura entre os elementos em vigência de maior destaque para a atuação da proteção de dados no ordenamento brasileiro. Tal remédio apresenta a peculiaridade de ter influído em outras legislações latino-americanas, sendo que certos fatores geopolíticos parecem ter contribuído para essa realidade, uma vez que em sociedades recém-saídas de regimes ditatoriais, como era o panorama de muitos desses países na década de 1980, persistia na sociedade o trauma pelo uso autoritário da informação (DONEDA, 2006, p. 328).

Assim, é possível afirmar que tal remédio fora concebido com o escopo de proporcionar ao cidadão um instrumento para conhecer diretamente e, se necessário, retificar as informações sobre sua própria pessoa armazenadas em bancos de dados em mãos do poder público. Portanto, tendo um papel importante na formação de uma cultura democrática no Brasil que ainda carece de afirmação.

No que se refere à aplicação da Lei 9507/97, em seu artigo 1º, parágrafo único, a definição de caráter público permite concluir que se incluem também os titulares de bancos de dados privados, conforme consta a seguir: “Considera-se de caráter público todo o registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações.” (BRASIL, 1997).

A ambiguidade da expressão “de caráter público” motivou uma atuação positiva da doutrina e da jurisprudência a fim de estender a abrangência da ação para além dos órgãos públicos, entendimento este que prosperou especialmente com a edição do Código de Defesa do Consumidor de 1990. A provável maior limitação desse instrumento consiste em ser uma ferramenta de proteção de dados pessoais que tenha como principais braços de atuação o recurso a uma ação judicial, com a exigência de um advogado, após um inafastável périplo administrativo. Portanto, ainda não se apresenta como um sistema adequado às exigências acerca da celeridade que caracteriza a matéria (DONEDA, 2006, p. 337).

Pérez Luño, por outro lado, leciona que o *Habeas Data* é apontado como ferramenta apta para a proteção jurisdicional do direito à autodeterminação informativa, expondo que tal direito se traduz em uma nova faceta do direito à privacidade e, como tal, requer novos instrumentos jurídicos para se tornar efetivo. Assim, para o autor, tal instrumento emerge enquanto principal ferramenta à disposição do jurisdicionado no que se refere à ampla tutela de seus dados pessoais (PÉREZ LUÑO, 2005, p. 357).

Importa salientar que os problemas relacionados ao tratamento de dados pessoais processam-se, cada vez mais, sem que o titular se aperceba. Logo, os instrumentos jurídicos dedicados à sua proteção devem ser satisfatórios, considerando que a vigilância opera mediante um veloz avanço tecnológico. De modo que, em igual proporção, expandem as violações da privacidade no ambiente virtual. Tal fato ilustra a respeito da necessidade urgente de adequação do ordenamento jurídico diante da realidade que o circunda, sob o risco de o direito à proteção de dados pessoais ser extinto diante de barreiras institucionais.

No que tange ao plano infraconstitucional, os direitos de personalidade são elencados no Capítulo II do Código Civil de 2002, que prevê a inviolabilidade da vida privada em seu artigo 21: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.” (BRASIL, 2002). Ademais, existem outras disposições esparsas que podem ser evocadas, especialmente advindas da tutela de dados do consumidor, tais como o artigo 43 da Lei nº 8.078/1990, Código de Defesa do Consumidor (BRASIL, 1990), e os artigos 3º, 5º e 14º da Lei nº 12.414/2011, Lei do Cadastro Positivo (BRASIL, 2011a).

No tocante às informações no âmbito da Administração Pública, ao contrário da esfera privada, a necessidade de transparência para os cidadãos resta enquanto um princípio fundamental, demonstrando ser uma integração do princípio da publicidade conjugado com o direito à informação previsto no artigo 5º, XXXIII da Constituição, agregado com o princípio democrático. Deste modo, o fato de a informação estar mais disponível corrobora para um maior cuidado no trato com os recursos públicos, bem como para uma diminuição do nível da corrupção (LIMBERGER, 2016, p. 45)

Com relação à divulgação de informações pelo poder público, merece destaque a Lei nº 10.520/2002 e Decretos n.º 5.450/2005 e n.º 5.504/2005 relativos ao Pregão Eletrônico (BRASIL, 2005), a Lei Complementar nº 101/2000, que disciplina a Lei de Responsabilidade Fiscal, com as alterações da Lei Complementar nº131/2009 acerca da publicação dos gastos da administração em rede (BRASIL, 2009), a Lei nº 12.527/2011 e o Decreto nº 7.724/2012 que a regulamenta, cujo escopo é difundir a informação pública, impondo aos entes da administração o dever de publicizar os dados que possam contribuir ao debate democrático e ao controle social (LIMBERGER, 2016, p. 48).

Além disso, relativamente a Constituição brasileira, considera-se que contempla a esfera da informação inicialmente através das garantias à liberdade de expressão previstas no artigo 5º, IX e no artigo 220 (BRASIL, 1988). Tais garantias se encontram em uma situação de confronto com a proteção da privacidade, sendo que o embate repercute em variados debates, sobretudo no cenário político, com destaque para a questão que atravessa o discurso de ódio e a divulgação de *fake news.*

Assim sendo, embora na Carta Magna não haja previsão direta e expressa que contemple o direito à proteção de dados pessoais, ao derivarmos esse direito do direito à privacidade, tal entendimento vem a abarcar a disciplina sob a égide constitucional, ainda que sob o risco de simplificar os fundamentos da tutela dos dados pessoais e eventualmente limitar seu alcance. Afinal, a proteção dos dados pessoais consiste em uma garantia de caráter instrumental, derivada da tutela à privacidade, no entanto, não limitada por esta, sendo que faz referência a um leque de garantias fundamentais presentes no ordenamento brasileiro (DONEDA, 2006, p. 326).

Dessa forma, os critérios suscitados pela inovação tecnológica implicam na imprescindibilidade de atualização na seara jurídica acerca da questão da privacidade ressignificada no direito à proteção de dados pessoais. Pois, a sociedade informacional se comporta de modo a expor opiniões e imagens no meio virtual, situação que possibilita com que tais revelações fiquem permanentemente expostas a monitoramento, projetadas sobre um conjunto mais amplo e global das relações intersubjetivas. Tal lógica impõe que cidadãos tenham compreensão acerca da sua identidade esculpida por algoritmos (DUNKER, 2020).

Com isso, destaca-se, o advento do “Marco Civil da Internet”, sob a Lei 12.965/2014, objeto das mais longas discussões no âmbito da sociedade civil, por meio de ferramentas de consulta pública, em um processo global pioneiro. Assim, instituindo uma carta de direitos para a internet no Brasil. Todavia, críticas podem ser feitas quanto a algumas falhas presentes na norma, sobretudo, quanto ao veto acerca da criação de uma autoridade reguladora independente. O que não abala o reconhecimento da contribuição dessa legislação para combater a anomia jurídica recorrente nesse campo até então, e seu potencial para influenciar novas conquistas democráticas para os internautas pelo mundo (BIONI, 2019, p. 132).

Tal legislação estabelece princípios, garantias, direitos e deveres, elencando em seu artigo 3º, II e III, a proteção da privacidade e dados pessoais enquanto fundamento que norteia o uso da internet no Brasil. Dessa forma, a normativa representa a regulamentação mais relevante relativa à proteção da privacidade e dados pessoais nesse território, mesmo que contemple exclusivamente o ambiente virtual. Destaca-se ainda a previsão acerca da responsabilização dos agentes de acordo com as atividades exercidas (BRASIL, 2014).

O Marco Civil da Internet se adianta no tratamento do tema da proteção de dados pessoais na internet, ao exigir que as informações sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais sejam claras e completas, limitadas a finalidades que justifiquem a coleta, não sejam vedadas pela legislação, estejam especificadas nos contratos de prestação de serviço ou ainda em termos de uso de aplicações de internet. Ademais, foi estabelecida a aplicação das normas de proteção e defesa do consumidor que abarcam as relações de consumo realizadas na internet (FORTES, 2016, p. 128).

No que concerne a tutela de dados pessoais, a normativa recepciona a exigência do consentimento de forma mais destacada que as demais cláusulas contratuais, do mesmo jeito que possibilita a exclusão em definitivo dos dados pessoais que tiverem sido fornecidos para determinada aplicação de internet, a requerimento do interessado, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registro elencadas em lei. Além disso, determina que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, devem compreender a preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (BRASIL, 2014).

Cumpre ainda salientar, que as disposições contidas no artigo 19 referem os danos decorrentes de conteúdo ofensivo gerado por terceiros, sendo que tal matéria vem sendo objeto de debates no meio jurídico. Segundo essas disposições, o provedor de aplicações da internet será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros, somente se após ordem judicial específica, não tomar as devidas providências para tornar indisponível o conteúdo apontado como infringente (BRASIL, 2014).

Tal previsão burocratiza o cumprimento da norma, em contrariedade a natureza cabível as medidas afeitas a coibir propagações de informações depreciativas, que devem ser céleres dadas a velocidade da transmissão de dados no meio informático. Nesse sentido, a lei se mostrou mais assertiva ao excepcionar a exigência de ordem judicial quanto à situação de conteúdos relacionados a sexo e nudez, de acordo com o artigo 21 (LIMBERGER, 2016, p. 79).

Nesse enquadramento, no ano de 2016 foi assinado o Decreto nº 8.771 regulamentando o Marco Civil da Internet, abarcando as hipóteses de discriminação de dados na internet e de degradação de tráfego, ao definir procedimentos para a guarda e a proteção de dados por parte de provedores de conexão e de aplicações de internet e aponta medidas de transparência na requisição de dados cadastrais pela administração pública, bem como determina parâmetros para a fiscalização e apuração de infrações (FORTES, 2016, p. 130).

Dessa forma, o Marco Civil da Internet representa uma evolução normativa acerca da discussão que circunda a matéria da proteção de dados pessoais no

Brasil, cujas disposições apontaram o caminho a seguir para a lei que abrangesse o nível protetivo adequado para a inserção do país no padrão europeu. Contudo, se trata de um debate permanentemente em construção, que teve seguimento mediante o processo de contribuições para um anteprojeto de lei de proteção de dados pessoais, no Brasil, no ano de 2015, na plataforma “Pensando o direito”, vinculada ao site do Ministério da Justiça na época.

Destarte, o anteprojeto de lei de proteção de dados, seguiu rumo à regulamentação da proteção de dados no país, sendo encaminhado ao Congresso Nacional em 2016 e então passando a tramitar como Projeto de Lei nº5. 276/2016, que acabou apensado ao Projeto de Lei nº 4060/2012, cujo se identifica a ampla abrangência da tutela dos dados pessoais contida no anteprojeto apresentado pelo Ministério da Justiça (FORTES, 2016, p. 131).

Dito isso, é possível afirmar que a pauta foi retomada no país também mediante a divulgação do escândalo envolvendo a empresa *Cambridge Analytica*. Ocasião em que se revelou que mais de 50 milhões de usuários da plataforma *Facebook* tiveram seus dados pessoais tratados pela empresa, sem o devido consentimento, com o escopo de manipular as eleições presidenciais norte-americanas de 2016, em favor de Donald Trump, candidato na época. E, também, pela entrada em vigor do RGPD da União Europeia, uma vez que tal normativa veda a transferência internacional de dados a países sem a devida adequação legislativa (ROSENBERG et al, 2018).

É notório que se vive em uma sociedade cada vez mais movida a dados, cuja falta de regulamentação adequada a resguardar, sobretudo, a dignidade humana, viabiliza a ocorrência de desfechos sociais calamitosos. Tal escândalo ilustra sobre práticas viabilizadas por um mercado informacional, capaz de desvirtuar sociedades da verdade, favorecendo a delegação de poder por meios fraudulentos a lideranças ilegítimas. Sendo assim, os impactos sociais possibilitados pela exploração de dados, demonstram ser capazes de atingir a essência do ideal democrático.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) brasileira, no ano de 2018, sob o nº 13.709/2018, foi sancionada para entrar em vigor inicialmente em agosto do ano de 2020. Trata-se de uma matéria de ampla relevância, sendo o direito à proteção de dados pessoais um direito fundamental e autônomo para a tutela da pessoa humana (BRASIL, 2018).

Em consonância com o presente paradigma informacional que favorece a consolidação de espaços públicos virtuais, sendo a gestão da informação pessoal uma expressão fundamental do indivíduo, o que se traduz no direito à autodeterminação informativa, a novel legislação (art. 1º) expressa que a proteção conferida tem o objetivo de “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, através da garantia de eficaz defesa e controle dos dados pessoais aos indivíduos (BRASIL, 2018).

Nessa sequência, a LGPD inspirada pelo RGPD europeu, e em harmonia com perspectivas contempladas em normas anteriores, como o Marco Civil da Internet e o anteprojeto de lei de proteção de dados, juntamente com o respeito à privacidade, a liberdade de expressão, de informação, de comunicação e de opinião e a inviolabilidade da intimidade, da honra e da imagem, dentre outros direitos (art. 2º), anuncia seus fundamentos, com destaque para a autodeterminação informativa, que passa a ser um direito definitivamente incorporado no ordenamento jurídico brasileiro (BRASIL, 2018).

Adiante, a lei brasileira manifesta aplicação extraterritorial, sendo aplicável também para empresas estabelecidas fora do território do Brasil, desde que o tratamento seja realizado em território nacional (art.3º, I) e que tenha, por finalidade, a oferta de bens ou serviços ao mercado consumidor brasileiro ou o tratamento de dados de indivíduos localizados no país (art. 3º, II), ou ainda que os dados tenham sido coletados no território nacional art.3º, III).

É possível concluir, de acordo com as hipóteses elencadas no artigo 3º, que, se o tratamento ocorrer no território brasileiro, ainda que tenha sido apenas com dados de pessoas naturais estrangeiras, aplica-se a lei. De outra banda, a LGPD protege qualquer indivíduo que se localize em território nacional na ocasião do tratamento de dados que tenha por objetivo a oferta de produtos ou serviços a este mercado, ainda que possa se tratar de estrangeiro em breve passagem pelo país (BRASIL, 2018).

Tendo como norte a identificação das bases legais acerca do tratamento de dados, se verifica que o foco da proteção conferida pela LGPD consiste na pessoa natural, cujos dados são tutelados em dois parâmetros, a depender de serem ou não sensíveis. É possível afirmar que “dado pessoal” assume concepção excessivamente abrangente ao ser definido (art.5º, I) como “informação

relacionada à pessoa natural identificada ou identificável". Assim, o "dado pessoal sensível" é tipificado como o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Com efeito, acerca de dados pessoais sensíveis, uma vez que faz referência a informações relacionadas aos aspectos mais íntimos da pessoa, portanto, podendo ser alvo de discriminações abusivas, importa atentar para o fato de que um dado inicialmente caracterizado como não sensível pelo legislador, pode o ser, por revelar indiretamente, aspectos alusivos à origem étnica, como é o caso do sobrenome, bem como quanto à convicção religiosa de acordo com os nomes atribuídos aos filhos. Desse modo, qualquer dado vinculado ou potencialmente vinculável a uma determinada pessoa natural, portanto, se encontra previsto no escopo protetivo da LGPD, observadas as exceções (art. 4º), independente do meio de armazenamento (art. 5º, IV) (OLIVA et al, 2019).

A afirmação quanto ao fato de dados pessoais aparentemente não sensíveis, que podem vir a se tornar sensíveis, é coerente e reforçada diante da técnica de coleta e cruzamento de milhares de bases de dados procedentes de diferentes origens, oportunizada pelo *Big Data*. Pois, algoritmos podem ser programados para estabelecer a correlação que se pretende ao se combinar informações aparentemente insignificantes, para se identificar uma série de padrões de comportamento, com o fim de traçar o perfil de indivíduos. Então, atingindo-se os dados sensíveis (BIONI, 2020, p. 37).

Assim como na definição relativa aos diferentes tipos de dados (art. 5º), pessoal, pessoal sensível, anonimizado, banco de dados, etc. a LGPD define outros conceitos que nortearão a sua interpretação e aplicação, como é o caso de "tratamento de dados" (art. 5º, IV), entre outros. Desse modo, é possível afirmar que, quanto à sua incidência, a LGPD mostra-se de forma ampla (art. 5º, X) (BRASIL, 2018).

Tal normativa em seu artigo 7º estabelece dez hipóteses que tratam acerca da autorização necessária para o tratamento de dados pessoais, a começar pelo consentimento do titular. Embora a lei não demonstre qualquer hierarquia entre tais hipóteses, ainda é possível se destacar o consentimento como o elemento principal entre as demais bases legais de tratamento de dados, sobretudo, ao se

ponderar que os princípios elencados pela lei, bem como a maneira como seu corpo normativo disseca tal elemento, demostram enfatizar o protagonismo do indivíduo no controle do fluxo de suas informações pessoais (BIONI, 2019, p. 134).

Nesse viés, a lei define consentimento (art. 5º, XII) como a "[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", cujo deverá ser fornecido por escrito, em cláusulas destacadas das demais, ou por qualquer outro meio capaz de demonstrar de forma inequívoca, ao especificar as finalidades determinadas, podendo ser revogado a qualquer tempo, conforme previsto no artigo 8º, caput e parágrafos. Assim, a lei permite a utilização de outros meios como arquivos de áudio e vídeo, entre outros, para a manifestação do consentimento, desde que devidamente relacionados aos termos do tratamento de dados especificados (BRASIL, 2018).

O consentimento, enquanto meio para a determinação da esfera privada, vem a se constituir em um instrumento que se presta para o livre desenvolvimento da personalidade. No entanto, os parâmetros a serem levados em consideração para determinar o perfil desse consentimento, não são os mesmos que embasam a atuação da autonomia privada nos mecanismos negociais tradicionais, uma vez que se deve levar em conta fatores particulares deste (DONEDA, 2006, p. 378).

Os problemas derivados de uma transposição rasa do consentimento negocial para o consentimento ao tratamento de dados pessoais implica em reflexos da adaptação de uma estrutura formal a uma realidade atravessada por subjetividades. Portanto, a fundamentação deste consentimento reside na possibilidade de autodeterminação informativa em relação aos dados pessoais, sendo esta autodeterminação o principal elemento para caracterizarmos a natureza jurídica e os efeitos desse consentimento e não a expansão da lógica mercadológica. Nessa acepção, justifica-se a não consideração do consentimento enquanto negócio jurídico (DONEDA, 2006, p. 380).

Ainda, é possível argumentar acerca do protagonismo do consentimento previsto no inciso I do art. 7º, tendo em vista uma série de disposições que dão um regramento específico para concretizar, orientar e, em última análise, reforçar o controle dos dados pessoais por meio do consentimento, como por exemplo, o consentimento deveria ser extraído por meio de "cláusulas contratuais destacadas" (Art. 8º, parágrafo 1); autorizações genéricas, ou, sem uma

determinada finalidade, seriam nulas (Art. 8º, parágrafo 4º); nas hipóteses em que inexiste consentimento se deveriam observar os direitos e princípios da LGPD (Art. 7º, parágrafo 6º); de modo que haja a possibilidade de o titular dos dados pessoais se opor ao tratamento de dados (Art. 18°, parágrafo 2º) (BRASIL, 2018).

Sendo assim, restam dúvidas acerca da adequação e suficiência desse instrumento normativo quando se analisa a capacidade dos titulares dos dados pessoais em exercer o devido controle sobre seus dados. Tendo em vista a disparidade de meios entre o cidadão e quem solicita os dados, por vezes, revestido por impessoalidade, especialmente nas relações *on-line*. Nessa conjuntura, é possível afirmar sobre a necessidade de se aprimorar tal estratégia regulatória para além do conteúdo que se depreende da LGPD (BIONI, 2019, p. 135).

Nesse sentido, a fim de que o consentimento seja legítimo, faz-se necessário ir além dos arranjos contratuais característicos das plataformas digitais representados por caixas de seleção de concordância com os termos e condições dos fornecedores de serviços, como condição única de acesso a conveniências inerentes a vida moderna. Para uma efetiva proteção de dados, é preciso garantir a individualização de tais interesses por meio de mecanismos regulatórios que concedam, ao usuário, a possibilidade de não consentir com a cessão de seus dados pessoais sem que isso acarrete na impossibilidade de acessar tais comodidades. Entretanto, tal tutela no atual estado da arte do consentimento ilustrada pelo tudo ou nada se mostra demasiadamente distante (BODIN DE MORAES; QUEIROZ, 2019).

Além disso, a LGPD estabelece diversas outras hipóteses que permitem o tratamento de dados pessoais, mesmo sem a manifestação da vontade do titular, são situações taxativas nas quais o tratamento de dados ocorre mesmo sem a o consentimento de seu titular com destaque para o inciso VI do artigo 7º, que permite o tratamento de dados quando for necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Ainda, o inciso IX do artigo 7º autoriza o tratamento de dados pessoais quando se mostrar necessário para atender aos interesses legítimos do controlador ou de terceiros, contudo, aponta como exceção os casos em que prevalecem direitos e liberdades fundamentais que exijam a proteção de dados pessoais (BRASIL, 2018).

A LGPD prevê no art. 9º a garantia ao titular dos dados quanto ao direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da finalidade específica do tratamento; da forma e da duração do tratamento, observados os segredos comercial e industrial; da identificação do controlador; das informações de contato do controlador; das informações sobre o uso compartilhado de dados pelo controlador e finalidade; das responsabilidades dos agentes que realizarão o tratamento; e dos direitos do titular. Além disso, faz menção explícita aos direitos contidos no art. 18° da LGPD, abarcando outras características previstas em regulamentação tendo como objetivo o atendimento do princípio do livre acesso aos seus dados (BRASIL, 2018).

À vista dos enfrentamentos que atravessam o campo da proteção de dados pessoais, Doneda (2006, p. 373) expõe que “A disparidade de meios entre a pessoa, de quem são exigidos os dados pessoais, e aquele que os solicita faz com que a verdadeira opção seja tantas vezes a de “tudo ou nada”, “pegar ou largar”.

Ao parecer buscar impedir tais políticas em que, para o usuário, inexiste outra opção a não ser a do consentimento, caso contrário, lhe será negado o acesso a produtos ou serviços, a LGPD dispõe (art. 9º, parágrafo 3º), que se o tratamento de dados for condição para o fornecimento de produto, serviço ou para o exercício de direito, o titular deverá ser informado de maneira destacada sobre esse fato e sobre os meios pelos quais poderá exercer os direitos elencados posteriormente pelo art. 18º (BRASIL, 2018). No entanto, este dispositivo parece não impedir tal prática abusiva.

No art. 10 da LGPD o legislador tratou de regulamentar o legítimo interesse do controlador, sendo que este somente poderá fundamentar o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, contudo, não se limitam a: (Art. X, I) apoio e promoção de atividades do controlador; e (Art. X, II) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e seus direitos e liberdades fundamentais (BRASIL, 2018).

Desse modo, qualquer utilização dos dados pessoais deve obedecer à finalidade legítima comunicada ao interessado antes da coleta de seus dados,

assim, fundamenta-se a restrição da transferência de dados pessoais a terceiros, bem como, estrutura-se um critério para valorar a razoabilidade da utilização de determinados dados para dada finalidade, fora da qual se configuraria abusividade (Parágrafo 1º). Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados (Parágrafo 2º). O controlador ainda deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse, (parágrafo 3º) cuja autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

O tratamento de dados sensíveis fora previsto no artigo 11º, estes dados são definidos pela lei como relacionados à [...] origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (Art.5º, II), considerando que tal tratamento torna o titular vulnerável a toda a sorte de discriminações. Tal tutela reflete quanto ao risco de macular-se a dignidade da pessoa humana, o que é agravado em face da opacidade presente nas formas como os dados são tratados (BRASIL, 2018).

Importa destacar que, de acordo com as bases legais elencadas no artigo 11º, mesmo os dados pessoais sensíveis poderão ser objeto de tratamento, ainda que sem o consentimento de seu titular. Todavia, não se pode perder de vista que o devido tratamento está relacionado, em grande medida, aos objetivos de proteção do próprio Estado Democrático de Direito e dos interesses públicos. Por isso, deve-se intentar um viés interpretativo dessa normativa de modo a se priorizar um tratamento de dados sensíveis restrito e limitado ao seu propósito específico, conforme expressam os princípios da finalidade e da não discriminação (MULHOLLAND, 2018, p. 163).

A denominação desses dados enquanto dados sensíveis que justificam uma proteção especial no que se refere aos riscos em torno de seu tratamento, deriva de seu potencial para serem utilizados de forma discriminatória. Portanto, tais dados integram fortemente a esfera privada exatamente para garantir a plenitude da esfera pública, o que se manifesta pela proibição de determinados

sujeitos realizarem sua coleta, a exemplo de empregadores. Assim sendo, para algumas categorias de dados sensíveis, deve prevalecer o direito fundamental da pessoa a qual se refere às informações consentir ou não no tratamento, sendo a única finalidade admissível o interesse ou não da pessoa considerada (RODOTÀ, 2008, p. 96).

Assim, ao dispor de um rol de situações amplo que dispensa o consentimento do titular em face do tratamento de dados sensíveis, grande parte em hipóteses que referem um suposto interesse público, a lei acaba por efetuar uma evidente ponderação de interesses, onde prevalecem os interesses de natureza pública sobre os interesses do titular, mesmo que se trate de direitos fundamentais. Tal contexto deixa em aberto riscos significativos para o pleno exercício de direitos e liberdades fundamentais, com ênfase para os da igualdade, liberdade e privacidade (MULHOLLAND, 2018, p. 168).

Vale notar, que o *Big Data* pode ser considerado o êxtase do processo de exploração mercantil dos dados pessoais, pois tal tecnologia abarca um volume excepcional de dados e permite que estes sejam ordenados e examinados para uma cadeia indeterminada de finalidades, possibilitando correlacionar uma série de dados, estabelecendo-se, entre eles, relações a fim de se desvendar padrões. Inclusive, com o escopo de inferirem probabilidades de acontecimentos futuros. Cada vez mais, os dados dos cidadãos, dispersos na rede, dizem mais ao seu respeito, sendo que, quem os manipula, sabe até mais do que seus titulares e seus pares (BIONI, 2019, p. 34).

Na sequência, o artigo 12 da LGPD estabelece que os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Não obstante as dificuldades e incertezas que o tema suscita, não há como não se deter quanto a possibilidade de reversão do processo de anonimização por terceiros, mediante “esforços razoáveis”, cuja determinação, nos termos do parágrafo 1º (Art. 12°), deve levar em consideração fatores objetivos, tais como custo e tempo necessários, de acordo com as tecnologias disponíveis.

Ainda, o artigo 18° (IV) da LGPD fixa enquanto um direito do titular dos dados pessoais a obtenção, junto ao controlador, da anonimização, bloqueio ou

eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a referida legislação (BRASIL, 2018).

Dessa forma, o legislador reconhece a possibilidade de reversão do processo de anonimização, sendo que, aparentemente seria legítimo ao operador de dados o realizar, desde que conforme os termos descritos na LGPD. Oportunizando uma perspectiva de regulamentação específica, o parágrafo 3º do Art. 12° da LGPD, autoriza a Autoridade Nacional de Proteção de dados, ainda a ser constituída, em conjunto com o Conselho Nacional de Proteção de dados pessoais, a fim de que venha a editar regulamento dispondo sobre os padrões e técnicas a serem empregadas em processos de anonimização (BRASIL, 2018).

De todo o modo, independente de qualquer regulamentação pela ANDP, parece ser o caso dessa anonimização ser feita por empresa independente e não internamente pelo próprio controlador, na tentativa de realizar tal processo de forma a assegurar mais efetividade no que tange a garantia do direito fundamental à proteção de dados *on-line*.

No rastro de muitos problemas, teóricos, práticos, virtuais e reais, suscitados pela capacidade de vigilância *on-line* favorecida pelo aparato tecnológico e pela crise do direito à proteção de dados nesse contexto, a questão acerca da possibilidade de reversão do processo de anonimização é particularmente preocupante. Pois, a internet e as demais tecnologias de informação podem ainda não ter posto fim a tal direito, no entanto, ressignificaram a privacidade. Fato é, que em uma era de processadores, sensores e redes com custos extremamente minimizados, a liberdade corre o risco de se tornar inversamente proporcional à eficiência dos meios disponíveis de vigilância (LEONARDI, 2011, p. 42).

Nessa conjuntura, os internautas, especialmente os menores de idade, se encontram em acentuada vulnerabilidade e à mercê de inúmeras violações, seja por parte de *Big Techs*, cuja ação velada e sofisticada dificulta a percepção dos ataques, seja pela atuação do Estado em razão do uso de seu aparato de vigilância sobre os cidadãos, o que é feito sob os mais variados argumentos, a exemplo da defesa da soberania nacional e do combate à criminalidade (LEAL, 2019, p. 20).

A LGPD inova ao apresentar regulamentação em referência ao direito dos usuários dessa faixa etária, pois as legislações anteriores, voltadas a regularem o

uso da internet, não apresentavam disposições nesse sentido. Dessa forma, a novel legislação se alinha a redação dos artigos 226 a 229 da Constituição Federal, assim como a Convenção Internacional sobre os Direitos da Criança (1989), da qual o Brasil é signatário e a Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente). Ao tratar da defesa, sobretudo, da dignidade da pessoa humana, em que pese sua vulnerabilidade ante o fenômeno informático, tais destinatários merecem um tratamento com o devido relevo, pois, por vezes, acessam a internet destituídos de mediação familiar, o que vem a ampliar sua exposição (BRASIL, 2018).

Nessa continuidade, o parágrafo 1º do artigo 14 da LGPD exige o consentimento específico de, pelo menos, um dos pais ou responsáveis para tornar legítimo o tratamento de dados dos usuários. Tal disposição se alinha com o sistema civilista brasileiro, que exige a representação ou assistência para dar validade aos atos jurídicos de crianças e adolescentes considerados incapazes. (Art. 3º do Código Civil) (BRASIL, 2018).

Na sequência, o artigo 15° da LGPD disciplina sobre o término do tratamento de dados, que ocorrerá quando a finalidade foi alcançada ou os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada (Art. 15°, I); houver o fim do período de tratamento (Art.15, II); o titular comunicar, inclusive no exercício de seu direito de revogação de consentimento, resguardado o interesse público (Art. 15°, III); ou quando houver determinação da ANDP, por violação ao disposto na referida Lei (Art. 15°, IV) (BRASIL, 2018).

Além disso, no artigo 16°, a LGPD determina que os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: cumprimento de obrigação legal ou regulatória pelo controlador (Art. 16, I); estudo por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (Art. 16, II); transferência a terceiro, desde que respeitados os requisitos de tratamento de dados (Art. 16, III); ou uso exclusivo do controlador, vedado seu acesso por terceiro e desde que anonimizados os dados (Art. 16, IV).

Diferentemente do posicionamento que a lei brasileira toma ao demonstrar um baixo caráter protetivo em relação aos dados sensíveis dos titulares, o mesmo não pode ser constatado com relação aos direitos garantidos aos titulares, regulamentados pelo Capítulo III da LGPD.

Desse modo, a lei reforça no artigo 17° as garantias constitucionais da liberdade, da intimidade e da privacidade, sendo que, no artigo 18°, a lei assegura: os direitos de confirmação da existência de tratamento (Art. 18°, I); acesso a dados (Art. 18, II); correção de dados incompletos, inexatos ou desatualizados (Art. 18, III); anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei (BRASIL, 2018).

Por meio desse catálogo de direitos, a LGPD especifica os conteúdos representativos do direito à autodeterminação informativa, qual seja, “o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada.” (RODOTÀ, 2008. p.109), sendo concedido ao titular dos dados, a possibilidade de exercer um controle direto e contínuo sobre os coletores das informações, independentemente da existência real de uma violação (RODOTÁ, 2008, p. 60).

Dessa forma, o legislador demonstra compreender acerca de que o principal vetor para alcançar tal objetivo consiste em franquear ao cidadão controle sobre o fluxo de seus dados, sendo que tal estratégia vai além do consentimento do titular dos dados. É a combinação dos elementos que integram a autodeterminação informativa tão significativo quanto o consentimento, sendo imperioso assegurar que o fluxo informacional atenda suas legítimas expectativas, sobretudo, não sendo prejudicial ao livre desenvolvimento da personalidade (BIONI, 2020, p. 105).

Para tanto, são necessárias medidas e procedimentos capazes de oportunizar que se descortine a existência de bancos de tratamento de dados em nome dos titulares, bem como o acesso a esses dados, ainda, a possibilidade de corrigi-los, de retificá-los, de solicitar o cancelamento do tratamento, quando necessário, entre outras medidas, conforme regulamenta a LGPD no artigo 18° (BRASIL, 2018).

No entanto, quanto a tais medidas, conforme o entendimento de Bioni (2019, p. 137), sustentam que o indivíduo é um ser dotado de capacidade para controlar as suas informações pessoais, propondo um quadro regulatório atravessado por uma visão simplista do conteúdo devido à autodeterminação informacional que, passadas mais de três décadas não mais se ajusta ao contexto compacto que caracterizava o fluxo de dados, sendo atualmente ativo econômico

em constante circulação que molda o livre desenvolvimento da personalidade dos cidadãos. Portanto, faz-se premente a própria compreensão do conteúdo e do significado de tal direito.

Tal conjuntura aponta para a necessidade de empoderamento dos titulares de dados por meio das possibilidades advindas da própria tecnologia, bem como do direito, para que, de fato, tenham capacidade de exercer plenamente seu direito de autodeterminação informativa. No entanto, conforme propõe Rodotà (2008, p. 60), uma proteção fundada unicamente nos poderes atribuídos aos titulares de dados é problematizada pela fluidez dos dados pessoais, sendo necessária a atribuição de um poder geral de vigilância a órgãos criados especificamente para a proteção de dados.

Por outro lado, é possível afirmar que havia certa expectativa, especialmente por parte da doutrina pátria, acerca de a LGPD vir a reconhecer e regulamentar no que toca ao direito ao esquecimento, que no entendimento de Parentoni (2015, p. 511):

> É a faculdade de obstar o processamento informatizado, a transferência ou publicação de dados pessoais, além de exigir que sejam apagados, sempre que a sua preservação esteja causando constrangimento ao sujeito envolvido, desde que não exista razão de interesse público que justifique a sua preservação.

O direito ao esquecimento, que consta expressamente no RGPD europeu, disciplinado no art. 17° sob o título: “Direito de ser esquecido ou apagamento”, está contido na ideia de privacidade, mais precisamente na parcela da privacidade que diz respeito ao tratamento informatizado de dados pessoais.

> Artigo 17°
> 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:
> a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
> b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n. º2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
> c) O titular opõe-se ao tratamento nos termos do artigo 21°, nº1, e não existem interesses legítimos prevalentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n° 2;

> d) os dados pessoais foram tratados ilicitamente. [...] (PARLAMENTO EUROPEU, 2016, s.p).

Tal direito na sociedade informacional comporta a harmonia entre a aspiração de preservar as informações publicadas em nome de uma internet livre e sem censura, e a sustentação do direito de extingui-las, quando prejudiciais ao sujeito, em benefício da privacidade ou de um recomeço. Sendo assim, o paradigma informacional, não pode legitimar que dados irrelevantes sejam mantidos na internet em detrimento aos direitos de personalidade dos titulares de dados, sendo preciso resgatar o equilíbrio entre a memória coletiva e a pretensão individual (PARENTONI, 2015, p. 545-548).

Desse modo, a LGPD além de prever os requisitos para que os dados anônimos, pessoais e sensíveis sejam tratados, determina, em seu art. 15, I, que ocorrerá o término do tratamento de dados pessoais quando verificado que a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada (BRASIL, 2018).

Também o art. 16° da LGPD dispõe que os dados pessoais sejam eliminados após o término do referido tratamento, no âmbito e nos limites técnicos da atividade, ressalvando-se a possibilidade de sua conservação para determinadas finalidades previstas na normativa. Afora a eliminação decorrente do próprio tratamento, o art. 18°, IV, da novel legislação garante o direito ao titular de dados de, a qualquer momento e mediante requisição, obter do respectivo controlador a anonimização, bloqueio ou eliminação dos dados pessoais tratados com o consentimento do mesmo. Com exceção para as hipóteses previstas no art.16 da lei, sendo, a correção de dados que sejam incompletos, inexatos ou desatualizados (Art. 18, III), dentre outros (BRASIL, 2018).

Nessa senda, insta dizer que, se uma informação se encontra desatualizada e causando danos à pessoa a quem se refere, bem como inexiste interesse público para que tal informação continue sendo veiculada. Pois, tal dado além de ter cumprido a sua finalidade, qual seja, a de informar, também é desnecessário e excessivo, razão pela qual o titular do dado pessoal poderá requerer a eliminação da informação, inclusive aos provedores de pesquisa, haja vista que estes também realizam tratamento de dados, conforme já ocorre na Europa.

Portanto, a Lei 13.709/2018 traz uma previsão que se aproxima à do RGPD da União Europeia no tocante ao apagamento de dados. Por conseguinte, se na Europa é possível solicitar a eliminação de provedores de busca com base no art. 17 do RGPD, a mesma solução também pode ser adotada no Brasil (BRASIL, 2018).

Com relação ao direito a eliminação de dados supracitado, que já integrava o rol de direitos do usuário no Marco Civil da Internet, Voss e Castets (2016, p. 298) afirmam que se trata de uma das cinco categorias abrangidas pelo direito ao esquecimento, dentre outras como, o direito de reabilitação - que seria o direito ao esquecimento do passado judicial; o direito de desindexação – a exclusão dos resultados de busca dos provedores de pesquisa de *hiperlinks* que direcionam os usuários a páginas da internet que apresentem conteúdos irrelevantes ou desatualizados; o direito à obscuridade – pelo qual as informações não seriam apagadas ou desindexadas, contudo, seriam aplicadas técnicas a fim de dificultarem que os dados fossem encontrados na rede, de modo que os mesmos ficassem obscuros e; o direito ao esquecimento dos dados recolhidos na sociedade da informação – pelo qual as informações compartilhadas teriam uma data de expiação.

A despeito disso e reconhecendo-se que o direito à desindexação, como a principal forma de efetivação do direito ao esquecimento na contemporaneidade, em conformidade com a definição estabelecida por Fortes (2016, p. 186), adequada à designação adotada pela RGPD da União Europeia, que compreende o direito do titular de dados pessoais de deletar tais dados no âmbito da internet dentro da esfera de abrangência do direito ao esquecimento, se entende que o artigo 18, VI da LGPD contempla o reconhecimento do direito ao esquecimento no que tange a sua categoria que contempla o direito à desindexação.

Logo, o ordenamento jurídico pátrio, contempla o reconhecimento do direito ao esquecimento enquanto um dos aspectos do direito à autodeterminação informativa, ainda que possa ser discutível a efetividade desse direito, uma vez que somente a entrada em vigor da LGPD definirá bases legais mais claras para a aplicação de tal direito.

No entanto, importa salientar que incorre em um imenso desafio para os controles normativos, o fato de que as técnicas de vigilância tem potencial para invadir todos os espaços, assim, tornando o passado visível, de modo a custodiar

os nossos comportamentos a uma implacável memória, inclusive pela viabilidade de controles de localização e das possibilidades ininterruptas de produção de perfis dos mais variados tipos, sendo que o direito ao esquecimento se encontra sob o permanente risco de eliminação na era informacional (RODOTÀ, 2008, p. 239).

Quanto aos direitos listados no art. 18 da LGPD, especialmente os direitos de anonimização, bloqueio ou eliminação de dados excessivos tratados com ou sem o consentimento do titular, o titular de dados tem garantido ferramentas que podem ser invocadas visando o cumprimento de tais direitos. Nesse sentido, o titular de dados pessoais deverá formular um requerimento expresso endereçado ao agente de tratamento, que poderá acolher o pedido ou negá-lo, comunicando que não é o agente responsável pelo tratamento e indicando as razões que impedem a adoção das providências solicitadas nos termos dos parágrafos 3º e 4º (BRASIL, 2018).

Ademais, o titular tem o direito de peticionar em relação aos seus dados contra o controlador perante a ANPD e pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento do disposto na Lei 13.709/2018 (Art. 18°, parágrafo 1º). Tal disposição confere ao titular de dados, a possibilidade de buscar o comprimento dos direitos previstos na normativa por via administrativa. Os dados pessoais serão armazenados em formato que favoreça o exercício de direito desse acesso. (Art. 19, parágrafo 1º) (BRASIL, 2018).

Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da ANDP, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento (Art.19, parágrafo 3º) (BRASIL, 2018).

Destarte, atualmente, começa-se a desenvolver as normas de proteção de dados para além do consentimento do titular, visto que a própria LGPD prevê diversas outras bases legais para o tratamento de dados ser reputado enquanto legítimo conforme visto anteriormente. Nesse enquadramento, ressalta-se a proteção de dados com base no princípio do *accountability*[11], ou seja, não mais

[11] Tendo em vista as falibilidades reputadas à proteção de dados com foco no consentimento do titular, sobretudo, ao se considerar a tendência atual para manifestações de inteligência artificial

com foco no controle pelo titular, por meio do direito à autodeterminação informativa, mas com foco nas empresas e demais pessoas jurídicas que lidam com o tratamento de dados, sendo necessária a observância da responsabilidade e da ética digital (CANTARINI, 2020).

Nessa continuidade, a LGPD dispõe em seu artigo 20 que o titular de dados tem o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetam seus interesses. Assim, sendo incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo ou de crédito ou os aspectos da sua personalidade. Ainda, prevê a possibilidade de a ANPD realizar auditoria acerca de aspectos discriminatórios em tratamento automatizado de dados pessoais (Art. 20, parágrafo 2º). Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo (Art. 21).

Quanto ao direito de revisão automatizada previsto no artigo 20 da lei, importa salientar que a possibilidade de tal revisão ser feita através de máquina, difere do que dispõe o direito europeu que em seu artigo 22, 3. Pois, o RGPD prevê que nos casos em que se referem às alíneas a e c do n.2, o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. Portanto, a previsão nos termos da LGPD da revisão humana se trata de mera faculdade, sendo possível afirmar que tal previsão afeta o direito de revisão.

Ao contrário da LGPD, o regulamento da União Europeia quanto à proteção de dados, dispõe sobre a possibilidade do titular de dados opor-se à decisão gerada artificialmente, nos termos do Considerado 71, bem como do artigo 22, 1, caso afete os interesses do mesmo. O artigo 22,1 prevê que: “O titular de dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com

---

(AI), surgem as normas de proteção de dados com fundamento no princípio do *accountability* ou responsabilização. Tal proteção tem como foco a responsabilidade das empresas e demais pessoas jurídicas que operam no tratamento de dados, que devem ter em conta a observância da ética digital, o dever de prestação de contas, bem como, o gerenciamento dos riscos no tratamento de dados. Nessa conjuntura, em 2017 o Parlamento Europeu publicou o Relatório sobre robótica e inteligência artificial (AI), posicionando a necessidade de ser atribuída aos robôs uma “personalidade eletrônica”, dessa forma, reconhecendo que estes são aptos para arcar com a responsabilização reputada aos seus atos.

base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.”.

Tais disposições lacunosas da LGPD remetem a necessidade da adoção e da previsão pela legislação de novos mecanismos, a exemplo de relatórios de impacto, auditoria de algoritmos, códigos de boas condutas, certificações e programas de boa governança que correspondem a ideia de *pricacy by design*[12], uma derivação do princípio de *accountability.*

Além disso, o artigo 41 da LGPD dispõe que ao encarregado são atribuídas as funções de receber reclamações e comunicados dos titulares e da autoridade nacional, prestando esclarecimentos e adotando providências (Art.41, I). Tal previsão assegura ao titular de dados a possibilidade de dirigir-se ao encarregado de proteção de dados (BRASIL, 2018).

Nos termos do Art. 5º, VII da Lei (BRASIL, 2018), o encarregado consiste em pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, o titular de dados e a ANPD. Conforme já citado, na LGPD consta a previsão pelo artigo 18, parágrafo 2º, trazendo o direito de oposição quando do descumprimento das hipóteses de dispensa do consentimento.

Ainda na esteira do princípio *privacy by design*, o Artigo 46 da LGPD dispõe 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.” Essas medidas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018),

Feita essa verificação no que tange aos direitos e garantias do titular, bem como das vias de requerimento na busca pelo cumprimento, importa pontuar críticas em relação à forma tímida, em comparação com outros instrumentos

[12] Trata-se do conceito “privacidade desde a concepção”, que se refere a um modelo de gestão do mercado informacional que considera a possibilidade de implantação de certas ferramentas que viabilizem a redução no que toca ao comprometimento dos dados pessoais nas plataformas digitais. É o caso do uso de ferramentas como as assinaturas digitais ou os pseudônimos digitais, que teoricamente teriam o efeito de ocultar a identidade do usuário. Tal expressão refere à necessidade da observância por parte dos designers do uso da “privacidade desde a concepção” das Coisas, ou seja, dos artefatos técnicos (CAMARA; RODRIGUES, 2019).

normativos internacionais, com que a Lei 13.709/2018 prevê basicamente, nos termos do seu Artigo 50, poucos instrumentos para tal proteção.

Ainda, registra-se acerca da natureza jurídica da ANDP, considerando que nos termos do Artigo 55, a mesma foi vinculada à Presidência da República, seguindo na esteira da proposta da Inglaterra, ao contrário de propostas de autoridades independentes, como ocorre na França (CANTARINI, 2020).

A partir desse ponto se insere a análise em torno da criação da Autoridade Nacional de Proteção de Dados e de um Conselho de Proteção de dados, que foram inicialmente vetados no ato de sanção da LGPD, nos artigos 55 a 59, sob a alegação da existência de um vício de iniciativa, que violava o Artigo 61, parágrafo 1º, II, e cumulado com o Artigo 37 da Constituição Federal. (BRASIL, 2018),

O texto legal que desde o início referia mais de 40 hipóteses em que a autoridade é chamada a atuar, sendo fortemente influenciado pelo RGPD europeu, demonstra ser o órgão o seu pilar de sustentação, sem o qual todo o arcabouço normativo e principiológico não está apto ao funcionamento adequado (MENDES; DONEDA, 2018).

Em face do veto à ANPD, após a edição da Medida Provisória nº 869/2018, foi sancionada a Lei 18.853, de 8 de julho de 2019 que veio a alterar a LGPD em diversos pontos, inclusive, ao dispor sobre a criação da ANPD, órgão da administração pública federal, responsável por zelar pela aplicação da Lei. Sendo assim, de modo a exercer a fiscalização no tocante ao tratamento de dados e a aplicação de sanções em caso de tratamento de dados realizado em descumprimento à legislação, bem como editando regulamentos e procedimentos acerca da proteção de dados pessoais e privacidade nas hipóteses não especificadas na legislação. Além de orientar a sociedade sobre a aplicação da Lei e receber demandas sobre violações às normas de proteção de dados (BRASIL, 2019).

Insta dizer que se cogita, neste estudo, a defesa da necessidade de que a ANDP seja, de fato, uma autoridade independente, para a prevenção contra possíveis ingerências ou interferências arbitrárias por parte do Poder Executivo, garantindo com isso a indispensável autonomia e o equilíbrio entre os poderes. Pois, a vinculação do órgão de controle brasileiro ao Poder Executivo, mais precisamente à Presidência da República, obsta a sua liberdade de atuação, em

que pese a lei garanta uma “[...] autonomia técnica e decisória ao órgão.” (Art. 55B.) (BRASIL, 2019).

Tais críticas desembocam na conclusão de que a estrutura atual da ANPD não possui independência para desempenhar de maneira satisfatória suas funções, sobretudo, quando se tratar de fiscalizar o Poder Público (BRASIL, 2019).

Na concepção de Parentoni, embora exista consciência de que esse não é o modelo ideal, é preciso considerar que esse é o modelo possível no atual contexto do país, sendo que a própria LGPD (art. 55-A, parágrafos 1º e 2º) reconhece essa estrutura como transitória, devendo ser reavaliada após dois anos, para possível conversão em autarquia. Logo, seu êxito dependerá mais da habilidade dos primeiros diretores, ao se exigir que sejam aprovados pelo Senado Federal antes da nomeação, como também a Lei reforça o perfil técnico dos mesmos (art. 55 - D, parágrafo 2º). O autor ressalta a necessidade de observar a relação entre a LGPD e as leis conexas à proteção de dados pessoais, como o CDC e o Marco Civil da Internet e a Lei de Acesso à Informação (Lei nº 12.527 de 2011) (PARENTONI, 2019, p. 211).

Com isso, adentra-se na análise do critério do tratamento de dados pelo Poder Público, disposto no capítulo IV da LGPD, um de seus pontos mais relevantes, tendo em vista que o setor público, em seus poderes Executivo, Legislativo e Judiciário e entes federativos, sendo União, Estados, Distrito Federal e Municípios, se valem do tratamento de dados pessoais dos cidadãos. Isso, não apenas para a elaboração e execução de políticas públicas, mas também para o oferecimento dos mais diversos serviços.

Assim, o uso das TICs e das técnicas de tratamento de dados tem sido cada vez mais vistos pela administração pública como importante ferramenta para a gestão pública de forma global. No Brasil, destacam-se os Programas de Governo Eletrônico[13] e as experiências com as chamadas cidades inteligentes.

Nessa senda, a transparência dos dados em mãos do Poder Público, foi regulamentada na Lei de Acesso à Informação e tem um dos seus limites na

[13] Em suma, faz referência ao uso das TICS tanto nos processos internos de governo, como na entrega dos produtos e serviços do Estado para os cidadãos, bem como, em sua relação com as demais organizações públicas e privadas. Visa possibilizar um sistema operacional ininterrupto, capaz de fornecer aos cidadãos acesso à informação e serviços de forma satisfatória. São exemplos de ferramentas utilizadas os portais de internet com fóruns, a exposição de bancos de dados, inclusive para prestação de contas, assim como os aplicativos para telefonia móvel.

vedação ao fornecimento de dados pessoais pelo Poder Público. Desse modo, o artigo 31 da LAI dispõe que “O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais [...] § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.” (BRASIL, 2011).

Dessa forma, o capítulo IV da LGPD faz expressas menções à LAI, conforme dispõe em seu Artigo 23 “o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do Artigo 1º da Lei 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: (parágrafo 1º) sejam informadas as hipóteses em que, no exercício de suas competências, realizarem o tratamento de dados pessoais, providenciando informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos. Ainda, prevê (parágrafo terceiro) que seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais (BRASIL, 2018).

Para disciplinar o tratamento de dados pessoais efetuado por empresas públicas e sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no Artigo 173 da Constituição Federal, o Artigo 24 da LGPD dispõe que ambas terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares. O parágrafo único prevê que, quando as empresas públicas e as sociedades de economia mista estiverem operacionalizando políticas públicas, no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e as entidades do Poder Público (BRASIL, 2018).

Dessa forma, é possível afirmar que um banco público no tratamento de dados pessoais de seus correntistas terá o mesmo tratamento de um banco privado. Contudo, quando este banco público estiver operacionalizando políticas públicas no âmbito da execução delas, terá o mesmo tratamento dedicado pela LGPD aos órgãos e às instituições do Poder Público.

Será o caso da Caixa Econômica Federal, em algumas situações, sendo que, quando atuar como um banco, tratando dados de seus correntistas para, por

exemplo, oferecimento de um financiamento, deverá seguir as regras aplicáveis ao setor privado. De outra banda, ao tratar dados pessoais no âmbito do FGTS, do Programa de Integração Social (PIS) ou do Seguro-Desemprego, deverá observar as regras aplicáveis ao setor público (BRASIL, 2018).

Com relação ao uso compartilhado de dados pessoais pelo Poder Público, o Artigo 26 da LGPD dispõe que deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art.6º da Lei. Nesse sentido, se percebe que o tratamento de dados pessoais é entendido pelos órgãos públicos como uma ferramenta importante para orientar os processos de planejamento, resposta e avaliação de políticas e intervenções públicas (BRASIL, 2018).

O mesmo se aplica inclusive acerca das medidas de monitoramento implantadas visando o contingenciamento da pandemia do Coronavírus. Contudo, apesar da tentativa de construção de uma narrativa de aceitação do uso desses dados, percebe-se a necessidade de um maior diálogo sobre tais processos, em que pese se revelarem, por vezes, instrumentos idôneos para o tratamento de dados sensíveis.

Desse modo, a construção de mecanismos de governança[14] pode se mostrar um fator chave para o uso equilibrado dos dados pessoais. Porém, o descuido com a dimensão da governança potencializa o risco das operações de compartilhamento de dados referidas no Artigo 26 da Lei, considerando que a ANDP não se encontra operacionalizada durante parte da citada crise (BIONI et al, 2020).

Ainda, para disciplinar o tratamento de dados pessoais que possuem acesso público a LGPD em seu Artigo 7, parágrafo 3º prevê a necessidade de observância da finalidade, da boa-fé e do interesse público que justificaram sua disponibilização. Nesse ponto, a Lei estabelece uma distinção entre os dados considerados públicos e os dados “tornados manifestamente públicos pelo titular, os quais dispensam a exigência do consentimento (parágrafo 4º), o que não afasta

[14] Conforme o Decreto nº 9.203, de 22 de novembro de 2017, governança pública consiste em um “conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.

a necessidade de observância dos princípios gerais do tratamento dos dados pessoais e da garantia dos direitos do titular, nos termos do parágrafo 6º do mesmo artigo (BRASIL, 2018).

Com relação a transferência de dados para o setor privado, o parágrafo 1º do artigo 26 proíbe o Poder Público de transferir para entidades privadas os dados pessoais existentes em bancos de dados a que tenha acesso, excetuando, no inciso III, os casos em que os dados forem acessíveis publicamente (BRASIL, 2018). A esse respeito, observa Bioni, que a análise da (i)legalidade do tratamento será definida com base na finalidade e no interesse público que justificaram a divulgação pública dos dados a partir de uma análise contextualizada (BIONI, 2019, p. 270).

Nessa sequência, quanto à responsabilidade civil do Poder Público pelo tratamento de dados, importa considerar que o Artigo 42 estabelece uma cláusula geral de responsabilidade civil, indicando que “O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”. Nessa direção, o Artigo 31 dispõe que a ANDP poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto acerca da proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público (BRASIL, 2018).

Por fim, após uma variedade de adiamentos acerca da data de vigência da Lei 13.709/2018 desde sua edição, no dia 26 de agosto de 2020 o Senado aprovou a MP 959/2020 com a supressão do seu Artigo 4º, que tratava da prorrogação da Lei. Desse modo, a LGPD passou a depender da sanção presidencial para vigorar, em que pese haver discussões acerca da sua eficácia e retroatividade nessa conjuntura. Então, o presidente Jair Bolsonaro sancionou no dia 17 de setembro de 2021 a Medida Provisória 959, a fim de autorizar da entrada em vigor da LGPD.

Contudo, as sanções administrativas previstas na normativa de competência exclusiva da ANPD, serão aplicadas somente em agosto de 2021, sendo que tal adiamento se deve ao Projeto de Lei nº1179/2020, que culminou na Lei 14.010/2020. Nessa senda, finalmente foi publicado o Decreto 10.474/2020

que dispõe sobre a criação da ANPD, sendo vinculada a Presidência da República, conforme previsão anterior.

Dessa forma, é possível afirmar, para além das incertezas, que os titulares de dados passarão a serem assistidos, no que toca, sobretudo, ao direito à autodeterminação informativa na esfera judicial. Fato é que tal direito já configura na sociedade europeia desde a década de 70, contudo, ainda se encontra em fase de construção no Brasil, o que reforça a necessidade de haver acordos entre os controladores e a ANPD para se propagar da melhor maneira possível uma cultura de proteção de dados.

3 O PODER DA VIGILÂNCIA E A APLICABILIDADE DAS ANÁLISES COMPUTACIONAIS PREDITIVAS

Uma questão relevante, no contexto contemporâneo e global, permeado pelo aparato tecnológico, pela vigilância contínua e pelas análises algoritmas e seus efeitos preditivos no comportamento individual e coletivo, se refere à capacidade ou pela falta desta que a sociedade civil possui de permanecer independente em suas convicções. Isso, tanto na vida privada como na vida social, em face desses novos fatos. Todavia, o advento tecnológico inova, mas não cria ou inventa práticas de injustiça, tendo aptidão apenas para potencializar formas de injustiça já recorrentes na trajetória da civilização humana, sobretudo, no viés econômico.

Dando seguimento a pesquisa, parte-se para a análise do panorama das "Coisas" conectadas, uma vez que, tal fenômeno reforça ainda mais a necessária reflexão sobre o direito à privacidade ressignificado no direito à proteção de dados. Nesse sentido, importa procurar respostas acerca do presente e do porvir, diante desse tempo imerso em mudanças e incertezas suscitadas pelo veloz e aparentemente indomável avanço tecnológico e, pelas consequências advindas desse "progresso", que desafiam a compreensão até mesmo em uma sociedade da informação e do Direito que a rege.

Nessa conjuntura, se encontra em curso uma nova lógica de acumulação, que pode ser denominada por (Zuboff, 2018, p. 25) "capitalismo de vigilância, da qual o *Big Data* é tanto uma condição como uma expressão". Tal lógica é compartilhada por *Big Techs* como o *Facebook* e a *Google,* parecendo ter influenciado parte significativa das *startups on-line* e demais aplicativos. Pois, a mediação[15] por computador impacta de forma ininterrupta a economia, de modo a torná-la mais ausente quanto às reciprocidades tradicionalmente estabelecidas entre as empresas e seus usuários.

Dessa forma, é possível afirmar que a tecnologia, por vezes, parece estar se tornando mais importantes que a Lei. Por isso, neste capítulo, em um primeiro momento, serão investigadas as respostas doutrinárias a respeito da construção,

[15] Acerca da constatação de que a mediação por computador impacta de forma ininterrupta a economia, importa referir o conceito de comércio eletrônico, que nada mais é do que toda a atividade consumerista que se utiliza da troca de informação e dados por meio do espaço virtual propiciado pela internet.

em curso, de uma nova forma de poder, em face das análises computacionais preditivas que rompem com o Estado de Direito e com a liberdade alcançada por este.

Nesse contexto, inexiste possibilidade de fuga, não há lugar para estar onde a mediação por computador não está, o poder é identificado com a propriedade dos meios de modificação comportamental, como afirma Zuboff (2018, p. 45). Desse modo, almeja-se obter elementos para a análise crítica do tema, de forma a responder satisfatoriamente ao problema de pesquisa.

Em um segundo momento, será analisado o caso *Cambridge Analityca X Facebook,* que ilustra acerca de uma afronta às práticas democráticas favorecida pela vigilância *on-line*. Trata-se de uma empresa conduzindo análises de dados pessoais da população norte americana em larga escala, sem consentimento, por meio da obtenção de informações provenientes do *Facebook*, com o escopo de persuadi-la a votar em Donald Trump. Tal fato esclarece sobre a aplicabilidade das análises computacionais preditivas, sobretudo, se utilizando de mensagens focadas para suscitar a modificação de comportamento em humanos.

3.1 A REVITALIZAÇÃO DA IDEIA DE VIGILÂNCIA EM FACE DA INSERÇÃO DA INTERNET DAS COISAS (OIT)

O uso da internet enquanto ferramenta dedicada a coletar e analisar os dados pessoais presentes nesse meio, de forma a dificultar a capacidade jurídica de regulamentação adequada para acompanhar tais processos, expandiu-se ao ponto de acomodar o chamado *Big Data*. Com isso, foi possível sistematizar quantidades antes inimagináveis de dados em diferentes formatos, seja texto, foto, vídeo, em alta velocidade. Pois, tal tecnologia viabiliza a eliminação da etapa prévia de estruturação dos dados, sendo possível correlacionar uma série de dados e estabelecer relação entre eles para desvendar padrões de maneira simultânea (BIONI, 2019, p. 35).

Desse modo, o *Big Data*, a custos extremamente baixos, é diuturnamente alimentado pela sociedade da informação, por meio das navegações na *web*, pelas trocas de *e-mails*, das múltiplas intervenções nas redes sociais e aplicativos e, também, pelos objetos conectados à internet, cada vez mais numerosos. As informações que se podem extrair dessa tecnologia são de uma diversidade

ilimitada, abarcando diferentes finalidades. Ao contrário de seus baixos custos de funcionamento, o tratamento de dados que este sistema opera, atinge um alto valor, pois constitui parte fundamental do modelo de negócios atrelado ao conceito ainda em construção de quarta revolução industrial (FERRY, 2018, p. 168).

A quarta revolução industrial teria iniciado na virada do século XXI a partir da revolução digital sendo caracterizada, sobretudo, por uma internet móvel e ubíqua, por sensores e dispositivos cada vez menores e barateados e, pelo desenvolvimento da inteligência artificial. Exemplos desse fenômeno são as fábricas completamente automatizadas, que funcionam sem a interferência humana direta. Além disso, tal conceito implica a fusão dos mais diversos tipos de tecnologias, em seus domínios físicos e digitais, entre elas, a chamada internet das coisas (OIT) (MAGRANI, 2018, p. 80).

Nesse cenário, atores públicos e privados têm atribuído aos fluxos informacionais um enorme valor, sendo que os dados e as informações coletadas se comunicam, transitando entre diferentes agências, não raro, por motivos alheios aos que motivaram sua revelação. Tal movimento de troca pode ser identificado entre governos, cujo objetivo consista em adquirir informações para a tomada de decisões políticas locais ou internacionais e, também, entre empresas que objetivem, além de estudar os consumidores, distinguir o que as empresas concorrentes estão fazendo para obter a atenção deles.

Trata-se de um fenômeno que implica em fluxos informacionais disponibilizados na rede mundial de computadores que virão a ser alvo de tratamento, sendo posteriormente negociados pelos atores que detêm a gerência sobre a arquitetura da rede, dada a sua complexidade. Com vistas à lucratividade e mediante o interesse de atores privados ou públicos em obter tais informações para diferentes usos, esse negócio ilustra acerca do implacável alcance da vigilância na contemporaneidade, bem como, das incertezas quanto às consequências sociais advindas dessa conjuntura.

Nessa senda, os *cookies* são elementos chaves para a compreensão da dimensão da vigilância no tocante à internet, sendo arquivos utilizados por sites visitados com o intuito de salvar as informações provenientes do acesso do usuário no próprio computador deste, por meio do navegador. Tal tecnologia teve início com o fim de possibilitar obterem-se informações com o objetivo de identificar as preferências do usuário e proporcionar uma experiência de

navegação customizada, bem como facilitar o trânsito de dados entre diferentes páginas de um mesmo site ou entre diferentes sites (ALVES, 2018).

Portanto, as inovações inerentes à internet acarretam impactos de ordem social, política e econômica, sobretudo, oferecendo oportunidades e ameaças em face do desafio de lidar adequadamente com os dados pessoais. O devido argumento se reforça com a implementação de uma nova economia chamada colaborativa, simbolizada pelos aplicativos que tecem vínculos entre particulares no modelo Uber[16]. Tais empresas, aparentemente, desinteressadas coletam, o tempo todo, uma infinidade de dados sobre o modo de vida dos usuários, os quais revendem a preços exorbitantes a outras empresas, sendo essa uma das principais fontes de valor do *Big Data* (FERRY, 2018, p. 81).

Acerca desse grande volume de dados e das sofisticadas ferramentas das TICs, é que, nas reflexões de Foucault, sobre o conceito de governamentalidade, nasceu a ideia de governamentalidade[17] algorítmica que, em suma, consiste em uma estratégia de governo por meio de algoritmos que viabiliza uma gestão de condutas que se vale das novas TICs. Desse modo, nas sociedades contemporâneas, os algoritmos são cada vez mais relevantes em termos de tecnologia de governo. Para ilustrar tal fato, considerem-se alguns serviços atualmente oferecidos pelo *Google, Facebook, Amazon* e pelo *Uber*, os quais, cada vez mais, influenciam, direcionam e afetam escolhas e condutas de forma global.

Nessa lógica, os dados coletados sequer precisam ser relevantes, pois a importância decorre do uso do algoritmo adequado, sendo inquestionável a

---

[16] Uber com o uso do trema faz referência a uma palavra de origem alemã, cujo significado é idêntico a “above” (acima, em cima ou sobre, tendo em vista a tradução para o português). Todavia, na linguagem do inglês americano a palavra sofreu algumas alterações de forma a se tornar uma gíria. Dessa forma, seu significado em inglês varia entre o super, o máximo, o melhor, o top. É o nome Trata-se da designação de um dos aplicativos de transporte particulares mais utilizados no mundo. (TECHTUDO, 2019).

[17] Foucault (1979, p. 291-292) atribui ao termo governamentalidade pelo menos três significados, sendo: “1. o conjunto constituído pelas instituições, procedimentos, análises e reflexões, cálculos e táticas que permitem exercer esta forma bastante específica e complexa de poder, que tem por alvo a população, por forma principal de saber a economia política e por instrumentos técnicos essenciais os dispositivos de segurança. 2. a tendência que em todo o Ocidente conduziu incessantemente, durante muito tempo, à preeminência deste tipo de poder, que se pode chamar de governo, sobre todos os outros – soberania, disciplina, etc. – e levou ao desenvolvimento de uma série de aparelhos específicos de governo ou de um conjunto de saberes. 3. o resultado do processo através do qual o Estado de justiça da Idade Média, que se tornou nos séculos XV e XVI Estado administrativo, foi pouco a pouco governamentalizado”.

onipresença de dispositivos capazes de coletar dados sobre o usuário e o ambiente onde se encontram instalados. Na realidade, a maioria dos aparatos eletrônicos, ainda que não possam ser conceituados como sensores, desdobram-se como tal, pois possuem sensores que melhoram a experiência do usuário e otimizam a funcionalidade do equipamento, é o caso dos giroscópios e sensores de proximidade, de movimento, de luz, de umidade e de campo magnético presentes na maioria dos smartphones (MENEZES NETO; MORAIS, 2018).

Assim, beneficiados pelas TICs, novos processos, que podem ser designados sob o acrônimo NBIC: nanotecnologia, biotecnologia, informática (*big data*, internet das coisas) e cognitivismo (inteligência artificial) se desenvolvem de forma plena atualmente. É importante salientar que se trata de inovações radicais o suficiente para fomentar mudanças impactantes em um período extremamente abreviado, acarretando transformações na sociedade, na medicina, na economia e em outras áreas de uma forma ainda não vivenciada pela humanidade (FERRY, 2018, p. 29).

Então, importa se refletir acerca de quais são os limites éticos no uso da OIT, pois, para além do crescimento exponencial dos smartphones que corroboram para a onipresença do ambiente virtual, tal tecnologia suscita que os mais variados objetos estejam conectados à internet. De acordo com Magrani (2018, p. 15), OIT “é a expressão que busca designar todo o conjunto de novos serviços e dispositivos que reúne ao menos três pontos elementares: conectividade, uso de sensores e capacidade computacional de processamento e armazenamento de dados”.

Nesse cenário, onde a OIT se desenvolve e se complexifica, avulta-se o volume imenso de dados que trafegam globalmente em um fluxo dinâmico e ininterrupto, sendo que as decisões são tomadas, cada vez mais, com base nesses dados. Assim, o aumento exponencial da utilização dos dispositivos conectados já existentes ou em véspera de adentrarem no mercado, acarretam riscos para a privacidade e para a segurança dos usuários. Com isso, ressalta-se a importância de se garantir a veracidade das informações divulgadas, inclusive em detrimento das chamadas *fake news*, acentuando-se a necessidade de regulação responsável no que toca ao uso da OIT para a proteção dos direitos fundamentais.

Vale notar que a realidade da IOT solidifica a questão da datificação da vida, ou seja, o ser humano cada vez mais terá sua existência por meio de um prolongamento e de uma projeção completa de seus dados no ambiente virtual. Dessa forma, muitos aspectos da vida de uma pessoa poderão ser decididos a partir da sua extensão eletrônica, o que problematiza ainda mais o desafio da tutela dos dados pessoais como um novo direito da personalidade. Logo, a vigilância, inicialmente associada a partir dos rastros deixados no ambiente *on-line,* é transposta para o mundo físico por meio dos objetos presentes no cotidiano do ser humano, se tornando ainda mais intrusiva e opaca (BIONI, 2019, p. 85-87).

Cabe pontuar, que todo o tratamento de cada dado deve ser considerado como referente ao corpo em seu conjunto, portanto, a uma pessoa que deve ser respeitada na sua integridade física e psíquica. Trata-se de uma concepção integral da pessoa, cuja proteção no mundo corresponde o direito ao pleno respeito de um corpo concomitantemente físico e eletrônico. Dessa forma, o direito à autodeterminação informativa, como ocorreu com o *habeas data*, torna-se um elemento indissociável da civilidade. Então, a reflexão sobre a proteção de dados representa uma passagem indispensável para a compreensão do ser humano no futuro, bem como para definir as novas características que a democracia passa a assumir em face do paradigma informacional (RODOTÀ, 2008, p. 241).

Assim sendo, para além da captação em *bits* do ser humano, com base em tais informações, ocorre a sua classificação e segmentação. Trata-se de verdadeiros estereótipos de modo a estigmatizar um sujeito perante seus pares, implicando em uma série de decisões que influenciam o rumo de suas vidas. Tanto a diretiva da UE de proteção de dados, como a LGPD, traz como objeto de abordagem expressa as decisões automatizadas, sendo que a partir de dados pessoais, pode repercutir ou não oportunidades sociais no contexto de uma sociedade e economia movida por dados, onde as pessoas datificadas seriam as potenciais vítimas dessa estrutura (BIONI, 2020, p. 87).

Segundo os estudos cunhados por Bauman (2013), o processo de tomada de decisão nesse tempo, mediante o paradigma informacional, caminha para uma percepção a partir da possibilidade de adiaforização, ou seja, da exclusão da categoria de ações sujeitas à avaliação moral. Sendo que os objetos inteligentes podem vir a desempenhar a função de isentar o operador da culpa, por exemplo, um *drone* não tripulado que seleciona seus alvos ao assumir a tarefa de coletar e

processar dados, de forma a isentar da culpa moral seu operador. Nessa esfera, estaria em curso um processo de naturalização do imoral, bem como de ausência de parâmetros de justiça (BAUMAN, 2013, p. 86).

No que concerne a questão da categorização, Eli Pariser aborda como as informações são sistematicamente filtradas e direcionadas, especialmente pelos aplicativos de busca e pelas redes sociais de forma personalizada, sem que o sujeito tenha consciência ou controle sobre tal ação. Esse fato viabiliza a instauração de bolhas digitais favorecendo a perda da alteridade e a erupção de discursos de ódio, sendo que o advento da IOT tende a intensificar essa problemática, ao acentuar de forma relevante tais fluxos (PARISER, 2012, p.14-20).

Portanto, a rede oferece universos distintos de acordo com a categorização que atribui a cada um de seus usuários, por meio de ferramentas de rastreamento pessoal instaladas nos recursos *on-line.* Com isso, a base de dados consiste em um braço para peneirar, separar o que se quer do que não se quer, por exemplo, os migrantes desejáveis dos indesejáveis. Logo, quando se reputa tais populações, as fronteiras estão em toda a parte, pois a capacidade de ação remota possibilitada pela tecnologia está presente em todas as formas de decisão que possam ser relevantes para as oportunidades de vida nas diferentes sociedades (BAUMAN, 2013, p. 88).

A respeito das IOT, prevê-se que, em um futuro próximo, o número de Coisas conectadas se expandirá de forma relevante no mundo. Tais Coisas pretendem, portanto, coletar bilhões e bilhões de dados sobre todos os sujeitos e temas imagináveis. Entre os eletrodomésticos, por exemplo, cita-se a geladeira que, equipada com diversos sensores, é capaz de perceber que algum produto está acabando, podendo pedir *on-line* os produtos mais usuais, os quais serão entregues sem que o ser humano precise tomar parte dessa tarefa. Logo, possibilidades imensas e aparentemente indispensáveis vão abrir em todas as áreas da vida humana por meio da IOT com a promessa de otimizar a eficiência da sociedade e, ao mesmo tempo, assegurar o bem-estar do planeta (FERRY, 2018, p. 92).

Tal previsão se aplica igualmente ao contexto urbanístico, o que vem dando forma as chamadas cidades inteligentes, nas quais a infraestrutura e os serviços são interligados de maneira supostamente mais racionalizada e eficiente mediante

o emprego integrado de tecnologias com um controle mais inteligente dos fluxos e uma securitização generalizada. Em suma, a cidade inteligente nasce da possibilidade de grandes volumes de dados serem produzidos incessantemente por meio de seus habitantes, mediante uma arquitetura de rede de conexão sem fio, e sensores disseminados nos mais variados objetos (OIT), com sistemas de filtragem e tratamento do fluxo de dados em tempo real (ALVES, 2019).

De igual maneira, essa nova forma de organização social, coloca inquietantes questões acerca do exercício da liberdade humana nesses novos ambientes administrados pela governamentalidade algorítmica que contrasta com o direito à privacidade, entre outros direitos. Pois, quanto mais informações são disponibilizadas, mais transparentes os titulares se tornam para os algoritmos que facilitam a vida, mas que, cada vez mais, são capazes de antecipar condutas e direcionar ações. Nessa realidade, parece sobrar pouco tempo para ações espontâneas, uma vez que as práticas passam a ser governadas mediante o *feedback* dos parâmetros, que indicam os cenários futuros produzidos com base nas predisposições estatísticas de cada perfil (DILEMA das redes, 2020).

Tais algoritmos são opacos ao público, que sofre as consequências das análises preditivas produzidas pelos mesmos sem nenhuma oportunidade de conhecer os processos. Desta maneira, o que está em risco é a viabilidade de manipulação em massa de comportamento por parte de uma empresa ou de um estado, mediante a criação de um presente alternativo que é o único apresentado enquanto verdadeiro o que consiste em uma nítida violação de direitos fundamentais (MENEZES NETO; MORAIS, 2018).

Nessa lógica, Rodotà expõe quanto às transformações das organizações sociais em sociedades de vigilância:

> Tomemos em consideração o tema da igualdade. Estamos assistindo a um progressivo alargamento das formas de controle social, motivado, sobretudo por exigências de luta ao terrorismo. Estamos diante de uma profunda mudança social. A vigilância se transfere do excepcional para o cotidiano, das classes “perigosas” para as pessoas em geral. A multidão não é mais “solitária” e “anônima”: está nua. A digitalização das imagens e as técnicas de reconhecimento facial permitem extrair o indivíduo da massa, individualizá-lo e segui-lo. O *data mining*, a incessante busca de informações sobre comportamentos de cada um, gera uma produção contínua de “perfis” individuais, familiares, territoriais, de grupos. A vigilância não conhece limites. (RODOTÀ, 2008, p. 238).

Nessa lógica, o controle de localização se mostra extremamente relevante, pois se uma pessoa é classificada como muito predisposta a cometer crimes, faz sentido perder sua liberdade de circulação, bem como todas as relativas formas de autonomia individual. À vista disso, cogita-se que a vigilância sofisticada pelas TICs poderia viabilizar que tal punição, ainda que preditiva, se dê, por exemplo, pela inserção de um microchip sob a pele que torne possível a localização a qualquer momento. No entanto, tal forma alteraria a própria natureza humana, em face de um corpo plenamente manipulado pela tecnologia, o que vai ao encontro da ideia de revolução transumanista[18]. Nesse seguimento, Bauman tece a oportuna reflexão:

> Amarremos isso às realidades de vigilância em nossos dias. Cada vez mais os corpos são "informatizados", palavra feia, mas adequada. Em numerosas situações de vigilância, corpos são reduzidos a dados, mais obviamente, talvez, pelo uso da biometria em fronteiras. Porém, nesse caso paradigmático, o objetivo em questão é verificar a identidade do corpo, da pessoa, para permitir que cruze a fronteira (ou não). Só podemos concluir que a informação sobre esse corpo está sendo tratada como se fosse conclusiva na determinação da identidade da pessoa. Se a distinção for mantida, então a pessoa pode se preocupar se a impressão digital ou o escaneamento da íris a registra adequadamente ou não no sistema. [...] Em forma condensada, essa é a história de como a informação desincorporada termina afetando de modo crítico as chances de vida de gente de carne e osso, como migrantes, pessoas em busca de asilo e, assim por diante. (BAUMAN, 2013, p. 124).

Destarte, em um cenário marcado pela hiperconectividade, a interação entre os humanos e as coisas tende a se intensificar. Por isso, faz-se fundamental a compreensão por parte de todos os atores sociais acerca dos temas da governamentalidade algoritma e da datificação da vida, o que é um grande desafio. Segundo Magrani (2018, p. 20), benesses e ameaças devem ter seus efeitos sopesados com moderação, sendo que, ao Direito, cabe não obstaculizar, de modo desmedido, o desenvolvimento econômico ao regular as práticas tecnológicas, portanto, deve coibir abusos e proteger os direitos fundamentais.

[18] De acordo com Ferry (2018, p.1) trata-se de um projeto abrangente de aperfeiçoamento da espécie humana nos aspectos "físico, intelectual, emocional e moral", possibilitado, sobretudo, pela evolução das biotecnologias. Seu principal objetivo é viabilizar uma nova e superior prática terapêutica com capacidade para melhoria ou mesmo aumento no que toca a solução de quaisquer debilidades (patologias ou doenças) ou mesmo pretensões humanas, a exemplo do não envelhecimento.

Dito isso, cogita-se que o desenvolvimento de microchips para implantação em humanos[19], mostra-se enquanto uma hipótese cabível ao se considerar a capacidade futura de vigilância. Pois, após ter sido vinculada a pegadas deixadas no ambiente *on-line,* passou a operar no mundo físico por meio de objetos conectados e, teria sua supremacia demostrada ao se conectar ao próprio titular de dados, dispensando quaisquer meios externos. No entanto, para além de tal tecnologia suscitar a extinção do direito à proteção de dados de forma plena, os riscos para a dignidade humana serão ainda maiores na hipótese de começarem a incorporar dados biológicos nos chips.

Vale notar, que tais microchips já são tendência em países ocidentais como Suécia, Alemanha, Austrália e Nova Zelândia onde há várias iniciativas para promover essa tecnologia futurista. Destaca-se a Suécia, onde milhares de pessoas implantaram o chip RFID na mão e o usam para diversas atividades. Argumenta-se que os microchips consistem em um sistema conveniente, um RFID, ao contrário de um código de barras, permite acesso remoto à informação que contém; possuem o tamanho de um grão de arroz; substituem muitas coisas, como o cartão de crédito ou as chaves; resolve a questão da perda, permitem realizar pagamentos sem contato, uma prática especialmente comum na Suécia, onde apenas 1% do valor de todas as transações é feito com dinheiro.

Tendo em vista que o tratamento desses dados serve tanto a interesses comerciais como a interesses políticos, a questão primordial consiste na ameaça que essa realidade impõe quanto ao respeito à vida privada e a intimidade, uma vez que nada se pode afirmar acerca dos possíveis efeitos, em longo prazo, resultantes desse cenário que pode ser caracterizado pelas interferências virtuais na realidade social. Tais constatações aventam para o risco da extinção do direito à proteção de dados, situar-se enquanto uma das principais ressignificações desse tempo, sobretudo, em face das possibilidades advindas do conjunto de fenômenos ligados à IOT.

Diante de tal realidade, inevitáveis são as repercussões acerca dos efeitos que atravessam a violação dos direitos fundamentais, seja por parte do Estado, ou por parte de particulares, frente às vulnerabilidades desencadeadas pela exploração de dados pessoais. Assim, no que se refere à dignidade da pessoa

[19] BBC.COM, 2020. Disponível em: <encurtador.com.br/lyAX3>. Acesso em: 28 mai. 2020.

humana, que resta intrínseca a preservação do direito fundamental à proteção de dados, vale notar que a ausência de privacidade conduz aos mais variados tipos de insegurança, inclusive jurídica.

Por isso, no capítulo seguinte, busca-se examinar acerca do poder que a vigilância oportuniza para os atores capazes de operá-la, bem como quanto à aplicabilidade suscitada por meio das análises computacionais preditivas. Importa considerar que não é possível conhecer acerca dos usos que tais atores podem fazer de posse desse poder na totalidade, no entanto, é perceptível que o uso da tecnologia para manipular populações é premente, o que favorece o fracasso da democracia.

3.2 A MANIFESTAÇÃO DE UM “NOVO” ESTADO DE EXCEÇÃO NA ERA DIGITAL GLOBAL

A composição de fatos manifestos com veemência na contemporaneidade sejam os rumores de guerra, questões sanitárias, as catástrofes ambientais, a exclusão econômica, demostram um mundo que apesar da presente sofisticação tecnológica se encontra em uma crise muito peculiar. Tal peculiaridade se evidencia em um cenário pós-nacional, forjado, sobretudo, pela intensificação dos fluxos informacionais e mercantis, interdependências político-econômicas e implicações ao fenômeno jurídico, ao buscarem-se soluções para além das instâncias tradicionais (VIEIRA, 2015, p. 163).

Tal contexto restou beneficiado pela revolução informacional que possibilitou a flexibilização das fronteiras estatais, para não dizer a desintegração, evidenciando-se movimentos em direção à necessidade de regulação em favor de certo controle globalizado, ocorrendo um significativo aumento nos pontos de contato entre ordenamentos jurídicos tradicionalmente centrados nas referências estatais, a exemplo das práticas de harmonização normativas econômicas presentes no arquétipo jurídico global atravessado pela mediação por computador.

Nesse sentido, é possível afirmar que a revolução informacional acarretou uma grande transformação a partir do século XX, impactando o modo de vida da sociedade civil e das relações estabelecidas com as instituições que a permeiam, em especial, perante o Estado. Um Estado concebido historicamente enquanto uma área geográfica identificada como possuidora de uma política legítima, capaz

de constituir pelos próprios meios um governo soberano, viu-se permeado pela presença de novos atores em uma nova conjectura de um mundo de fronteiras flexíveis e de riscos impostos à cidadania (NASCIMENTO, 2011, p. 144).

Dessa forma, o Estado, historicamente soberano, teve de submeter-se inicialmente a lógica mercadológica burguesa, por vezes, lançando mão enquanto Estado de direito da proteção dos cidadãos, para fazer aliança com atores econômicos privados, que passaram a ocupar lugar de destaque na era liberal. Nesse sentido, notabilizaram-se as *Big Techs* que, por meio da operação do *Big Data*, transformaram o cotidiano da sociedade global em estratégia de monetização, resultado da transcendente mediação por computador que permeia quase a totalidade dos aspectos do mundo que renasce como dados. (ZUBOFF, 2018, p. 24).

Portanto, avulta-se uma emergente forma de mercado que Shoshana Zuboff (2018, p. 25) denomina de capitalismo de vigilância, demonstrando que essa lógica de acumulação para prosperar demanda um novo uso do território político, inclusive, porque produz predições acerca do possível comportamento humano independente da obtenção de consentimento, com a finalidade de oportunizar meios de controle. Deste modo, tais arranjos manifestam ter potencial para, em um futuro próximo, extinguir com as liberdades individuais obtidas pelo Estado de Direito.

Nessa senda, Giorgio Agamben manifesta que o totalitarismo moderno se revela com a instauração, por meio do estado de exceção, de uma guerra civil legal que permite a eliminação física não somente dos adversários políticos, mas também de categorias inteiras de cidadãos que, por qualquer razão parecem não ser integráveis ao sistema político. “O Estado de Exceção, apresenta-se nessa perspectiva, como um patamar de indeterminação entre democracia e absolutismo” (AGAMBEN, 2004, p. 13). Dessa forma, é possível afirmar quanto ao aspecto meramente formal do princípio democrático em face do núcleo autoritário.

Assim, a possibilidade da democracia é obscurecida e ameaçada pelo estado de conflito que aparentemente se instalou de maneira permanente no mundo. Considere-se que a democracia não passou de um projeto inconcluso ao longo da era moderna, mas o obstáculo básico enfrentado pela democracia é o estado de guerra global econômica (HARDT; NEGRI, 2014, p. 9). Torna-se possível afirmar que devido pensamento explicita questões centrais do mundo

contemporâneo, uma vez que, nem mesmo com os avanços correlatos a uma sociedade informacional, foi possível reduzir o abismo social que segue vitimando ao negarem-se oportunidades análogas entre supostos iguais.

Por isso, é possível afirmar quanto aos riscos e aos perigos que circundam o ideal democrático na esfera das liberdades individuais, representados por um poder que possa ter a sua disposição, de forma ilimitada, a informação acerca do comportamento dos indivíduos a nível global. Sendo que, um enfoque perceptível diante dessa lógica, se refere à imbricação das autoridades privadas e públicas no projeto de vigilância, incluindo reciprocidades e interdependências entre as autoridades de governo do Estado e as *Big Techs* e seus investidores (CARDOSO et al, 2018).

Com efeito, tal imbricação intenta viabilizar as condições necessárias para o desenvolvimento e a operação de meios que oportunizam o controle da sociedade global, a exemplo das plataformas digitais que possibilitam a disseminação de notícias falsas e manipuladoras com uma facilidade sem precedentes e, consequentemente, criam as condições para desestabilizar o tecido social ao redor do mundo. Como resultado dessas práticas, tem-se, sobretudo, alienação, populismos, desinformação e exploração de humanos em um contexto apto a ampliar o abismo social que já é enorme (BAUMAN, 2008, p. 129).

Nesse sentido, as tecnologias de elaboração de perfis são usadas para determinar quem será colocado em vigilância específica, manifestação evidenciada pelo poder excepcional em sociedades liberais expresso por meio de estados de exceção que se tornam rotineiros e, pela elaboração de perfis que excluem certos grupos em função de seu potencial comportamento futuro. Assim, os efeitos do poder e da resistência não são mais sentidos somente entre Estado e sociedade, mas em um movimento global (BAUMAN, 2013, p. 63).

À vista disso, a presente atuação do estado de exceção em contrariedade à previsão legal da excepcionalidade, guarda íntima relação com as formas fluídas de vigilância características da contemporaneidade, conforme explica Bauman (2001, p. 156) “[...] essa é a cara contemporânea da dominação.” Importa salientar que, em oposição ao que se verificava em outras épocas, quando a sociedade civil resistia às formas de controle por parte dos governantes na busca por democracia, atualmente percebe-se uma abertura da mesma a tal domínio em troca das conveniências advindas do aparato tecnológico.

Tal comportamento social conveniente a práticas de distanciamento democrático se justifica pelas benesses que o aparato tecnológico possibilitou nas formas de produzir, de consumir, de se relacionar, de deslocamento de pessoas e bens, dentre outras, ao possibilizar um significativo ganho de tempo capaz de alcançar à instantaneidade. As propostas de controle em diferentes formas seriam justificáveis pelas assimetrias de poder e conhecimento existentes entre autoridades e subordinados ou empresas e usuários e, também na medida em que acabam por condicionar a participação na vida social (BIONI, 2020, p. 25).

Como exemplo da vigência do estado de exceção, tem-se o sistema Detecta utilizado pela polícia do Estado de São Paulo, fornecido pela *Microsoft*. Trata-se de um aparato que conjuga tecnologias de monitoramento e *Big Data* por meio de câmeras inteligentes capazes de reconhecer padrões suspeitos e acionar medidas com o escopo de evitar incidentes ou crimes. Portanto, a partir de padrões comportamentais e não de um saber propriamente dito sobre quem é o suspeito ou os indivíduos potencialmente criminosos. Vale notar que a antecipação possui a prerrogativa de performar o que se previu, realidade que confronta à democracia (GOVERNO DE SÃO PAULO, 2017).

Nessa acepção, a vivência imposta frente ao Coronavírus veio a clarificar com relação a práticas sociais condizentes com o estabelecimento de um novo estado de exceção na era digital. A propósito, para o atendimento dessa demanda sanitária excepcional, o governo brasileiro editou a Lei nº 13.979/2020, que discorre sobre medidas emergenciais no âmbito da saúde em face da disseminação da COVID-19.

Ocorre que o art. 6º e parágrafos do diploma legal dispõem acerca do compartilhamento de dados de saúde entre as instituições da administração pública, em todas as suas esferas, e as pessoas jurídicas de direito privado, sendo que estas, quando requeridas pela autoridade sanitária, igualmente compartilharão informações com a intenção de identificar os contaminados e suspeitos de contaminação pelo vírus. Tal fato culminou com a iniciativa de mapeamento de dados de indivíduos em alguns estados brasileiros, objetivando monitorar o deslocamento dos mesmos para averiguar-se quanto à adesão à quarentena[20].

[20] INFOMONEY, 2020. Disponível em: <https://www.infomoney.com.br/economia/tim-fecha-parceria-com-prefeitura-do-rio-para-rastrear-movimento-e-combater-vírus/>. Acesso em: 23 mai. 2020.

Ao se considerar que se trata de uma crise sanitária global, vários países adotaram medidas consubstanciadas em políticas de ação em combate à pandemia com base em controles realizados a partir da apreensão de dados dos cidadãos. São exemplos: Israel, local onde as empresas de telecomunicações fizeram o compartilhamento dos dados de localização dos dispositivos móveis com as autoridades de saúde[21], e a China que adotou práticas de controle mais diversas e rígidas[22].

Tais práticas chinesas abrangem reconhecimento facial capaz de identificar a temperatura dos indivíduos, uso de *drones* enquanto ferramentas de vigilância na política de *lockdown* e de robôs entregando comida em hospitais, sendo que o país possui o controle informacional de parte significativa da população. Assim, é possível precisar quem são os infectados, quem integra algum grupo de risco, o local de residência e a geolocalização em tempo real destes. Para tanto, os cidadãos chineses recebem um dispositivo com a finalidade de rastrear seus passos e emitir alertas as autoridades caso as determinações do governo não sejam obedecidas[23].

Importa ressaltar que o art.6º da Lei 13.979, ao impor a obrigatoriedade de compartilhamento de dados sensíveis, o faz de forma a suprimir o direito do titular a autodeterminação informativa. Todavia, tal direito não pode ser impedido mesmo nos casos que possibilitam o uso dos dados sem o consentimento do titular, a fim de que o titular acompanhe o fluxo informacional compartilhado e seja partícipe do processo decisório acerca de qual informação é relevante para se atingir o fim almejado. Logo, se percebe uma ausência de transparência e *accoutability* que visem dar nitidez e segurança em tais processos de tratamento de dados (BIONI et al, 2020, p. 23).

Nesse enquadramento, é devida a inquietação acerca da possibilidade pós-pandemia da normalização no tocante a medidas que surgiram como solução apenas para o “estado de exceção”. Tais ferramentas de vigilância já são

---

[21] TECHCRUNCH, 2020. Disponível em: <https://www.techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing>. Acesso em: 26 out. 2020.

[22] SUPER ABRIL, 2020. Disponível em: **<**https://super.abril.com.br/tecnologia/china-esta-usando-tecnologias-de-vigilancia-em-massa-para-combater-coronavirus/>. Acesso em: 26 out. 2020.

[23] BBC NEWS BRASIL, 2020. Como a China usa seu sistema de vigilância para conter coronavírus. Disponível em: <https://www.bbc.com/portuguese/internacional-52129955>. Acesso em: 05 jun. 2020.

regulamentadas no que tange a capacidade de compra e crédito dos consumidores brasileiros. Isso, desde a edição da Medida Provisória 518 que resultou no chamado “Cadastro Positivo de Crédito”, adiante convertida na Lei nº 12.414, que instituiu a criação de um banco de dados para a análise do histórico de créditos dos consumidores, sendo finalmente alterada pela Lei Complementar nº 166 que veio a aprofundar a vigilância na medida em que tornou compulsória a participação dos consumidores no cadastro positivo.

Ainda, é possível referir enquanto faceta desse novo estado de exceção na era digital, o Pix[24] que concerne à nova plataforma de pagamentos do Banco Central do Brasil, que visa realizar transações instantâneas, a qualquer tempo, via *Q R Code* e com baixo custo. Desse modo, pode ser realizada a partir de uma conta corrente, conta poupança ou conta de pagamento pré-paga. Logo, a tecnologia impacta nas formas tradicionais de transacionar valores monetários, oportunizando meios mais ágeis e acessíveis.

Nesse cenário, muitos benefícios estão sendo mencionados, inclusive em torno da segurança eletrônica, uma vez que, com o Pix, não é necessário saber onde o beneficiário da transação possui conta, possibilizando a transferência a partir, por exemplo, de um telefone da lista de contatos do *smartphone* por meio da Chave Pix. Todavia, importa que nesse viés, o Banco Central, ou seja, o Estado, assenhorar-se-á de uma base de dados centralizada sobre as movimentações financeiras dos indivíduos, findando com a burocracia anterior em que o governo precisava solicitar esses dados bancários para diferentes bancos. Realidade que favorece uma variedade de possibilidades referente ao cruzamento desses dados, a qualquer tempo e para diferentes finalidades.

Além disso, embora a inovação prometa a inclusão financeira, se percebe o contrário, pois formas que visem à substituição do dinheiro de papel, que sejam subordinadas a um órgão centralizador, favorecem a exclusão financeira. Tal fato se justifica, na medida em que o dinheiro de papel, por vezes, é a única forma que viabiliza que os indivíduos desprovidos da documentação exigida pela burocracia bancária, possam participar do sistema financeiro. Contudo, trata-se de mais uma tendência tecnológica inafastável, a exemplo das *cripto* moedas, do *PicPay* e de iniciativas de *Big Techs* nesse sentido.

[24] BBC, 2020. Disponível em: <encurtador.com.br/blqKV>. Acesso em: 27 out. 2020.

Imperioso o temor diante da viabilidade de um Estado que controla, de forma ampla, os dados pessoais de seus cidadãos, podendo-os utilizar para propósitos diversos no futuro, sendo que poderá exercer, de maneira arbitrária, o poder procedente desse controle. Tais práticas podem se dar inclusive pelo agravamento de decisões discriminatórias favorecidas por tecnologias de classificação e filtragem (RODOTÁ, 2008, p. 96).

Nessa perspectiva, é possível afirmar que a transparência dos dados pessoais tem sido apontada enquanto solução para as demandas vigentes, no entanto, em que pese os titulares de dados não parecerem se importar com a perda da privacidade, qual a visão destes ao se considerar privacidade como condição para se exercer liberdades individuais?

Por isso, é possível afirmar que esses arranjos descrevem o surgimento de uma nova arquitetura de poder global, conforme Zuboff (2018, p. 42):

> A participação consensual nos valores dos quais a autoridade legítima é derivada, juntamente com o livre arbítrio e os direitos e obrigações recíprocos, é substituída pelo equivalente universal da tornozeleira eletrônica do prisioneiro. A autoridade depende de uma construção social animada por valores fundacionais compartilhados. [...] a autoridade é suplantada pela técnica, o que eu chamo de “dimensão material do poder”, em que sistemas impessoais de disciplina e controle produzem certo conhecimento do comportamento humano independentemente do consentimento. [...] um território político vital para o regime de capitalismo de vigilância.

Importa ressaltar que a vigilância atinge para além da privacidade, sendo preponderante na afetação da dignidade humana, bem como propulsora da segregação social, subjugando quaisquer instrumentos de proteção de dados pessoais frente à realidade que abarca ideias de desterritorialidade e desespacialidade apropriadas à contemporaneidade. Arendt (2006, p. 336) aduz que “o perigo é que uma civilização global, universalmente correlata, possa produzir bárbaros em seu próprio seio por forçar milhões de pessoas a condições que, a despeito de todas as aparências, são as condições da selvageria”.

Contudo, os titulares de dados, por vezes, desconhecem os desdobramentos dessa realidade, portanto, encontram-se sem possibilidades de interferência nos resultados. Ainda que estes signifiquem implicações radicais para suas vidas. Ocorre que dentro do contexto dos avançados algoritmos de extração e análise de dados, os titulares têm pouco ou nenhum conhecimento

sobre como tais dados são tratados e monetizados, o que significa escassas opções de exercerem o direito à autodeterminação informativa. Logo, é possível afirmar que essa nova forma de poder se aperfeiçoa na ignorância do público (CARDOSO et al, 2018).

Uma das esferas importantes onde o estado de exceção é operativo se assenta no fato da proliferação dos dispositivos de segurança biométrica ou sensorial que permeiam cada vez mais todos os aspectos da vida cotidiana, ainda que tenham origem no intuito de reconhecerem-se criminosos reincidentes. Assim, as tecnologias que foram inventadas para animais, criminosos, estrangeiros ou judeus foram estendidas a todos os seres humanos por meio da mediação por computador, possibilitando o uso de *scanners* ópticos para gravar não apenas impressões, mas a retina ou a estrutura da íris ocular (AGAMBEN, 2004).

Assim sendo, apura-se acerca dos enfrentamentos necessários em face da nova relação perceptível entre a sociedade civil, o Estado contemporâneo e as *Big Techs* e seus investidores, que pelo advento da governança por algoritmos têm atuado para uma ampliação no que se refere às formas de subjugar os cidadãos a mera condição de uma massa suscetível de controle. Fernanda Bruno (2013, p. 93) explica que a crescente presença das câmeras de vigilância nos espaços públicos reflete um estado de suspeição generalizada onde todos são suspeitos, até que se prove o contrário.

Sobre essas novas formas de controle social que visam imediatamente à ação e não o sujeito, Agambem adverte:

> E é significativo que semelhante transformação da ordem constitucional, que hoje ocorre em graus diversos em todas as democracias ocidentais, apesar de bem conhecidas pelos juristas e pelos políticos, permaneça totalmente despercebida por parte dos cidadãos. Exatamente no momento que gostaria de dar lições de democracia a culturas e a tradições diferentes, a cultura política do ocidente não se dá conta de haver perdido por inteiro os princípios que a fundam. (AGAMBEM, 2004, p. 33).

Cumpre salientar que tais formas de controle possibilitadas pela tecnologia assumem um formato mais dócil do que as praticadas na sociedade disciplinar[25],

[25] De acordo com Foucault (1976, p. 32) “sociedade disciplinar” refere-se a sociedade moderna surgida no século XVII, que foi fundamentada sobre dois pilares, sendo, de um lado, os sistemas jurídicos herdados da teoria da soberania, e de outro, as técnicas de dominação por meio da disciplina, que eram mascaradas através da ideia então legitimada de um Estado soberano. Dessa forma, possibilitou-se a democratização da soberania, a partir do estabelecimento de um direito

sendo capazes de, ao mesmo tempo, restringir e passar uma falsa sensação de liberdade. É premente que o alcance do controle se distancia cada vez mais dos corpos, para se manifestar nas mentes, uma vez que os dispositivos tecnológicos que controlam se prestam a oferecer conforto, resolver demandas e, sobretudo, ensejam possibilidades de melhoramentos desejáveis na experiência humana.

Esse aspecto da contemporaneidade relaciona-se com a ideia ensejada pelo estado de exceção que reflete a ilegitimidade totalitária. Assim, aplica a lei diretamente na humanidade, sem atrelá-la a sua conduta, esperando que esta engendre a humanidade como produto. Tal finalidade está por trás da pretensão de governo global sendo acalentada por todos os governos totalitários (ARENDT, 2006, p. 514).

Sendo assim, argumenta-se que o sistema de vigilância que caracteriza os governos hodiernos, assim como as *Big Techs* e seus investidores, tem por objetivo máximo atingir um controle de domínio universal. Afinal, as demandas são globais, a exemplo das questões ambientais, dos desdobramentos nocivos do capitalismo econômico, da problemática imigratória, da ameaça terrorista, do combate à corrupção, enquanto que as normas internas demostraram ser incapazes de responder eficientemente. Nesse ínterim, é possível afirmar que a predição algoritma tem sido apontada enquanto solução inevitável para o mundo.

Desta maneira, dados sobre os comportamentos dos corpos e das mentes ocupam lugar de relevância em uma compilação em tempo real de dispositivos conectados que respondem a um domínio global, possibilitando modificar os comportamentos humanos objetivando o lucro e o controle. Nessa lógica, inexiste pessoalidade, apenas o organismo mundial e os seus componentes internos, sendo que o algoritmo entende acerca das possibilidades de futuro e cria as condições para que esse futuro se concretize. Todavia, se uma decisão implica em violência ou discriminação, ela estará invariavelmente errada, ainda que esteja matematicamente correta (CARDOSO et al, 2018).

Acerca das novas bases do poder em face dos desencaixes favorecidos pelo advento da revolução informacional, Manuel Castells (2013, p.29) aduz que "[...] o poder se baseia no *controlo* da comunicação e da informação, seja o macro

---

público articulado a partir de uma soberania coletiva e sustentado pelos mecanismos de coerção disciplinar. As escolas, os hospitais, as prisões, as oficinas, os manicômios e os exércitos estariam entre as principais instituições onde se operam tais mecanismos de coerção, bem como, de produção de saberes, a fim de tornar os sujeitos dóceis e úteis.

poder do estado e dos grupos de comunicação, ou o micro poder de todo o tipo de organizações.” Portanto, resistir ao estado de exceção na era virtual, faz-se uma necessidade primordial da sociedade hodierna, inicialmente através da tomada de consciência sobre os fatos correlatos a sistemas de controle e vigilância que trazem consequências drásticas para os indivíduos.

Assim sendo, o Brasil está prestes a realizar o leilão 5G, pois, em que pese a tecnologia 4G ter oportunizado a conexão entre “todas” as pessoas, a implementação da tecnologia 5G viabilizará a conexão da sociedade global, ou seja, de todas as pessoas e de todas as coisas. Tal fato enseja usos tecnológicos sem precedentes, que podem ser sinalizados pelos carros autônomos, por operações cirúrgicas a longa distância, pela automação industrial, pela interação com hologramas e realidade virtual aumentada.

Nessa senda, a empresa chinesa *Huawei* tem ocupado lugar de destaque enquanto fornecedora da tecnologia 5G, seguida pela sueca *Ericsson* e pela finlandesa *Nokia*. No entanto, os USA a acusam de repassar informações ao Partido Comunista Chinês, sendo que, a embaixada norte-americana no Brasil afirma que a lei chinesa obriga que empresas como a *Huawei* cooperem com os serviços de inteligência, criando condições para monitoramento sem autorização e roubo de informações comerciais, ou seja, espionagem. A *Huawei* nega tais acusações, todavia, permanece inegável que o controle de dados global se encontra na mira de diferentes atores.

Com isso, conjectura-se que as possíveis consequências em face de a contemporaneidade refletir crises que perpassam as fronteiras estatais que a muito já foram flexibilizadas pelo aparato tecnológico, e pela capacidade que tal sistema tem de moldar o comportamento humano, podem revelar a viabilidade de um novo estado de exceção na era digital de alcance global. Fato é que certos atores públicos e privados convergem para assumir uma liderança global que, cada vez mais, poderá vir a ser desejada pela sociedade, diante do cenário de caos existente, de incerteza, insegurança e medo, conforme Bauman (2008, p. 133).

Nessa lógica, segundo Bauman (2013, p. ?) “[...] a categorização social é basicamente o que a vigilância realiza hoje, para o bem ou para o mal”, com tendência a evoluir para a individualização dos vigiados, pois dessa forma tal controle finalmente será pleno. Nessa perspectiva, pode se mostrar oportuna, por

exemplo, uma regulamentação global com viés econômico que disponha acerca da obrigatoriedade de uma identificação mais precisa nos indivíduos, capaz de abarcar os processos de transações monetárias sem quaisquer intermediários.

Dessa forma, percebe-se que a implantação de chips em humanos pode se mostrar o meio mais vantajoso para oportunizar tal identificação, podendo ser legitimada enquanto solução para harmonizar as demandas econômicas. Porém, tendo a finalidade de possibilitar o controle absoluto dos corpos e das mentes. Conforme explica (Rodotà, 2008, p. 95), “Deterioram-se as tradicionais formas de controle social, cujo lugar é assumido, por controles mais penetrantes e globais, tornados possíveis pelo tratamento eletrônico das informações.” Logo, cogita-se da plenitude da mediação eletrônica que é um fenômeno em acelerada expansão. A esse respeito, o autor ainda observa:

> “[...] alguns estudos norte americanos têm sustentado que a passagem de formas concentradas em certos indivíduos e grupos sociais tidos como perigosos para um controle objetivo e universal teria um efeito de “democratização”, pois excluiria qualquer forma de seleção dos indivíduos e, portanto, de discricionariedade. Todos iguais, visto que todos controlados e fichados. A igualdade perante o Estado seria garantida somente pelo abandono de qualquer garantia.” (RODOTÀ, 2008, p. 238).

Assim, considera-se quanto as implicações suscitadas na hipótese de vigorarem tais legislações totalitárias, que viabilizariam o monitoramento ininterrupto e global, de modo que, fatalmente, acabará por suprimir as liberdades individuais. Tem-se como pano de fundo um discurso de benefícios, mas que na prática retrata a máxima do estado de exceção. Nesse cenário, aqueles que não concordarem em aderir a vigilância no corpo, poderão ser considerados contraventores penais. Tais indivíduos poderão ser passíveis de prisão ou de penas mais pesadas nesse contexto. Assim, a supressão da privacidade poderá ter como consequência a total perda das liberdades individuais. Nesse sentido, interessa a observação de Jaron Lanier (2018, p. 144):

> [...] Estamos realmente em tempos excepcionais? A mim parece que algo deu errado e ganhou um caráter sinistro em nosso mundo, e isso aconteceu de repente, nos últimos anos, com a chegada da Bummer. Não é que estejamos vendo horrores sem precedentes – eles têm precedentes -, mas o precioso arco da vitória se reverteu. Estamos degringolando de maneira terrível e repentina.

Dito isso, adiante será investigado o caso *Cambridge Analityca x Facebook*, visto que o fato ilustra acerca da possibilidade da supressão do direito à proteção de dados e do impacto dessa questão para a sociedade, através de um estudo de caso. Nesse sentido, opta-se por um recorte, tendo em vista a sociedade norte-americana nas eleições presidenciais de 2016. Contudo, conforme já se constatou, tais repercussões têm alcance global, mediante a vigilância ubíqua possibilitada em face do paradigma informacional.

3.3 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS RUMO À EXTINÇÃO? PERSPECTIVAS TENDO EM VISTA O CASO CAMBRIDGE ANALITYCA X FACEBOOK

O caso *Cambridge Analytica X Facebook* esclarece sobre as complexidades que atravessam o ambiente virtual, especialmente no que toca as redes sociais, que são um importante braço da comunicação mediada por computadores no âmbito da aplicabilidade das análises computacionais preditivas. É fato que a conexão à internet propiciou meios singulares capazes de oportunizar companhia, verificação de acontecimentos, armazenagem de informações, e até mesmo espécies de terapia na contemporaneidade, onde a informação tornou-se um elemento basilar para o desenvolvimento da sociedade.

Contudo, tais benesses, de forma alguma são gratuitas, sendo possível afirmar que a sociedade, em geral, desconhece como seus dados estão sendo usados contra ela própria. Em suma, trata-se de um modelo de negócios onde os dados dos usuários são a matéria-prima, vendida por um valor que se sobrepõe ao petróleo, aos anunciantes e atores políticos pelas *Big Techs*. Ambos interessados em modificar o comportamento de humanos para obtenção de vantagens. Ressalta-se que tal modelo de negócios concentra muito poder em um pequeno número de mãos que controlam nuvens gigantescas (LANIER, 2018, p. 25).

Acerca da legislação estadunidense, território onde ocorreram tais fatos, considere-se que nos Estados Unidos, país que opera pelo sistema de common law, cuja jurisprudência é a principal fonte de direito, os modelos regulatórios concernentes à proteção de dados pessoais vigoram em maior proporção sob certa liberdade de circulação da informação. (DONEDA, 2006, p. 306).

Desse modo, é possível identificar pelo menos oito instrumentos normativos que tratam da proteção de dados pessoais. Destaca-se o USA Patrioct Act ou Ato Patriota, que vigorou de 2001 até 2015, com a finalidade de reagir aos atentados de 11 de setembro de 2001, cuja essência remete a facilitação do compartilhamento de informações além da colaboração entre as agências governamentais para que pudessem fazer as ligações dos dados pretendidos de forma mais assertiva. É possível afirmar que o governo norte-americano, naquela ocasião, sob o discurso de segurança nacional, impulsionou as ações de vigilância já costumeiras entre pessoas, empresas e governos naquele território (FORTES, 2016, p. 152).

Nessa acepção, a extinta empresa inglesa *Cambridge Analytica*, criada em 2014 pelo SCL *Group*, este atuante desde 1993 na gestão de campanhas políticas e em projetos humanitários e de defesa em mais de 50 países, e o *Facebook,* compartilhavam da mesma visão idealista de proporcionar, ao mundo, conectividade e engajamento. O território em que a C.A almejava se destacar, sendo a política, era até então tido pela organização como inexplorado nesse contexto. Todavia, enquanto corretora e analista de dados, a empresa era apenas uma entre muitas das grandes empresas atuantes no mundo nesse segmento (KAISER, 2020, p. 46-47).

Logo, a C.A constituía-se enquanto mais um ator integrado à economia informacional, considerando que esse negócio abarca práticas governamentais possibilitadas pela cooperação com instituições privadas de análises de dados. Assim, o *Big Data* e a mineração de dados alteram o funcionamento das práticas estatais, trazendo insegurança para a sociedade que se encontra atravessada por uma realidade de vigilância e manipulação que se solidifica no mesmo ritmo dos avanços tecnológicos. Além disso, o *Big Data* e os algoritmos são favorecidos ao serem reputados como uma caixa preta para a sociedade (MENDES; VECHI, 2020, p. 233).

De tal modo, a C.A apresentava-se para seus *prospects* como fornecedora de um serviço revolucionário inerente ao *Big Data* e a análise de dados, considerando o território norte-americano, afirmava possuir um banco de dados de tamanho e escopo sem precedentes. Tratava-se de 2 a 5 mil pontos de dados individuais de todos os cidadãos com idade superior a 18 anos nos USA, cerca de 240 milhões de pessoas. Desse modo, a empresa mostrava-se capaz de operar

formas mais científicas e precisas de categorizar as pessoas e esquadrinhar indivíduos por meio de qualquer aparelho conectado ou mídia concebível (KAISER, 2020, p. 20).

A propósito, os setores de *marketing* das grandes empresas comerciais parecem estar assumindo a liderança do atual desenvolvimento de ferramentas e estratégias de vigilância que, anteriormente, pertenciam aos ultrassecretos laboratórios militares. Fato é que, por distintas formas, o consumismo tornou-se basilar para as divisões sociais e de identidade. Se a sedução do consumidor desde os primórdios é uma máxima do *marketing*, tal estratégia é sofisticada pela tecnologia que possibiliza vigilância sistemática em grande escala. O advento do *Facebook,* da *Google* e da *Amazon* indica o atual estado da arte (BAUMAN, 2013, p. 113).

Dessarte, cada vez mais os usuários da internet transformam-se em consumidores, realidade que reforça a chamada publicidade comportamental *on-line*, sendo uma espécie da publicidade direcionada. Tal prática permitiu uma personalização ainda mais plena na relação entre consumidores e fornecedores. Com isso, por meio de inúmeras ferramentas tecnológicas, destacando-se os *cookies*, possibilitou-se rastrear a navegação do usuário, a fim de inferir suas preferências para correlacioná-las aos anúncios publicitários. Por conseguinte, a abordagem publicitária passou a ser vinculada, com precisão, ao perfil do potencial consumidor (BIONI, 2020, p. 16).

Tal é o caráter oblíquo da internet que, juntamente com a tecnologia de monitoramento de dados de geolocalização presente nos smartphones, possibiliza que a publicidade se utilize dessas informações ao considerar a proximidade física entre o consumidor e o bem ofertado. De forma correlata, atuam as redes sociais que extraem e concentram uma variedade de dados pessoais dos usuários durante a interação destes com o aplicativo, inclusive ao impelir que o usuário marque os locais que frequenta via *“check-in*” (BIONI, 2020, p. 18).

Outra referência, quanto à utilização dos dados de geolocalização, notabilizou-se com a declaração do estado de pandemia do Coronavírus ou COVID 19, pela Organização Mundial da Saúde, quando Big *Techs*, *startups* e empresas de telecomunicações foram contatadas por agentes governamentais em busca de acesso a esses dados. A existência de tais políticas de monitoramento reflete o aprofundamento do dilema jurídico acerca da possibilidade de extinção do

direito à proteção de dados, sendo que se verificou omissão legislativa no tocante à regulamentação específica para o tratamento desses dados na ocasião[26].

Corroborando com esse cenário de práticas que favorecem a manipulação, a C.A mostrava-se, enquanto uma empresa especializada em executar análises computacionais preditivas, com resultados mensuráveis para seus clientes quando se tratava de consultoria política. Então, a empresa usando o *microtargeting*[27], após capturar os indivíduos, demostrava fazer com que estes pensassem, votassem e agissem de maneira diversa do que faziam antes de serem observados. Afinal, isto é o que todo o projeto sempre almejou, seja comercial, eleitoral ou social, lançar uma propaganda com a certeza prévia de que será um sucesso. Todavia, o que está em jogo aqui é o futuro de humanos (KAISER, 2020, p. 21).

Nesse sentido, é inegável que a eficiência no consumo, na economia e em outros aspectos da vida cotidiana perpassa pela maior quantidade possível de dados fornecida pelos usuários, o que se mostra imediatamente benéfico. Contudo, a opacidade acerca da forma de como tais dados são tratados evoca legítimas inquietações[28] no contexto da privacidade. Ocorre que as legislações que garantam a proteção de dados se encontram prejudicadas pelo limite jurisdicional, o que pode acarretar a falta de comprometimento legal em territórios para além das fronteiras onde tais dados se originaram. Logo, um problema multifacetado que abarca consequências de impacto global (CAMARA; RODRIGUES, 2019).

Acerca da opacidade que atravessa o tratamento dos dados pessoais, a mídia ofereceu algumas respostas com a publicação da matéria sobre um escândalo envolvendo a C.A e a campanha de Ted Cruz em 11 de dezembro de

---

[26] ESTADO, Agência. TIM fecha parceria com Prefeitura do Rio para rastrear movimento e combater vírus. Disponível em: < https://www.infomoney.com.br/economia/tim-fecha-parceria-com-prefeitura-do-rio-para-rastrear-movimento-e-combater-virus/>. Acesso em: 15 abr. 2020. Gabinete de Imprensa. Prefeitura do Recife usa tecnologia como aliada na contenção do novo coronavírus. Disponível em: < http://www2.recife.pe.gov.br/noticias/24/03/2020/prefeitura-do-recife-usa-tecnologia-como-aliada-na-contencao-do-novo-coronavirus>. Acesso em: 15 abr. 2020.

[27] Microssegmentação: refere à técnica de marketing que possibilita ataques focais ao público que almeja por meio da exploração de dados pessoais. Vale notar o quanto tal técnica pode ser nociva a democracia, tendo em vista que muitas vezes são associadas a disseminação de *fake news*.

[28] Cita-se como exemplo os USA, em que o então Presidente Trump com o escopo de obter acesso a localização dos norte-americanos infectados ou com suspeita de infecção, recorreu aos representantes do Facebook, Google, Amazon e Apple para verificar a adesão à política de isolamento social.

2015. Em suma, alegava-se que a C.A obtivera dados do *Facebook* por meio de violação aos termos de uso do site. Tais dados abarcariam informações privadas de 30 milhões de usuários da plataforma e de seus amigos, obtidos sob o pretexto de participação dos usuários em uma pesquisa acadêmica aplicada pelo professor *Kogan*, fundador da empresa GSR, que após vendeu os dados para a C.A. (KAISER, 2020, p. 148).

Logo, não houve um consentimento livre, inequívoco e informado por parte desses usuários que foram ludibriados durante o processo de extração de seus dados, cujo desencadeou outro processo de acesso aos dados de seus amigos, de maneira imprevisível. Portanto, uma prática ilegal realizada mediante a atuação de uma rede de atores para operacionalizar um modelo de negócio baseado na extração de dados, o que ilustra acerca da fluidez e da volatilidade das informações pessoais. Trata-se de uma nova vulnerabilidade, no qual o titular de dados resigna-se as forças do mercado informacional (BIONI, 2020, p. 156).

Nesse enquadramento, desde 2010, o famoso *Friends* API possibilitava que empresas como a C.A instalassem seus próprios aplicativos no *Facebook* para coletar dados dos usuários da plataforma e de todos os seus amigos. Assim, quando os usuários do *Facebook* optavam por usar um desses aplicativos terceiros, eles clicavam nos termos de serviço do mesmo, “concordando” em fornecer acesso a 570 pontos de dados sobre si mesmos e cada um de seus amigos em troca de um teste ou jogo. Todavia, a rede social encerrou o acesso a desenvolvedores terceiros de aplicativos em 30 de abril de 2015 (KAISER, 2020, p. 149). Oportunamente, argumenta Bioni que:

> O consentimento tem sido visto como o pilar dessa estratégia regulatória, mais como um meio para legitimar os modelos de negócio da economia digital, do que como um meio eficiente para desempenhar a proteção de dados pessoais. Ele tem sido encarado como uma verdadeira ficção legal deformadora e voraz do teorizado regime legal de proteção de dados pessoais e da sua aplicação na prática. Não seria mais do que uma mistificação, na medida em que não é confrontado com o anotado contexto socioeconômico que estrangula a prometida liberdade da autodeterminação informacional. Por tal motivo, é de suma importância frisar essa incompatibilidade do desenho normativo de proteção de dados pessoais e, por conseguinte, pensar como isso pode ser absorvido para fins de reflexão e reajustes do ponto de vista de uma (nova) estratégia regulatória. (BIONI, 2020, p. 160).

Nessa perspectiva, é possível afirmar que o titular de dados se encontra em um estado de hipervulnerabilidade em relação à rede de atores partícipes do mercado informacional. Tal fato reforça a ideia acerca da existência de movimentos em direção à extinção do direito à proteção de dados estarem em pleno curso, na medida em que a estruturação do modelo de negócio informacional abdica das expectativas de privacidade dos usuários, operando mediante uma assimetria de poder. Assim, cogita-se que a gestão eficaz dos dados pessoais é incompatível com a gestão satisfatória de *Big Techs* e similares, conforme se evidencia no caso em questão (CAMARA; RODRIGUES, 2019).

A atuação do *Facebook*, nesse caso, clarifica acerca dos dilemas que as *Big Techs* impõem na contemporaneidade, considerando que a própria tecnologia pode ser subvertida para violação de direitos dos titulares de dados ao ponto de afetar processos democráticos. Assim, é possível afirmar que se encontra em risco a independência dos usuários de redes sociais e de todas as demais Coisas conectáveis, sendo pontos de observação de terceiros nem sempre identificáveis, mas que podem ser as corporações mais ricas da história, operando com o propósito de obter lucro mediante a manipulação do comportamento de humanos (LANIER, 2018, p. 11).

Em síntese, trata-se de um mercado sem precedentes que negocia exclusivamente o futuro de humanos. Assim, tudo o que é realizado *on-line,* está sendo rastreado, arquivado, observado, processado e negociado. Tal observador ou vigilante domina a arte de saber todo o possível sobre os indivíduos, sua personalidade, se está sozinho ou acompanhado, se está deprimido. Dessa forma, os dados são inseridos nos sistemas com o escopo de resultarem em análises computacionais preditivas, ou seja, manipulação. Assim como os mágicos perceberam como a mente humana funciona sendo vulnerável a ilusão, tal qual a tecnologia está operando (DILEMA DAS REDES, 2020).

Nesse contexto, a coleta de dados de Kogan ocorreu em 2013, quando este pagou a cada usuário um dólar para que respondessem um questionário de personalidade chamado *This is Your Digital Life*. Dessa forma, quando estes concluíram o teste no *Facebook,* o aplicativo se conectou ao *Friends* API para coletar os dados de cada um dos usuários, bem como de toda a lista de amigos deles. Com as respostas obtidas, Kogan desenvolveu formas de criar modelos de personalidades dos participantes e vendeu o conjunto de dados e os modelos de

personalidades para a C.A que então criou outros modelos mais precisos (CADWALLADR, 2018).

No centro de tais processos situam-se os algoritmos, que consistem basicamente em um conjunto de instruções para realizar uma tarefa, produzindo um resultado a partir de algum ponto de partida. De fato, os algoritmos estão incumbidos de permear todas as esferas da vida humana, a fim de produzirem análises, decisões, pareceres, sendo que algumas tarefas por sua complexidade chegam a extrapolar os limites humanos. Desse modo, os algoritmos podem se mostrar inclusive autônomos, sendo capazes de interferir nos processos decisórios humanos, favorecendo aqueles que exercem poder real sobre seu uso (DONEDA; ALMEIDA, 2018).

Assim, quando a matéria do *The Guardian* foi publicada ameaçando desestabilizar a C.A e a campanha de Ted Cruz, o *Facebook* posicionou que estava no controle dos dados de seus usuários, pois havia findado com o *Friends* API, causa da questão relacionada à segurança de dados. Nessa ocasião, a plataforma contatou a C.A solicitando a exclusão dos dados ligados a Kogan, reprimindo a polêmica a respeito da violação de dados, ao garantir que havia feito todo o possível para solucionar o problema, inclusive, banindo Kogan da plataforma e acusando a C.A. Mas afinal, qual é o negócio do *Facebook*? (KAISER, 2020, p. 158).

As redes sociais são projetadas para criar algoritmos, seu funcionamento tem como base a exploração da necessidade humana de conectar-se com outros, possibilitando um sistema de recompensas através das curtidas. Tal realidade afeta diretamente a produção de dopamina. Portanto, tais plataformas tem um potencial viciante, alterando questões ligadas à autoestima e a identidade, por exemplo. Assim, as curtidas são percebidas enquanto verdade, no entanto, trata-se de uma popularidade artificial, também como verdade são compreendidos os conteúdos a serem visualizados no *feed* de notícias personalizado que é disponibilizado (DILEMA DAS REDES, 2020).

Os usuários de redes sociais recebem estímulos individualizados, continuamente ajustados, cada pessoa tem sua própria verdade, sendo apresentada a realidade de seu próprio mundo. Nesse cenário, é possível afirmar que o que leva o *Facebook* a obter lucro, embora cause danos relevantes e até mesmo indetermináveis para a sociedade, é a possibilidade de modificação de

comportamento que é inerente à monetização dos dados. Dessa forma, a manipulação das emoções negativas mostra-se mais potente para gerar engajamento e efeitos de cunho pessoal, econômico, político, cultural e social (LANIER, 2018, p. 20).

Nesse contexto, a campanha de 2008 de Obama deu origem à participação dos especialistas em dados políticos nesse âmbito, esses sabiam como se utilizar das propagandas do *Facebook*, colocando em aperfeiçoamento o uso da plataforma em favorecimento dos democratas, com um desempenho consistente entre a criação de conteúdo e o envio de mensagens. Além disso, a partir de 2010 o *Facebook* havia encontrado meios de se monetizar no campo dos negócios externos, sobretudo, pela riqueza de dados produzidos advindos de usuários de todo o mundo (KAISER, 2020, p. 155).

Destaca-se o desenvolvimento do *Friends* API como uma das inovações mais lucrativas. Tal advento permitia que, mediante pagamento, desenvolvedores terceiros criassem o seu próprio aplicativo na plataforma, que lhes daria acesso aos dados privados dos usuários, análogo ao que Kogan realizou. Assim, com os dados coletados, a campanha de Obama logrou ser mais estratégica em relação à abordagem comunicativa. Salienta-se que a prática impossibilitava que os amigos dos usuários que tiveram seus dados acessados pudessem dar ou não consentimento. Neste ponto, o *Facebook* agiu ilegalmente ao dar acesso à desenvolvedores terceiros aos dados de seus usuários sem consentimento (KAISER, 2020, p. 156).

Acerca de tal postura, Zuboff (2018, p. 47) expõe que “No caso do *Google*, do *Facebook* e de outros exemplos de capitalistas de vigilância, muitos de seus direitos parecem vir do ato de tomar os direitos dos outros sem consentimento”. Com isso, depreende-se quanto a perspicácia de tais atores privados, sendo que a velocidade de suas habilidades de vigiar excedeu em muito o entendimento da sociedade, bem como o desenvolvimento de leis e regulamentações capazes de exercer limites sobre essas novas operações de negócios. Trata-se de uma ameaça sobremodo antidemocrática.

A Comissão Federal de Comércio dos USA (FTC) advertiu o *Facebook* pelo uso do *Friends* API e de práticas fraudulentas em 2010. Mas os propósitos de proteção de dados e da manutenção de lucros excepcionais em função da exploração dos dados parecem inconciliáveis. Fato é que o *Facebook* não mudou

o seu modo de operar com os desenvolvedores terceiros que se utilizavam do *Friends* API até 2015. Desse modo, novamente a campanha de Obama foi beneficiada em 2012 pelo uso da plataforma, mesmo ano em que o *Facebook* deu início a uma oferta pública de 18 bilhões de dólares (KAISER, 2020, p. 157).

A partir do fechamento do *Friends* API, os desenvolvedores passaram a usar ferramentas de anúncios do *Facebook* a fim de alcançarem os usuários pretendidos, ou seja, foram providenciados novos meios para preencher as lacunas. O *Facebook f*oi bem-sucedido nessa empreitada, uma vez que se tornou a plataforma de publicidade mais exitosa do mundo. Se as expectativas com relação à proteção de dados dos usuários não estavam sendo satisfeitas, não foi motivo para prejudicar o desempenho comercial extraordinário da *Big Tech* (KAISER, 200, p. 158).

Entretanto, o início de 2018 foi marcado por uma publicação acerca da impactante coleta de dados operada por tais empresas. De acordo com a investigação, a C.A coletou informações privadas de, ao menos, 50 milhões de usuários do *Facebook* sem consentimento, o que seria provavelmente o maior vazamento de dados da história da plataforma. O uso do termo “vazamento” mostra-se questionável na medida em que a monetização de dados consiste em uma prática afeita à rede social. Então, evidenciou-se que a C.A nunca deixou de ter acesso a tais dados, o que permitiu a exploração da vida privada de grande parte do eleitorado americano, em favor de seu trabalho baseado em técnicas de modelagem psicográfica, dessa vez, na campanha de Trump em 2016 (ROSENBERG et al, 2018).

É perceptível, nessa conjuntura, que o caráter imaterial da informação veio a reduzir a percepção social quanto a desvios convenientes a práticas totalitárias. Logo, a era informacional requer uma árdua tarefa, atribuir um valor norteador para o futuro, no que concerne aos contratantes hipossuficientes do negócio informacional. Uma vez que os conceitos vigentes foram estruturados visando uma época na qual a informação ainda não se encontrava na posição central do sistema econômico, onde a lógica do mercado pode ser entendida como violações a esfera privada (RODOTÁ, 2008, p. 58).

Assim, de forma precária, sobrevive à antiga estrutura jurídica e institucional de proteção de dados, centrada no consentimento individual, sendo um braço para a tecnologia que possibiliza que um regime autoritário suceda sem

a manifestação dos sinais que, tradicionalmente, os precediam. Tal é o feito das eleições presidenciais norte-americanas de 2016, a propósito, Bauman (2013, p. 129) esclarece que “a vigilância pode anular alguns escrúpulos morais ao manifestar suas “aplicações de proteção”.

A ocasião da eleição de Trump em 2016 suscitou um dos piores cenários possíveis para a democracia. Pois, a C.A, a trabalho para o republicano, se utilizou de operações de informações privadas do eleitorado americano para a criação de perfis psicológicos e políticos sofisticados a serem manipulados com o escopo de votarem no candidato. Esses perfis foram abastecidos com anúncios políticos arquitetados para atuarem em suas composições psicológicas próprias, ao correlacionarem traços de personalidade com comportamento político (CADWALLADR, 2018).

Desse modo, o Projeto *Álamo*, criado para conduzir a campanha de Trump, sobretudo, se empenhou em prever a personalidade de cada adulto dos USA. Considerando que a personalidade é o conjunto de características psicológicas que determinam os padrões de pensar, sentir e agir, se trata de um conhecimento conveniente para práticas de manipulação, portanto, influente na forma como se vota. Assim sendo, tal processo democrático foi comprometido, reforçando a ideia de que a tecnologia aliada às táticas de comunicação pode ser usada para controlar uma sociedade quando o direito à proteção de dados é negado (PRIVACIDADE HACKEADA, 2020).

Deste modo, uma mudança comportamental relevante e inovadora foi viabilizada por meio da operação de algoritmos indiferentes, ocorrendo de maneira inexorável e maquínica, a serviço de manipuladores nem sempre identificáveis, mas que, no evento em questão, foram revelados[29]. Trata-se de poderosos na busca por mais poder operando um sistema da nova economia informacional, com visões antigas e estruturais, que buscam impor extremos políticos em detrimento da heterogeneidade de pensamento. Isto posto, Lanier (2018, p. 37) expõe que “[...] as redes sociais têm sido usadas com sucesso para perturbar sociedades.”.

Necessário referir que a C.A também prestou serviço na campanha de referendo do *Brexit*, onde seu trabalho, por meio de modelagem com base em

[29] Steve Bannon, empresário da comunicação no mercado norte-americano, ex-estrategista da campanha de Trump e ex-conselheiro da Casa Branca no governo Trump; Robert Mercer, o co-CEO do fundo de hedge Renaissance Technologies e sua filha Rebekah, bilionários doadores para causas e candidatos republicanos e o próprio Donald Trump (THE GUARDIAN, 2020).

metodologia psicográfica e algoritmos preditivos, possibilitado pelo acesso à dados privados obtidos por meio de questionários e concursos *on-line*, permitiu o direcionamento de conteúdos segmentados para grupos focais. Tal comunicação teve como cerne provocar o medo dos eleitores indecisos, indicando que votar pela permanência era votar a favor do desmantelamento dos serviços públicos, bem como pela invasão de imigrantes e terroristas (KAISER, 2020, p. 201).

A campanha de Trump, em 2016, ocorreu durante o período de junho a novembro. Nessa época, a C.A de posse de seu robusto banco de dados, que incluía informações de milhões de usuários do *Facebook* desde 2015, passou a segmentar tais pessoas em dois grandes grupos, sendo um do lado de Trump e outro do lado de Hillary. Entre as estratégias de direcionamento de conteúdo, destaca-se a que se dedicou a convencer eleitores de Hillary a não irem às urnas. Tal estratégia pode ser compreendida como supressão de eleitores, sendo considerada ilegal nos USA e, também, ilustra acerca da prática de manipulação comportamental (KAISER, 2020, p. 218).

Após tais operações serem reveladas na mídia, o *Facebook* sofreu uma queda sem precedentes no valor de suas ações, do mesmo modo que significativa oposição não apenas de seus usuários, mas da sociedade global. A situação foi agravada quando a *Channel* 4 News transmitiu imagens de câmeras escondidas com negociações e telefonemas de Alexander Nix, chefe executivo da C.A. Demostrando assim, o estilo fraudulento como a empresa operava em campanhas eleitorais ao redor do mundo. No entanto, não foi causa suficiente para desestabilizar a economia do *Facebook* (BOLDYREVA; GRISHINA; DUISEMBINA, 2018).

Nessa conjuntura, verifica-se que a vigilância para além de violar os direitos civis e políticos dos cidadãos, viola também os direitos sociais, econômicos e culturais, entre outros. Pois, a partir do momento que o titular de dados tem sua vida privada invadida para propósitos obscuros, que não refletem o seu consentimento, como é o caso de ser perturbado por conteúdos individualizados construídos a partir de um conhecimento de terceiros acerca de sua intimidade, a exemplo do que ocorreu no estudo em tela, os efeitos contrários à dignidade humana são mais amplos do que se possa imaginar (FAVERA, 2018, p. 91).

Tais bases de dados relacionais tendem, em certas esferas, a negar ou, ao menos, ofuscar as relações humanas. De tal modo, humanos são decompostos

em dados, onde a pessoa humana desaparece da mente e da vista do vigia. Trata-se, supostamente, de informação desencarnada, selecionada a partir de técnicas de mineração de dados, sendo que o próprio conceito de informação em si subjuga a humanidade do sujeito vigiado. Fato é que o tratamento de dados ocorre hoje em um cenário vastamente despersonalizado, no qual o respeito ao outro é sobrepujado por novas lógicas mercadológicas (BAUMAN, 2013, p. 127).

Shoshana Zuboff explica sobre a manifestação dessa nova lógica mercadológica:

> Os processos extrativos que tornam *o big data* possível normalmente ocorrem na ausência de diálogo ou de consentimento, apesar de indicarem tanto fatos quanto subjetividades de vidas individuais. Essas subjetividades percorrem caminhos ocultos para agregação e descontextualização, apesar de serem produzidos como íntimas e imediatas, ligadas a projetos e contextos individuais...Para o *Google* e outros agregadores de *big data*, no entanto, os dados são apenas *bits*...Os sentidos individuais dados pelos usuários não interessam ao *Google* ou às outras empresas nessa cadeia. Dessa forma, os métodos de produção de *big data* a partir de *small data* e as formas pelas quais o *big data* adquire valor refletem a indiferença formal que caracteriza o relacionamento da empresa com suas populações. As populações são as fontes das quais a extração de dados procede e os alvos finais das ações que esses dados produzem. A "extração" resume a ausência de reciprocidades estruturais entre a empresa e suas populações. Esse fato sozinho separa a *Google*, bem como outros que participam da sua lógica de acumulação, da narrativa histórica das democracias de mercado ocidentais. (ZUBOFF, 2018, p. 34).

A partir dessas considerações, pode-se afirmar quanto à ruptura, que o mercado informacional representa não somente em relação às reciprocidades que vigoravam até então entre empresas e consumidores, mas, mormente, quanto a violações aos princípios democráticos em geral. Nesse sentido, alerta Rodotà (2008, p. 233) "Apesar de acreditarmos estar apenas tratando do tema de proteção de dados, na verdade, estamos nos ocupando do destino das nossas sociedades, do seu presente e sobretudo do seu futuro."

Tal é a realidade que o caso C.A X *Facebook* expõe, onde a supressão do direito à proteção de dados de cidadãos norte-americanos pode ter sido causa de um futuro escolhido por meios antidemocráticos. Assim, a democracia foi afetada de uma forma ampla, onde as possibilidades de reparação parecem inexistentes. Pelo contrário, tais efeitos calamitosos demostraram ter robustez para causar impactos ainda maiores, pois os meios e os atores envolvidos demostram ter

aspirações globais. Lanier (2018) argumenta que a tecnologia global tem operado para restringir a liberdade humana.

Nesse âmbito, o poder identifica-se com a propriedade de dados humanos, que possibilitou através da hipótese em que a campanha de Trump não observasse o comportamento desejado dos vigiados, pudesse adaptar, individualmente, os anúncios para obter melhor desempenho em tempo real. Assim, milhares de campanhas individuais, dentro da campanha principal, foram executadas, inclusive se utilizando de dados de plataformas de sentimentos que mediam os efeitos positivos ou negativos dos conteúdos publicados nas pessoas. Dessa forma, observavam, se pausaram o vídeo ou terminaram de assistir, se clicaram nos links anexados para saber mais, se compartilharam os conteúdos e ainda como se sentiram (KAISER, 2020, p. 221).

Uma fronteira totalmente nova foi aberta, onde um grupo de mídia *on-line* ofereceria, a qualquer pagante, a possibilidade de disponibilizar um conteúdo de um anúncio no seu site*,* estruturando-o de modo como se fosse idêntico ao conteúdo original. Logo, os eleitores confundiam anúncios com notícias, e o conteúdo era retirado de contexto a fim de desabonar a imagem de Hillary. Assim, os dados e a tomada de decisão com base neles parecem ter sido essenciais para a eleição de Trump. Mas o combate não havia sido somente contra Hillary, mas contra o povo americano, esperava-se repetir o resultado em 2020 (KAISER, 2020, p. 226).

O *Facebook* e a C.A enfrentaram múltiplas investigações dos legisladores nos USA e na Europa, sobre o tratamento de dados pessoais de usuários em prejuízo de seus direitos de privacidade e a divulgação de notícias falsas. Nos USA, investigadores do Congresso questionaram Alexander Nix, na época executivo da C. A, bem como, Mark Zuckerberg, fundador e CEO do *Facebook,* sobre tais violações. Então, o posicionamento predominante dos investigados foi o de negar as evidências apontadas por ex-funcionários e documentos da C.A (ROSENBERG et al, 2018).

Além disso, o advogado especial do Departamento de Justiça Americano Robert Mueller, que conduz uma investigação acerca da interferência russa nas eleições americanas, por meio do uso do *Facebook*, entre outras plataformas de mídia da América, para divulgação de propaganda russa e notícias falsas, exigiu e-mails dos funcionários da C.A que atuaram na campanha de Trump em 2016,

como parte de sua investigação. Ocorre que a C.A fez uma apresentação para executivos da *Lukoil*, empresa petrolífera russa, interessada na forma como os dados eram usados para atingir os eleitores americanos (CADWALLADR, 2018).

Na Europa, destaca-se a investigação por parte do Gabinete do Comissário da Informação e da Comissão Eleitoral, órgãos públicos do Reino Unido. Tais investigações abarcam o papel que a C.A desempenhou no referendo da União Europeia, havendo alegações de que realizou trabalho ilegal na campanha do *Brexit.* Ainda, tratam acerca de como o *Facebook*, entre outras plataformas de mídia, está usando e analisando dados pessoais para manipular eleitores no Reino Unido. Nesse sentido, é possível afirmar ser emblemático, tanto o fato de C.A atuar em um território onde as leis de privacidade são mais rígidas, bem como o fato de a C.A ser uma empresa europeia (CADWALLADR, 2018).

As revelações da mídia tradicional sobre o *Facebook* ter permitido que terceiros extraíssem significativa quantidade de dados privados da plataforma para uso em fins políticos, prejudicaram o valor de mercado das ações da empresa. Nesse contexto, a promessa mais relevante foi acerca da criação de uma ferramenta que permitiria, aos usuários, forçar o *Facebook* a excluir todas as informações pessoais que reúne sobre estes enquanto navegam, ainda não foi efetivada. A plataforma alega já há algum tempo, estar tendo dificuldades para acertar tal mecanismo (CADWALLADR, 2018).

Outra promessa anunciada refere à integração das três plataformas da empresa, *WhatsApp*, *Instagram* e *Messenger* em uma, que seria totalmente criptografada. Todavia, essa medida envolve o uso engenhoso da privacidade como justificativa para objetivos anticompetitivos no mercado informacional. Como declara Zuboff (2020, p. 47): “Em vez de um grande número de pessoas possuindo alguns direitos de privacidade, esses direitos foram concentrados no interior do regime de vigilância.” Assim, repercuti a violação por parte do *Facebook*, e outras *Big Techs*, ao privar a sociedade global da escolha no que diz respeito a que partes da sua intimidade desejam manter em sigilo ou revelar.

Em resposta a tal pretensão, a Comissão Federal de Comércio e 48 estados norte-americanos anunciaram que entraram com dois processos contra o *Facebook* por monopólio ilegal. Os autores acusam a plataforma de estar mantendo seu domínio nas redes sociais por meio de uma conduta anticompetitiva praticada por anos, que resultou em lucros exorbitantes. Destacando que, em

2019, a companhia gerou US$ 70 bilhões em receitas e mais de US$ 18,5 bilhões em lucros. Trata-se dos aplicativos mais baixados da última década, atingindo aproximadamente 5 bilhões de pessoas, cerca de 2,3 da população mundial (G1, 2020).

São citadas como partes da estratégia de monopólio, as compras dos então rivais em ascensão *Instagram* e *WhatsApp* pela companhia em negócios bilionários fechados em 2012 e 2014 respectivamente. A venda de tais empresas pelo *Facebook* consta entre os pedidos dos processos, a fim de atingir-se a desintegração do monopólio. A plataforma rebateu as acusações dizendo as aquisições dos aplicativos foram aprovadas pela FTC na época. Em cada um dos processos, há exigências diferentes, sendo que o caso pode levar anos até o trânsito em julgado[30].

Portanto, um império digital foi erguido com base na monetização de dados ao redor do mundo, a custos relativamente baixos, já que os legítimos proprietários dos dados, os titulares, não obtêm nenhuma contrapartida financeira nesse negócio. Quanto a C.A, entre os desdobramentos advindos do escândalo que impactou o mundo, está à falência da mesma que foi impelida a pedir concordata nos Estados Unidos e na Grã-Bretanha. Mas, veio a reabrir com um novo nome, *Emerdata Limited*, com sede no mesmo endereço da C.A e mantendo praticamente a igual diretoria. A *Emerdata* também não existe mais (FORNASIER; BECK, 2020).

Vale notar que a metodologia de pesquisa desenvolvida por Kogan, que apresentava uma forma de medir traços de personalidade de eleitores de todo o globo, com o fim de correlacionar os resultados obtidos com as curtidas do *Facebook,* teve diversas abordagens por parte dos serviços de inteligência dos USA. Inclusive a *Boing*, uma importante empreiteira de defesa norte-americana, financiou o PHD de Kosinsk e a *Darpa*, a secreta Agência de Projetos de Pesquisa Avançada de Defesa do governo dos USA, é citada em, pelo menos, dois artigos acadêmicos de apoio ao trabalho do professor (CADWALLADR, 2018).

Diante disso, a questão acerca da sociedade informacional encontrar-se ou não sob o risco de extinção do direito à proteção de dados, parece indicar como

[30] JORNAL DA GLOBO, 2020. O Texas e outros nove estados americanos abriram um processo contra o Google. (Exibição em 16 de dezembro de 2020) Disponível em: <https://globoplay.globo.com/v/9108341/>. Acesso em: 17 de dez. 2020.

resposta que, se não houver uma mudança relevante no processo decisório sobre o tema, evitar-se a extinção de tal direito será muito improvável. Nesse sentido, a única alternativa satisfatória refere-se a uma transformação no comportamento e nas tendências que atravessam o setor público, o setor privado e a própria sociedade.

No entanto, o setor público enquanto primeiro usufruidor das possibilidades que o aparato tecnológico apresenta em termos de vigilância, parece ter no setor privado um aliado indispensável para que tal vigilância seja constantemente sofisticada. Tal fato pode vir a explicar quanto à morosidade que atravessa as demandas regulatórias sobre a matéria. Afinal, será mesmo interesse do setor público que as ferramentas de vigilância disponibilizadas pelo setor privado se sujeitem a limitações regulatórias?

Vale notar que, de um dia para o outro, o *Facebook* transformou dados pessoais em públicos sem nenhuma regulamentação específica. Assim, as *Big Techs*, por vezes, parecem ser tratadas pelo setor público como se fossem instituições de utilidade pública. Reforça essa ideia, a fala de Eric Schimidt, Presidente do Conselho Administrativo da Google, “A retenção dos seus dados pelo Google não é uma decisão do Google, e sim uma decisão política imposta por vários governos.” (SUJEITO A TERMOS E CONDIÇÕES, 2013).

Assim, as demandas sociais para o uso dos dados pessoais só aumentam, pois áreas como medicina, segurança e finanças podem ser favorecidas significativamente. No entanto, tais benesses jamais podem se sobrepor ao princípio da dignidade da pessoa humana que é intrínseco ao direito proteção de dados. Todavia, a sociedade informacional demostra querer ser cada vez mais *smart*, não se importando com os riscos em longo prazo decorrentes de tal vigilância, mas aberta para as novas tecnologias, ainda que as tendências como internet 5 G, OIT e inteligência artificial sejam mantidas por meio de dados.

De fato, os dados pessoais já são usados nos processos decisórios inerentes à sociedade, como é o caso dos requisitos que cercam a análise de crédito financeiro. Mas, uma vez que o algoritmo segue a um padrão, ele pode vir a romper com a oportunidade humana de alterar o padrão, assim abre-se um precedente para que as minorias sejam afetadas, o que pode contribuir para o abismo social que já é enorme. Um significativo exemplo dessa alternância no padrão foi a inclusão das mulheres no mercado de trabalho. Além disso, o

algoritmo é criado por humanos, portanto, apresentam vieses de seu criador, como sua história, sua visão de mundo, seus juízos de valores, sendo, dessa maneira, passível de preconceitos.

Diante disso, é seguro afirmar que, embora o caso em questão, por si só, não tenha o condão de induzir a extinção do direito fundamental à proteção de dados, ele veio a manifestar desdobramentos relevantes que levaram a enfrentamentos que buscaram reprimir movimentos nessa direção. Reforça essa ideia, a posterior entrada em vigor do RGPD, que repercutiu outras normas de proteção de dados pessoais ao redor do mundo, como é o caso da LGPD brasileira.

No entanto, a questão ainda encontra-se aberta, na medida em que a regulamentação relativa à proteção de dados baliza, também, novas formas de redistribuição de poder, cujas consequências podem assumir notável dimensão. Tal como ocorrido nesse estudo de caso, que engloba um fenômeno relativamente novo, bem como o aspecto ético do uso não oficial e incontrolável de dados pessoais para manipulação humana destinada a fins políticos.

4 CONCLUSÃO

Cada parte dessa pesquisa que agora se encerra foi construída pretendendo-se responder ao problema proposto, sendo: qual o potencial que a vigilância operada por meio do aparato tecnológico demonstra ter para exercer controle sobre a sociedade global, tomando por base o caso *Cambridge Analytica X Facebook (2016)*?

Desse modo, o presente estudo revela que se vive em um tempo onde a imbricação da vigilância, com o aparato tecnológico, suscitou uma complexa economia global que renasceu nos dados, onde estes são apresentados como requisitos fundamentais para dar continuidade à suposta evolução humana, e ainda, a certa revolução pós-humana. No entanto, juntamente com as tendências tecnológicas futuras, entre elas, a internet 5 G, a internet das coisas (OIT) e a inteligência artificial (AI), é possível vislumbrar uma provável redução no que toca a capacidade democrática no campo social nesse contexto.

As coerências mercadológicas e as políticas favorecidas pelo paradigma informacional se encontram cada vez mais infiltradas no mundo da individualidade humana, realidade em afronta ao direito à proteção de dados. Não são poucos os impactos ocasionados por estes novos fatos contemporâneos tanto benéficos, como prejudiciais aos usuários da rede. Tendo em vista a maneira como os mecanismos de navegação estão se configurando, a internet tem se apresentado como um espaço no qual se mostra o que alguns poucos atores acham que é do interesse da multidão que está navegando.

Tal conjuntura é possibilitada por meio do rastreamento de múltiplas informações, inclusive pelo advento da OIT, que se constituem em ferramentas aptas para proporcionar uma customização dos conteúdos exibidos para cada indivíduo. Dessa forma, atores públicos ou privados, que possam exercer controle sobre tais meios tecnológicos, são empoderados ao conhecerem a maioria possível sobre todos os sujeitos em todos os lugares do globo. Trata-se de um novo tipo de vulnerabilidade humana que, na maioria das vezes, não é percebida, pois a execução de tal condicionamento, até então, se expressa de forma velada. Afinal, as conveniências atreladas ao acesso de terceiros a dados pessoais, por vezes, parecem inafastáveis do cotidiano moderno.

Ainda que as possibilidades de domínio, pelo menos, por enquanto, sejam operadas de maneira suavizada, o que se encontra em risco, são restrições aos direitos humanos e fundamentais, sobretudo, quanto às liberdades individuais. Vale notar que a sociedade informacional está sendo cada vez mais orientada nas mais diversas áreas por decisões algorítmicas, onde agentes não humanos com base na extração de dados produzem efeitos nas práticas humanas ou, até mesmo, tomam decisões relevantes no lugar dos indivíduos.

Portanto, a imbricação da vigilância com o aparato tecnológico viabilizou a materialização de um novo estado de exceção na contemporaneidade. Nesse contexto, garantias individuais estão sendo violadas em larga expansão, na medida em que o direito de acesso à informação, realmente desejada ou necessária para o usuário é, em alguma medida, ocultado pelo determinismo dos algoritmos, fato que, consequentemente, prejudica o direito à liberdade de expressão. Nesse raciocínio, a autonomia dos indivíduos se encontra cerceada, tendo em vista que um processo de manipulação de humanos, sem precedente, está sendo construído de forma suavizada.

Então, com o estudo de caso, constatou-se que as redes sociais foram uma ferramenta potencialmente relevante para o êxito da proposta comunicativa da campanha presidencial de Trump (2016). As estratégias sistemáticas de vigilância, operadas nesse meio, possibilitaram a categorização individual de eleitores com o uso de metodologia psicográfica e microtargeting, selecionando-os conforme seus perfis de personalidade para, posteriormente, serem levados a visualizarem conteúdos compatíveis com seus medos. Como afirma Bauman (2013), a invalidação de questões éticas e morais é um atributo presente nos processos da vigilância contemporânea.

Para tanto, os cientistas de dados se utilizaram de modelos preditivos que viabilizaram conhecer acerca das necessidades individuais de tais eleitores, de modo a relacionar seus medos com a figura de Hillary Clinton, então adversária de Trump. Tais conteúdos direcionados continham inclusive *fake news* e eram ajustados com base em seu desempenho praticamente em tempo real. Dessa forma, se os controladores não observassem o comportamento desejado nas reações dos eleitores, adaptavam diferentes versões para cada anúncio. Com isso, foi possível apresentar visões diferentes de mundo para cada eleitor observado com o objetivo de exercer manipulação.

Kaiser, ex-executiva da *Cambridge Analytica,* entregou aos jornalistas uma série de documentos, entre eles gráficos, que provaram com precisão como cada anúncio personalizado na campanha de *Trump* havia sido decisivo para sua eleição. Tais gráficos continham taxas de cliques, índices de engajamento e outras informações que comprovavam a melhoria nas pesquisas de intenção de voto a favor de Trump como resultado da campanha baseada em vigilância *on-line*. Para confirmar esses resultados, foram contratados terceiros que chegaram as mesmas conclusões acerca da assertividade dos processos empregadas na campanha na época.

Nesse sentido, impacta o fato de as redes sociais se configurarem em um aplicativo de relevância global, sendo que a mais acessada é o *Facebook,* que pertence a um único dono, Mark Elliot Zuckerberg, cujo negócio é sustentado pelos interesses dos investidores em manipular humanos. Nessa lógica, foi possível concluir que está em curso um sistema global onde os dispositivos de vigilância disponíveis aos Estados e aos demais atores paralelos a este, irão ao encontro de uma supressão do direito fundamental à proteção de dados pessoais, privilegiando-se o total controle de dados pessoais no que se refere à sociedade civil, sendo tal realidade amparada, sobretudo nas lógicas mercadológica informacional e política.

Diante disso, é possível constatar que o caso *Cambridge Analytica X Facebook* traz à tona a questão de como a vigilância operada em uma plataforma digital logrou êxito em manipular humanos estadunidenses, de modo a persuadi-los a eleger um candidato ao cargo máximo do executivo por meios antidemocráticos. Além disso, destaca-se quanto à impossibilidade de reparação em face das ações operadas pelos poderosos atores que exercem tal vigilância. Logo, constata-se que a legislação que regula a proteção de dados, naquele território, foi ineficiente para assegurar tal tutela.

Portanto, foi possível compreender que não se trata de um caso único, mas de uma tendência que aponta para um futuro onde a multidão estará de forma individualizada, obrigatoriamente, transparente aos olhos de poucos, ou mesmo de um único governo mundial. Pois, é fato que o cenário nacional se mostra insuficiente para responder, de forma adequada, as demandas contemporâneas, sobretudo, em uma sociedade hiperconectada, onde os impactos sobre a soberania dos Estados parecem ser de longo alcance.

Nesse sentido, a tecnologia, em várias áreas, tem assinalado acerca da possibilidade de uma sociedade global, considerando que o mercado informacional já atua dessa forma. Então, argumenta-se que a hipótese de operarem-se transações pecuniárias através de um microchip implantado sob a pele humana, conforme já ocorre na Suécia, mostra-se oportuna futuramente, inclusive por permitir a realização de pagamentos sem contato, necessidade potencializada em face da pandemia COVID-19.

No entanto, a adoção de possíveis dispositivos virá a potencializar ainda mais o processo de revelação dos dados em detrimento das liberdades individuais. Assim, o incremento da vigilância mediante uma tecnologia capaz de conectar todos os indivíduos e todas as coisas em tempo real possibilita o controle da população global de maneira sem precedentes. Pois, a atuais práticas totalitárias estabelecem novas formas de dominação de corpos e mentes. Como tantas vezes bem mostrado pela ficção, o futuro aponta para a transparência dos indivíduos, em um cenário onde a lei, mais do que nunca, é um braço dos controladores.

Por fim, acredita-se que tal conjuntura torna a proteção de dados pessoais uma meta muito difícil de ser alcançada, de modo que, outros direitos que foram estabelecidos para garantir a dignidade humana, também se enfraquecem, com destaque para o direito à liberdade. Não há liberdade quando os aspectos mais pessoais da vida de indivíduos são permanentemente vigiados com vistas a torná-los submissos a uma lógica.

Quanto aos desafios enfrentados nessa trajetória, destaca-se o fato de que foi preciso abrir mão do trabalho que me oportunizava certa estabilidade financeira para haver tempo suficiente para me dedicar ao mestrado, que inclui essa pesquisa. Tal decisão exigiu muita fé e coragem. Para além dos enfrentamentos financeiros, a escassez de tempo continuou presente, pois quando minha primeira filha estava ficando um pouco mais independente, no momento em que eu iria começar esse estudo, nasceu minha segunda filha. Elas são realmente maravilhosas, mas conciliar tudo foi um dos meus maiores desafios certamente.

De todo o modo, considero o tema desta pesquisa muito relevante na luta pela preservação da dignidade humana, sobretudo, no cenário futuro. Para as pesquisas vindouras é possível investigarmos formas de tornar a legislação que regulamenta o tema da proteção de dados mais eficaz.

Pois, acredita-se que as legislações que regulamentam a proteção de dados, levando-se em conta a análise da LGPD e do RGPD contempladas nesta pesquisa, somente serão satisfatórias para tutelar tal direito, na medida em que regulamentarem a arquitetura da rede de forma a torná-la favorável a tal objetivo, pois a arquitetura, até então apresentada, não tem na proteção de dados um propósito. Além disso, reputa-se por legítima a necessidade de recompensar os usuários por seus dados acessados, entendimento que também merece ser aprofundado.

Afinal, os protocolos de transmissão de dados podem ser reescritos pelos técnicos, uma vez que sua natureza não é imutável e permanente. A tecnologia compreende uma criação operada por mãos humanas, sendo que o modo como os dados são vigiados e manipulados, na atual conjuntura, não representa o modo ideal e como deve ser. Portanto, tornar a arquitetura da rede segura para que os dados dos usuários não sejam revelados, armazenados e mercantilizados sem o devido consentimento, consiste em uma questão possível, a partir da modificação dos protocolos e padrões que compõem a arquitetura da rede, visando fomentar os princípios e tutelar os direitos, sobretudo o direito à proteção de dados.

Enfim, toda a iniciativa que promova uma cultura de proteção de dados é legítima. Ademais, no Brasil, um dos últimos países a dar relevância para o tema na América Latina, sendo que a maioria dos países latino-americanos, como o Uruguai e a Argentina já haviam adotado leis de proteção de dados pessoais com aproximadamente duas décadas de antecedência.

REFERÊNCIAS

AGAMBEN, Giorgio. **Estado de Exceção.** São Paulo: Boitempo, 2004.

ARENDT, Hannah. **Origens do totalitarismo.** São Paulo: Companhia das Letras, 1989.

BAUMAN, Zigmunt; LYON, David. **Vigilância líquida:** diálogos com David Lyon. Rio de Janeiro: Zahar, 2013.

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

BRUNO, Fernanda. **Máquinas de ver, modos de ser:** vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

CARDOSO, Bruno et al (Orgs.). **Tecnopolíticas da Vigilância:** perspectivas da margem. 1. ed. São Paulo: Boitempo, 2018.

CERVO, Amado Luiz. **Metodologia científica**: para uso dos estudantes universitários. São Paulo: Editora McGraw-Hill Ltda., 1983.

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

FERRY, Luc. **A revolução transumanista.** Barueri: Manole, 2018.

FLICK, Uwe. **Introdução à pesquisa qualitativa**. Trad. Joice Elias Costa. 3. Ed. Porto Alegre: Artmed, 2009.

FINCATO, Denise Pires; GILLET, Sérgio Augusto da Costa. **A pesquisa jurídica sem mistérios**: do projeto de pesquisa à banca. 3 ed. Porto Alegre: Fi, 2018.

FORTES, Vinicios Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet.** Rio de Janeiro: Lumen Juris, 2016.

FOUCAULT, Michael. **Vigiar e punir.** Petrópolis: Editora Vozes, 2013.

FOUCAULT, Michel. **Em defesa da sociedade**: curso no Collège de France (1975-1976). São Paulo: Editora WMF Martins Fontes, 2010.

GARGARELLA, Roberto. El derecho a la protesta social. **Derecho y Humanidades**, n. 12, 2006, p. 141-151.

GERVASONI, Tássia A. **Estado e direito em trânsito na pós-modernidade.** Florianópolis: Empório do Direito, 2017.

GORCZEVSKI, Clovis. **Direitos humanos, educação e cidadania:** conhecer, educar, praticar. Santa Cruz do Sul: EDUNISC, 2016.

HARDT, Michael; NEGRI, Antonio. **Multidão**. Rio de Janeiro: Record, 2014.

KAISER, Brittany. **Manipulados:** como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque. Rio de Janeiro: Harper Collins, 2020.

LANIER, Jaron. **Dez argumentos para você deletar agora suas redes sociais.** 1. ed. Rio de Janeiro: Intrínseca, 2018.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Editora Saraiva, 2011.

LIMBERGER, Têmis. **Cibertransparência:** informação pública em rede: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016.

MAGRANI, Eduardo. **A internet das coisas.** Rio de Janeiro: FGV Editora, 2018.

NASCIMENTO, Valéria Ribas do.; SALDANHA, Jânia. **Os direitos humanos e o constitucionalismo em perspectiva**: espectros da DUDH e da Constituição da República Federativa do Brasil. Rio de Janeiro: Lumen Juris, 2019.

NASCIMENTO, Valéria Ribas do. **O tempo das reconfigurações do constitucionalismo**: os desafios para uma cultura cosmopolita. São Paulo: LTr, 2011.

PARENTONI, Leonardo. **Direito ao Esquecimento**. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coords). **Direito & Internet III** – Tomo I: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 539-618.

PARISER, Eli. **O filtro invisível:** o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

PEREZ LUÑO, Antonio Enrique. **Derechos humanos, estado de derecho y constitucion.** Madri: Tecnos Editorial, 1986.

PEREZ LUÑO, Antonio Enrique. **Los derechos humanos en la sociedad tecnológica.** Madrid: Editorial Universitas S.A., 2012.

RODOTÁ. Stefano. A vida na sociedade da vigilância: A privacidade de hoje. 1ª

SALDANHA, Jânia Maria Lopes. **Os Direitos Humanos e o Constitucionalismo em Perspectiva.** Rio de Janeiro: Lumen Juris, 2019.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre. Livraria do advogado Editora. 2015.

SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldissera Carvalho. Algoritarismos. São Paulo: Tirante Lo Blanch, 2020.

VIEIRA, Gustavo Oliveira. **Constitucionalismo na mundialização**: desafios e perspectivas da democracia e dos direitos humanos. Ijuí: Ed. Unijuí, 2015.
YIN, R .K. Estudo de caso: planejamento e métodos. 5 ed. Porto Alegre. Bookman, 2015.

- **Artigos, sites, vídeos, etc.**

AFONSO, Henrique Weil. Unidade e fragmentação do direito internacional: o papel dos direitos humanos como elemento unificador. **Revista Eletrônica de Direito Internacional**. Coordenação geral de Leonardo Nemer Caldeira Brant, v. 4, p. 53-90. Belo Horizonte: CEDIN, 2009.

ALVES, Marco Antônio Sousa. Cidade inteligente e governamentalidade algorítmica: liberdade e controle na era da informação. **Philósophos - Revista de Filosofia**, v. 23, n. 2, 7 jan. 2019.

ALVES, Paulo. O que são cookies? Entenda os dados que os sites guardam sobre você. TechTudo. 04 out. 2018. Disponível em: <https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml>. Acesso em: 21 set. 2020.

ANAC. **Resolução n° 255 entre em vigor a partir de junho.** ANAC. 25 abr. 2014. Disponível em: <https://www.anac.gov.br/noticias/2014/resolucao-no-255-entra-em-vigor-a-partir-de-junho>. Acesso em: 15 mai. 2020.

ASSEMBLEIA Geral da ONU. Convenção internacional sobre os Direitos da Criança. 1989.

ASSEMBLEIA Geral da ONU. **Declaração Universal dos Direitos Humanos** (217 [III] A). 1948.

BÍBLIA. In: Bíblia Sagrada Online. Brasil: Livro de Romanos, 2009. Disponível em: <https://www.bibliaon.com/romanos/>. Acesso em: 02 fev. 2021.

BODIN DE MORAES, Maria Celina. QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. In: **Cadernos Adenauer - Proteção de dados pessoais:** privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019, ano XX, n. 3, p. 113-135.

BODIN DE MORAES, Maria Celina; QUEIROZ, João Quinelato de. Autodeterminação Informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. In: **Cadernos Adenauer - Proteção de dados pessoais:** privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019, ano XX, n. 3, p. 112.

BOLDYREVA, Elena L.; GRISHINA, Natalia Y.; DUISEMBINA, Yekaterina. Cambridge Analytica: ethics and online manipulation with decision-making process. **The European Proceedings Of Social & Behavioural Sciences**, [S.L.], v. 4, n. 37, p. 91-102, 31 dez. 2018. Cognitive-Crcs. http://dx.doi.org/10.15405/epsbs.2018.12.02.10.

BRASIL. Constituição Federal do Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 3 de ago. 2019.

BRASIL. Lei n° 12.414/2011, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 10 jun. 2011.
BRASIL. Lei n° 8.069/1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 13 jul. 1990.

BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 13 nov. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acesso em: 30 maio 2020.

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 08 set. 2019.

BRASIL. Medida Provisória nº 869/2018, de 27 de dezembro de 2018. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 28 dez. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 08 set. 2019.

BUOSI, Ana Paula Assis; XAVIER JÚNIOR, Sílvio Gonçalves; NETO, João Araújo Monteiro. A governança do compartilhamento de dados pessoais em tempos de crise: Desafios e perspectiva. In: BIONI, Bruno R.; ZANATTA, Rafael A.; RIELLI, Mariana; VERLIGI, Gabriela; FAVARO, Iasmine (Orgs.). **Os dados e o vírus:** pandemia, proteção de dados e democracia. São Paulo: Reticências Creative Design Studio, 2020.

BURKERT, H. Privacy – Data Protection: a German/European Perspective. In: ENGEL, C.; KELLER, K. H. (Org.). **Governance of Global Networks in the Light of Differing Local Vocals**. Baden-Baden: Nomos Verlagsgesellschaft, 2000. P. 43-70.

CADWALLADR, **Carole. ‘I made Steve Bannon’s psychological warfare tool’:** meet the data war whistleblower. The Guardian. 18 mar. 2018. Disponível em:

<https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>. Acesso em: 16 dez. 2020.

CALDERÓN, Enrique Santos. La libertad de expresión en las democracias latinoamericanas. **Revista Perspectiva**, n. 22, dez. 2009, p. 50-53

CAMARA, Maria Amália Oliveira; RODRIGUES, Walter de Macedo. A gestão de dados pessoais por grandes empresas: considerações geopolíticas e jurídicas. In: **Cadernos Adenauer - Proteção de dados pessoais:** privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, ano XX, n. 3, p. 71-92, 2019.

CANTARINI, Paola. Princípios da proporcionalidade e razoabilidade no tratamento de dados pessoais na LGPD. **Opice Blum Academy.** 05 ago. 2020. Disponível em: <https://opiceblumacademy.com.br/2020/08/proporcionalidade-razoabilidade-tratamento-dados-pessoais-lgpd/>**.** Acesso em: 01 set. 2020.

CARTA dos Direitos Fundamentais da União Europeia. **Jornal Oficial das Comunidades Europeias**. 18 dez. 2000. Disponível em: <https://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 23 mai. 2020.

CASTANHEIRA, Fernando Henrique. Fragmentação do direito internacional e law making no campo jurídico internacional contemporâneo. **Revista da SJRJ**, Rio de Janeiro, n. 25, 2009, p. 63-78. Disponível em: <http://www4.jfrj.jus.br/seer/index.php/revista_sjrj/article/viewFile/2/167>. Acesso em: 10 jan. 2016.

CHEQUER, Cláudio. **Por que a liberdade de expressão é um direito fundamental?** Carta Forense, 03 de outubro de 2011. Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/por-que-a-liberdade-de-expressao-e-um-direito-fundamental/7736>. Acesso em: 10 jan. 2016.

CHICARONI, Camilla Lopes; SERRAGLIO, Lorena Pretti; DA SILVA, Ricardo Barretto Ferreira. **Vai-e-vem da vigência da LGPD e desafios de sua implementação.** Disponível em: <http://www.azevedosette.com.br/noticias/pt/vai-e-vem-da-vigencia-da-lgpd-e-desafios-de-sua-implementacao/5820>. Acesso em: 03 ago. 2020.

COMISSÃO AFRICANA PARA OS DIREITOS DO HOMEM E DOS POVOS. **Declaração de Princípios sobre a Liberdade de Expressão em África**. Disponível em: <http://library.fes.de/pdf-files/bueros/angola/hosting/upd11_05princip_liberdade.pdf>. Acesso em: 10 jan. 2016.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Regulamento da Comissão Interamericana de Direitos Humanos**. Disponível em: <http://www.cidh.org/Basicos/Portugues/u.Regulamento.CIDH.htm>. Acesso em: 10 jan. 2016.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. Relatoria Especial para a Liberdade de Expressão. **Marco jurídico interamericano sobre o direito à liberdade de expressão**. 2010. Disponível em: <http://www.oas.org/pt/cidh/expressao/docs/publicaciones/20140519%20-%20PORT%20Unesco%20-%20Marco%20Juridico%20Interamericano%20sobre%20el%20Derecho%20a%20la%20Libertad%20de%20Expresion%20adjust.pdf>. Acesso em: 10 jan. 2016.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Resolução CGI.br/RES/2012/008/P.** São Paulo. s/d. Disponível em: https://www.cgi.br/publicacoes/indice/documentos/ Acesso em: 02 de dez. 2019.

CONSELHO DA EUROPA. **Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais**. Roma, 04 de novembro de 1950. Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 10 jan. 2016.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Handyside vs. Reino Unido** (n. 5493/72), julgado em 7 dez. 1976. Disponível em: <http://artigo19.org/centro/arquivos/download/130>. Acesso em: 10 jan. 2016.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso “A Última Tentação De Cristo” (Olmedo Bustos e outros) *vs.* Chile. In: SECRETARIA NACIONAL DE JUSTIÇA; COMISSÃO DE ANISTIA; CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Jurisprudência da Corte Interamericana de Direitos Humanos**. [Direito à liberdade de expressão]. Tradução da Corte Interamericana de Direitos Humanos. Brasília: Ministério da Justiça, 2014, p. 59-95.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Claude Reyes e outros *vs*. Chile. In: CORTE INTERAMERICANA DE DIREITOS HUMANOS; SECRETARIA NACIONAL DE JUSTIÇA; COMISSÃO DE ANISTIA. **Jurisprudência da Corte Interamericana de Direitos Humanos**. [Direito à liberdade de expressão]. Tradução da Corte Interamericana de Direitos Humanos. Brasília: Ministério da Justiça, 2014, p. 215-264.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Fontevecchia e D’Amico *vs*. Argentina. In: CORTE INTERAMERICANA DE DIREITOS HUMANOS; SECRETARIA NACIONAL DE JUSTIÇA; COMISSÃO DE ANISTIA. **Jurisprudência da Corte Interamericana de Direitos Humanos**. [Direito à liberdade de expressão]. Tradução da Corte Interamericana de Direitos Humanos. Brasília: Ministério da Justiça, 2014, p. 431-458.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Kimel *vs.* Argentina. In: CORTE INTERAMERICANA DE DIREITOS HUMANOS; SECRETARIA NACIONAL DE JUSTIÇA; COMISSÃO DE ANISTIA. **Jurisprudência da Corte Interamericana de Direitos Humanos**. [Direito à liberdade de expressão]. Tradução da Corte Interamericana de Direitos Humanos. Brasília: Ministério da Justiça, 2014, p. 265-297.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Opinión Consultiva n. 5/1985** (La colegiación obligatoria de periodistas). 13 nov. 1985. Disponível em: <http://www.corteidh.or.cr/docs/opiniones/seriea_05_esp.pdf>. Aceso em: 10 jan. 2016.

COSTA, Maria Cristina Castilho. Liberdade de Expressão como Direito – História e Atualidade. **Revista Nhengatu** – **Revista Iberoamericana de Comunicação e Cultura Contra-hegemônicas**, v. 1, n. 1, 2013. Disponível em: <http://www.nhengatu.org/revista/index.php?journal=nhengatu&page=article&op=download&path%5B%5D=8&path%5B%5D=4>. Acesso em: 10 jan. 2016.

CRUZ, Gisela Sampaio da; MEIRELES, Rose Melo Venceslau. Término do tratamento de dados. In: TOPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro. São Paulo: **Revista dos Tribunais – Thomson Reuters Brasil**, 2019. p. 122.

DEBATE ANPD E LGPD. Apresentado por Danilo Doneda e Arthur Sabbat [s.l:s.n], 10 jun. 2020. 1 vídeo (1h 09 min 25 seg). Publicado pelo canal CDTV. Disponível em: https://youtu.be/8qkZjX0WZbk. Acesso em: 11 set. 2020.

DIAS, Marina. **Adiamento da LGPD é uma tragédia.** Conjur. 29 jun. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-29/marina-dias-tragico-adiamento-lgpd>. Acesso em: 3 ago. 2020.

DIAS, Felipe da Veiga; Kampff, Luíza Cerveira. Algoritmos de manipulação: um retrato da fantasia fake no Brasil. In: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldissera Carvalho. Algoritarismos. São Paulo: Tirante Lo Blanch, 2020, p. 539.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, p. 91-108, 13 dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 10 ago. 2020.

DONEDA, Danilo; ALMEIDA, Virgílio A. F. O que é a governança de algoritmos? In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (Orgs.). **Tecnopolíticas da Vigilância**: perspectivas da margem. 1 ed. São Paulo: Boitempo, 2018. p. 141-142.

DONEDA, Danilo; SABBAT, Arthur. **Debate ANPD e LGPD.** 2020. (1h09m25s). Disponível em: <https://youtu.be/8qkZjX0WZbk>. Acesso em: 10 set. 2020.

ESTADOS UNIDOS DA AMÉRICA. Suprema Corte dos Estados Unidos. **The New York Company vs. L. B. Sullivan** (n. 39), 376 U.S. 254, julgado em 9 mar. 1964. Disponível em: <http://caselaw.findlaw.com/us-supreme-court/376/254.html>. Acesso em: 10 jan. 2016.

EUROPARL. In: Parlamento Europeu. Estrasburgo: Disposições de Direito Civil Sobre Robótica, 2017. Disponível em <https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html>. Acesso em 20 mar. 2020.

EXECUTIVO federal traduz para o português a jurisprudência da Corte Interamericana de Direitos Humanos. **Secretaria de Direitos Humanos da Presidência da República**. 1. out. 2014. Disponível em: <http://www.sdh.gov.br/noticias/2014/outubro/governo-traduz-para-o-portugues-a-jurisprudencia-da-corte-interamericana-de-direitos-humanos>. Acesso em: 10 jan. 2016.

FACEBOOK é alvo de processos nos EUA por monopólio nas redes sociais. G1. 09 dez. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/09/facebook-e-alvo-de-acao-antitruste-nos-estados-unidos-diz-agencia.ghtml>. Acesso em: 15 dez. 2020.

FAVERA, Rafaela Bolson Dalla. **Surveillance e direitos humanos:** o tratamento jurídico do tema nos EUA e no Brasil, a partir do caso Edward Snowden. Rio de Janeiro: Lumen Juris, 2018.

FERNANDES, Cláudio. **Queda de Constantinopla em 1453**. Brasil Escola. Disponível em: <https://brasilescola.uol.com.br/historiag/queda-constantinopla-1453.htm>. Acesso em: 24 abr. 2020.

FERREIRA, Rafael Fonseca; SALDANHA, Jânia Maria Lopes. Perspectivas do direito processual internacional dos direitos humanos:desenvolvendo a promoção e a proteção dos direitos humanos. **Juris** (FURG), 2012, v. 17, p. 123-144.

FERREIRA, Vitor Hugo do Amaral. JENSEN, Vinícius de Sousa. Relações virtuais de consumo: perspectivas de direitos no e-commerce. **Revista:** Direitos Emergentes na Sociedade Global, vinculada ao Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria - ISSN 2316-3054. Disponível em: <https://periodicos.ufsm.br/REDESG/article/view/6053#.YLjSO_lKjIU>. Acesso em: 07 abr. 2021.

FILHO, Mattos; FILHO, Veiga; MARREY JR; ADVOGADOS, Quiroga. Transferência de dados pessoais de passageiros e tripulantes na indústria aeronáutica. **Lexicology**. s/l, 2018.

FORJAZ, Maria Cecília Spina. Globalização e crise do estado nacional. **Rev. adm. empres.**, São Paulo, v. 40, n. 2, p. 38-50, June 2000. Available from Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-75902000000200005&lng=en&nrm=iso>. Acesso em: 27 ago. 2020. .

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: Escândalo, Legado e possíveis futuros para a democracia. **Revista do Departamento de**

Ciências Jurídicas e Sociais da Unijuí, ano XXIX, n. 53, jan-jun. 2020, p. 182-195.

FRAZÃO, Ana; ABILI, Vivianne da Silveira. Compilação de dados pessoais. In: TOPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro. São Paulo: **Revista dos Tribunais – Thomson Reuters Brasil**, 2019. p. 676.

GARGARELLA, Roberto. No hay democracia sin protesta. Las razones de la queja. **[Entrevista disponibilizada na internet].** Disponível em: <http://www.miguelcarbonell.com/artman/uploads/1/No_hay_derecho__sin_protesta._Entrevista_a_Roberto_Gargarella.pdf>. Entrevista concedida a Esteban Rodríguez. Acesso em: 10 jan. 2016.

GENEVOIS, Margarida. **Direitos Humanos na História**. Dhnet. Disponível em: <http://www.dhnet.org.br/direitos/anthist/margarid.htm>. Acesso em: 10 jan. 2016.

GONDIM, Abnor. **Prorrogada MP que adia vigência da LGPD para maio de 2021**. 2020. Disponível em: <https://www.telesintese.com.br/prorrogada-mp-que-adia-vigencia-da-lgpd-para-maio-de-2021/>. Acesso em: 03 ago. 2020.

GOVERNO DO BRASIL, In: Governo Digital. Brasil: Do eletrônico ao digital, 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>. Acesso em: 20 mar. 2020.

GOVERNMENT Tracking How People Move Around in Coronavirus Pandemic. **The Wall Street Journal.** 28 mar. 2020. Disponível em: <http://www.wsj.com/articles/governement-tracking-how-people-move-arond-in-coronavírus-pandemiac-11585393202>. Acesso em: 25 nov. 2020.

GOVERNO DE SÃO PAULO. **Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo.** Portal do Governo de São Paulo. 02 maio 2017. Disponível em: <https://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-o-estado-de-sao-paulo-com-3-mil-cameras-de-video/>. Acesso em: 22 out. 2020.

GLOBO. In: TECHTUDO. Site de tecnologia da Globo.com. Disponível em: <https://www.techtudo.com.br/noticias/2019/06/o-que-significa-uber-confira-perguntas-e-respostas-sobre-o-aplicativo.ghtml>. Acesso em: 22 mar. 2020.

KELLER, Clara et al. **LGPD entra em vigor em 2020**: Como a reviravolta afeta empresas e usuários. 2020. (38 min 22seg). Disponível em: <https://www.youtube.com/watch?v=nhyjjd8FUOw>. Acesso em: 11 set. 2020.

LEI Geral de Proteção de Dados Pessoais (LGPD) e setor público. Um guia da Lei 13.709/2018, voltado para os órgãos e entidades públicas. Disponível em: <https://itsrio.org/wp-content/uploads/2019/05/LGPD-vf-1.pdf>. Acesso em: 08 set. 2019.

LGPD em Vigor? Principais pontos de atenção. [s./l.: s./n.], 2020. 1 vídeo (1h 09 min 05 seg). Publicado pelo canal Opice Blum, Bruno e Vainzof Advogados

Associados. Disponível em: <https://www.youtube.com/watch?v=xb0Bj9rg5TM&t=1625s>. Acesso em: 11 set. 2020.

LGPD entra em vigor em 2020: Como a reviravolta afeta empresas e usuários – Big Data Venia, ep. 6. [s./l.: s./n.], 2020. 1 vídeo (38 min 22 seg). Publicado pelo canal Jota. Disponível em: <https://www.youtube.com/watch?v=nhyjjd8FUOw>. Acesso em: 11 set. 2020.

NUNES. Vidal Serrano Jr. Et al. Enciclopédia Jurídica da PUCSP, tomo II direito administrativo e constitucional - São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/>. Acesso em: 10 de jan. 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a Nova Lei Geral de Proteção de dados. In: MARQUES, Claudia Lima. **Revista de Direito do Consumidor**, v. 120, ano 27. São Paulo: Revista dos Tribunais – Thomson Reuters Brasil, nov-dez. 2018). p. 469-483.

MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de. Análises computacionais preditivas como um novo biopoder: modificações do tempo na sociedade dos sensores. **Novos Estudos Jurídicos**, [S.l.], v. 24, n. 3, p. 1129-1154, 21 dez. 2018.

MESQUITA JÚNIOR, Sidio Rosa de. Os principais paradigmas do pensamento jurídico. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 20, n. 4241, 10 fev. 2015. Disponível em: <https://jus.com.br/artigos/36218/os-principais-paradigmas-do-pensamento-juridico>. Acesso em: 15 jan. 2019.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, [S.L.], v. 19, n. 3, p. 159-180, 29 dez. 2018. Sociedade de Ensino Superior de Vitoria. http://dx.doi.org/10.18759/rdgf.v19i3.1603.

NASCIMENTO, Valéria Ribas do**. O tempo de reconfigurações do constitucionalismo:** os desafios para uma cultura cosmopolita. 322 f. 2010. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade do Vale dos Sinos, São Leopoldo, 2010.

NASCIMENTO, Valéria Ribas do. Direitos fundamentais da personalidade na era da sociedade da informação: Transversalidade da tutela à privacidade. **Revista de Informação Legislativa**. v, 54, n. 213, p. 265-288, jan./mar. 2017. Disponível em: phttps://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p265. Acesso em: 28 nov. 2018.

OPICE BLUM ACADEMY. In: Instituição de ensino dedicada ao Direito Digital, Tecnologia, Privacidade e Proteção de Dados, 2020. Disponível em

<https://opiceblumacademy.com.br/2020/08/proporcionalidade-razoabilidade-tratamento-dados-pessoais-lgpd/>. Acesso em 18. nov. 2020.

ORGANIZAÇÃO DA UNIDADE AFRICANA. **Carta Africana dos Direitos do Homem e dos Povos**. Disponível em: <http://www.saflii.org/ao/legis/num_act/cadddhedp396.pdf>. Acesso em: 11 jan. 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Disponível em: <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 11 jan. 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Civis e Políticos**. 1994. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm>. Acesso em: 11 jan. 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Civis e Políticos**. 1966. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm>. Acesso em: 11 jan. 2016.

ORGANIZAÇÃO das Nações Unidas. **Pacto Internacional sobre Direitos Civis e Políticos.** Adotado pela XXI Sessão da Assembleia Geral das Nações Unidas, em 16 de dezembro de 1966.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Carta Democrática Interamericana**. 2001. Disponível em: <http://www.oas.org/charter/docs_pt/carta_pt.htm>. Acesso em: 11 jan. 2016.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Convenção Americana de Direitos Humanos**. San José, Costa Rica, nov. 1969. Disponível em: <http://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm>. Acesso em: 11 jan. 2016.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Declaração Americana dos Direitos e Deveres do Homem**. Aprovada na IX Conferência Internacional Americana. Bogotá, Colômbia, abr. 1948. Disponível em: <http://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm>. Acesso em: 11 jan. 2016.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Declaração de Nuevo León**. 2004, México. Disponível em: <http://www.oas.org/xxxivga/portug/reference_docs/CumbreAmericasMexico_DeclaracionLeon.pdf>. Acesso em: 11 jan. 2016.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Declaração de Princípios sobre Liberdade de Expressão**. Out. 2000. Disponível em: <http://www.cidh.oas.org/basicos/portugues/s.Convencao.Libertade.de.Expressao.htm>. Acesso em: 11 jan. 2016.

PARENTONI, Leonardo. Lei Geral de Proteção de Dados Pessoais. Autoridade Nacional de Proteção de Dados Brasileira: uma visão otimista. **Revista do Advogado**, ano XXXIX, n. 144, nov. 2019, p. 209-218.

PARLAMENTO EUROPEU. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas: União Europeia, 2016.

PROCESSO nos EUA: Facebook pode ter que vender WhatsApp e Instagram. **G1**. 10 dez. 2020. Disponível em: <https://g1.globo.com/globonews/jornal-globonews-edicao-das-10/video/processo-nos-eua-facebook-pode-ter-que-vender-whatsapp-e-instagram-9090919.ghtml>. Acesso em: 20 dez. 2020.

REVOLUÇÃO 5G: conheça a tecnologia que promete conexões ultra-rápidas de internet. Fantástico. **G1**. 25 out. 2020. Disponível em: <https://g1.globo.com/fantastico/noticia/2020/10/25/revolucao-5g-conheca-a-tecnologia-que-promete-conexoes-ultra-rapidas-de-internet.ghtml>. Acesso em: 28 out. 2020.

RIANELLI, Erick. **Contribuintes aparecem como mortos no sistema da Caixa e têm auxílio emergencial negado no RJ.** G1. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2020/05/21/contribuintes-aparecem-como-mortos-no-sistema-da-caixa-e-tem-auxilio-emergencial-negado-no-rj.ghtml>. Acesso em: 01 jun. 20.

ROSENBERG, Nicholas et al. How Trump Consultants Exploited the Facebook Data of Millions. **New York Times**. 17 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em: 18 nov. 2018.

SILVA, Rosane Leal. O Direito Humano à Privacidade Revisitado pelo uso das Tecnologias: a Proteção dos Dados Pessoais de Crianças e Adolescente Internautas Ante a Lei 13.709/2018. In: NASCIMENTO, Valéria Ribas do; SALDANHA, Jânia Maria Lopes (Org.) **Os Direitos Humanos e o Constitucionalismo em Perspectiva**. Rio de Janeiro: Lumen Juris, 2019.

SOMBRA, Tiago Luís. **Transferência de dados pessoais de passageiros e tripulantes na indústria aeronáutica**. Disponível em: <https://www.lexology.com/library/detail.aspx?g=01fdb879-822c-44da-8160-4e13f564e2ac>. Acesso em: 15 mai. 2020.

THE WALL STREET JOURNAL. In: Jornal internacional sobre notícias econômicas. Nova York, 2020. Disponível em: <http://www.wsj.com/articles/governement-tracking-how-people-move-arond-in-coronavírus-pandemiac-11585393202>. Acesso em: 25 nov. 2020.

TRANSFORMAÇÃO DIGITAL. In: Encurtador. Brasil, 2019. Disponível em: <encurtador.com.br/gmDW0> Acesso em 18 mar. 2020.

TYBUSCH, Jerônimo Siqueira; ARAUJO, Luiz Ernani Bonesso de; SILVA, Rosane Leal da. **Anuário do Programa de Pós-Graduação em Direito da UFSM**: Direitos Emergentes na sociedade global. Ijuí: Ed. Unijuí, 2013.

VARELLA, Marcelo Dias. **Internacionalização do direito:** direito internacional, globalização e complexidade. 2012. 606 p. Tese (Doutorado) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

VECHI, Fernando; MENDES, Carlos Helder Furtado. Tecnovigilância e controle e(m) tempos securitários: quem são os alvos? In: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldissera Carvalho. Algoritarismos. São Paulo: Tirante Lo Blanch, 2020, p. 233

VOSS, W. Gregory; CASTETS-RENARD, Céline. Proposal for na International Taxonomy on the various forms of the “Right to Forgotten”: A study on the convergence of norms. **Colorado Technology Law Journal**, Boulder, v. 14, n. 2, 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800742>. Acesso em: 12 out. 2020.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação. In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (Orgs.). **Tecnopolíticas da Vigilância**: perspectivas da margem. 1 ed. São Paulo: Boitempo, 2018. p. 18-68.