UNIVERSIDADE PRESBITERIANA MACKENZIE

TRABALHO DE CONCLUSÃO DE CURSO DA FACULDADE DE DIREITO

MELYSSA SANTOS

ANÁLISE DA CIBERSEGURANÇA DE USUÁRIOS DA INTERNET NO BRASIL:

Um desafio na era do *big data* e *dataveillance versus* a privacidade e proteção de dados dos usuários sob a ótica da Lei n° 13.709/18.

SÃO PAULO

2023

MELYSSA SANTOS

ANÁLISE DA CIBERSEGURANÇA DE USUÁRIOS DA INTERNET NO BRASIL:

Um desafio na era do *big data* e *dataveillance versus* a privacidade e proteção de dados dos usuários sob a ótica da Lei n° 13.709/18.

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie como parte dos requisitos exigidos à obtenção do título de Bacharel em Direito, sob a orientação da Prof. Dra. Ruth Carolina Rodrigues Sgrignolli.

SÃO PAULO

2023

MELYSSA SANTOS

ANÁLISE DA CIBERSEGURANÇA DE USUÁRIOS DA INTERNET NO BRASIL:

Um desafio na era do *big data* e *dataveillance versus* a privacidade e proteção de dados dos usuários sob a ótica da Lei n° 13.709/18.

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie como parte dos requisitos exigidos à obtenção do título de Bacharel em Direito, sob a orientação da Prof. Dra. Ruth Carolina Rodrigues Sgrignolli.

BANCA EXAMINADORA

_____

Prof.ª Dra. Ruth Carolina Rodrigues Sgrignolli

Universidade Presbiteriana Mackenzie

_____

Prof.ª Dra. Michelle Asato Junqueira

Universidade Presbiteriana Mackenzie

_____

Prof.ª Dra. Ana Cláudia Pompeu Torezan Andreucci

Universidade Presbiteriana Mackenzie

AGRADECIMENTOS

Agradeço, primeiramente, a Deus pelo dom da vida, pela coroa de vida eterna que me ofereceu até aos céus se eu for uma filha firme e fiel até o fim. Sem a proteção do Senhor eu jamais estaria aqui, nesse momento, louvando-o e dizendo o quanto ele é bom e presente na minha vida. Que toda a honra e glória sejam dadas a Ele.

Segundamente, necessito manifestar minha profunda gratidão à minha mãe, Miriam, e ao meu irmão, Diego. Obrigada, mamãe, por ter sido a base da nossa família e nunca ter desistido de nós. Obrigada, Dido, por sempre demonstrar o quanto o trabalho duro compensa. Obrigada aos dois, por serem compreensivos e pacientes comigo, sempre me incentivando a estudar e ser alguém melhor a cada dia. Eu amo vocês.

Agradeço também aos professores da Faculdade de Direito do Mackenzie pelo aprendizado profissional, principalmente à minha orientadora, Prof. Ruth Carolina, por me acompanhar nesse período com motivação e disposição.

Esse trabalho igualmente não seria possível sem o apoio das pessoas que estiveram à minha volta, aguentando e suportando todo o estresse causado pelo fim de graduação junto comigo. Obrigada Universidade Presbiteriana Mackenzie por ter me dado a oportunidade de conhecer as melhores pessoas que poderia ter compartilhado a minha graduação, em especial Ali, Bia, Giu, Lari, Lau, Lelê e Lucca. Vocês são meu alicerce.

Por fim, e não menos importante, não poderia esquecer do meu amigo Ivo, que sem pre me fez rir quando estava em momentos de desespero e só precisava de uma piada para alegrar meu dia. Obrigada por tudo.

"*You have zero privacy anyway. Get over it.*"

Scott McNealy

RESUMO

A rápida evolução da tecnologia e a crescente dependência da internet têm levado a um aumento significativo nas preocupações com a cibersegurança e a privacidade dos usuários no Brasil. Esta pesquisa analisa o cenário da cibersegurança e da proteção de dados dos usuários na era do *big data* e *dataveillance*, com foco na legislação brasileira, em particular, a Lei n° 13.709/18. Para isso, serão expostos apontamentos sobre a construção da sociedade da informação, bem como o desenvolvimento do *big data* como uma mercadoria propriamente dita. Em seguida, será feita a análise do conceito de privacidade e, por fim, a análise da LGPD. Esta pesquisa busca compreender o sistema de internet atual e definir se o usuário brasileiro está devidamente amparado pelo aparato legal do ordenamento jurídico brasileiro.

PALAVRAS-CHAVE: *big data;* proteção de dados; capitalismo de vigilância; sociedade da informação.

ABSTRACT

The evolution of technology and the growing dependence on the Internet have led to a significant increase in concerns about cybersecurity and user privacy in Brazil. This research analyzes the scenario of cybersecurity and user data protection in the era of big data and dataveillance, focusing on Brazilian legislation, in particular, the Law n° 13.709/18. For this, notes will be made on the construction of the information society, as well as the development of big data as a commodity itself. Then we will analyze the concept of privacy and, finally, the analysis of the LGPD. This research seeks to understand the current Internet system and to define whether the Brazilian user is properly supported by the legal apparatus of Brazilian legal system.

KEYWORDS: big data; data protection; surveillance capitalism; information society.

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

ANPD Autoridade Nacional de Proteção de Dados

CDC Código de Defesa do Consumidor

CNPD Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GPS *Global Positioning System*

IOT Internet das Coisas

IP *Internet Protocol*

LGPD Lei Geral de Proteção de Dados

MCI Marco Civil da Internet

MPDFT Ministério Público do Distrito Federal e Territórios

RGPD Regulamento Geral sobre a Proteção de Dados

SUMÁRIO

INTRODUÇÃO

O direito à privacidade e à proteção de dados enfrentam uma nova gama de desafios e complexidades à medida que a sociedade evolui em direção a um cenário cada vez mais digitalizado. No contexto da crescente interconexão tecnológica, os desafios tornam-se significativos até mesmo para a própria manutenção do Direito.

Durante a construção da era digital, no qual a tecnologia da informação tornou-se quase onipresente, o mundo torna-se cada vez mais orientado por dados: grande parte das informações pessoais de usuários está contido e armazenado em bancos públicos e privados de grandes redes. Denota-se, dia após dia, a assimetria de poder entre entidades de tecnologia e usuários.

Torna-se notório que a revolução tecnológica é construída em ritmo acelerado, a fim de satisfazer as demandas de um mundo mais conectado. A disparidade entre o progresso tecnológico e a regulamentação jurídica é, sem dúvida, um desafio complexo. Nesse contexto, emergem dúvidas sobre a capacidade da resguarda da Lei n° 13.709/18 para com os usuários brasileiros, no que concerne a própria proteção de seus dados e seu direito à privacidade na nova era do *big data.*

Estaria o usuário de internet brasileiro, em 2023, amparado pela Lei n° 13.709/18? Foi por meio desta pergunta que se desenvolveu o tema do presente artigo. Para tanto, discutir-se-á ao longo dos capítulos os desafios para consolidação e construção da confiança e garantia dos direitos fundamentais, sobretudo ao direito à privacidade, ambivalente à análise da regulamentação da internet no Brasil em detrimento da Lei n° 13.709/18, com o objetivo de determinar se é possível mensurar o nível de proteção dos usuários de internet no Brasil a partir da regulamentação da LGPD, além de pesquisar, definir e validar os conceitos sobre *big data*, *dataveillance* e o capitalismo de vigilância.

Para a persecução desses objetivos, será realizada a revisão de literatura que utiliza a biblioteca eletrônica “SciELO”, a fim de identificar artigos científicos publicados no período de 2005 a 2023. A busca da bibliografia será feita pelos indexadores *“big data”, “dataveillance”*, “proteção de dados”, “direito fundamental” e “Lei Geral de Proteção de Dados”, bem como seus correspondentes em inglês.

Outrossim, será utilizado o método de pesquisa bibliográfica teórico-qualitativa, em que se busca o conhecimento em diversos tipos de publicações, como livros e artigos em jornais,

revistas e outros periódicos especializados, além de publicações oficiais da legislação e da jurisprudência, bem como a utilização de doutrina jurídica e da tecnologia da informação para definição de conceitos.

Também utilizar-se-á a pesquisa documental, procedendo à análise de julgados e dispositivos normativos, que permitem analisar o direito fundamental à privacidade por meio do método dedutivo analítico, em conjunto com a Lei Geral de Proteção de Dados (Lei n° 13.709/18) e seus desdobramentos.

1. OS DESAFIOS TRAZIDOS PELA SOCIEDADE DA INFORMAÇÃO E A INTERNET DAS COISAS (IOT)

A construção da era digital teve como produto principal a formação de uma nova sociedade, a sociedade da informação[1]. Segundo os apontamentos trazidos pelo Prof. Frederico Gazolla[2], tal construção foi possível graças à reestruturação do capitalismo no final da década de 80 do século XX: após a revolução agrícola e dos bens de produção na revolução industrial, houve a supervalorização da informação.

Define-se informação como um dado ou conjunto de dados brutos ou processados, em qualquer meio ou suporte, capaz de produzir conhecimento[3]. Este é o principal ativo e característica da sociedade da informação, tornando-se um pilar inquestionável para o desenvolvimento econômico e social, além de se apoiar no largo e intensivo uso da tecnologia da informação como mecanismo de coleta, produção, processamento, transmissão e armazenamento de dados[4].

---

[1] A Sociedade da Informação é identificada a partir do contexto histórico em que há a preponderância da informação sobre os meios de produção e distribuição dos bens na sociedade, decorrente principalmente da introdução dos computadores conectados em rede nas relações jurídicas. Ver: DUFF, Alistair A. **Information society studies.** Londres: Routledge: 2000; MASUDA, Yoneji. **The information society as post-industrial society.** Tóquio: Institute for the Information Society, 1980; MACHLUP, Fritz. **The production and distribution of knowledge in the United States**. Nova Jersey: Princeton University Press, 1962; DIJK, Jan van. The network society. 3. rd. Londres: Sage Publications, 2012;

[2] GAZOLLA, Frederico. **Direito à privacidade na sociedade da informação e o pós-panoptismo** uma análise sobre privacidade e regulação da proteção de dados pessoais. São Paulo: Editora Dialética, 2021. p. 20.

[3] Para conferir o conceito, VER: ANGELONI, Maria Terezinha. **Elementos intervenientes na tomada de decisão**. Ci. Inf., Brasília, v. 32, n. 1, p. 17-22, Apr. 2003. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652003000100002&lng=en&nrm=iso>. Acesso em 25 set. 2023.

[4] GAZOLLA, op cit, 2021, p. 43.

A tecnologia da informação foi desenvolvida a ponto de afetar não apenas a rede de computadores, mas também a de dispositivos de microeletrônica, a telecomunicação e até a engenharia genética. Objetos foram transformados para atender a uma rotina cada vez mais moderna: atualmente, são quase 42 bilhões de dispositivos conectados de forma global.[5]

O termo Internet das Coisas (IoT), do inglês *Internet of Things*, pode ser entendido como um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente e voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia.[6] Também pode ser considerado como " a progressiva automatização de setores inteiros da economia e da vida social com base na comunicação máquina-máquina: logística, agricultura, transporte de pessoas, saúde, produção industrial".[7]

Smartphones, televisores, *tags* para pedágio, pulseiras identificadoras de funções físicas e de saúde e até geladeiras[8]: é inegável que a tecnologia torna nossas vidas mais convenientes. A popularização da IoT trouxe consigo uma nova forma de captação e produção inesgotável de dados dos usuários e nos parece inadequado e até ingênuo evitar tal coleta optando pela completa reclusão digital ou até mesmo a abolição de tal prática.

Diante desse contexto, surgem questionamentos: há uma política eficiente para a proteção de dados e privacidade das pessoas que utilizam tais objetos? Tais usuários de fato sabem que estão sendo rastreados? Ainda que soubessem da coleta de dados, estes estariam dispostos a renunciar a própria proteção à privacidade, em contrapartida aos benefícios

---

[5] Cerca de 41,76 bilhões de dispositivos ativos conectados à IoT (*Internet of Things* – Internet das Coisas) globalmente em 2023, o que, comparado com 2022, resulta em um impulso no crescimento de 18% nas conexões. A informação é de Renato Pasquini, Conselheiro Consultivo da Associação Brasileira de Internet das Coisas (Abinc) e vice-presidente da Pesquisa IoT, Edge e Serviços Digitais da Frost & Sullivan. Vide: OLIVEIRA, Marcos de. **(IoT): 41,76 bilhões de dispositivos ativos conectados globalmente em 2023**. Monitor Mercantil, maio. 2023. Disponível em: <"https://monitormercantil.com.br/iot-4176-bilhoes-de-dispositivos-ativos-conectados-globalmente-em-2023">. Acesso em: 23 de set. 2023.

[6] Há diversas divergências a respeito do conceito de IoT, não podendo ser definido de forma unânime. Para conferir o conceito adotado por este artigo, VER: MAGRANI, Eduardo. **A internet das coisas.** — Rio de Janeiro: FGV Editora, 2018. p 20.

[7] Ibid, 2018. p 15.

[8] A nova geração de geladeiras pode, além de refrigerar, ser controlada via *smartphone*s, emitir lembretes, conferir promoções e até mandar recados para membros da mesma família. VER: DENT, Steve. **Samsung 's latest smart fridge has cameras and a huge display: see your food without the hassle of opening the refrigerator door**. Disponível em: <"https://www.engadget.com/2016-01-04-samsung-family-hub-smart-fridge.html">. Acesso em: 3 out. 2023.

evidentes que a tecnologia os proporciona, justificando um *trade-off* com base na convivência pessoal?

Para Caitlin Mulholland[9], a resposta de grande parte das perguntas é não. De fato, muitos usuários cedem uma parcela de sua privacidade em prol da conveniência que a IoT os oferece, sem necessariamente ser informado para onde seus dados podem ser transferidos e não tendo uma ideia clara do impacto por traz de tal decisão. O desconhecimento (não só da privacidade, mas também sobre a interpretação do que é a internet de fato) é tamanho que é refletido em pesquisas: para 55% dos usuários brasileiros, o Facebook é a própria internet[10].

Dessa forma, o consentimento expresso, livre e informado concedido por estes usuários torna-se apenas uma ficção jurídica, haja vista que se trata de um falso consentimento, concedido apenas para o usuário tenha acesso ao produto[11].

É evidente a necessidade de um balanço adequado entre a privacidade do usuário e o ordenamento brasileiro, a fim de garantir a tutela não apenas à privacidade, mas também ao livre acesso à internet de forma segura e consciente. Para tanto, entendemos que é complexo o desafio entre a proteção mediada versus a constante inovação presente na sociedade digital.

Outras questões relevantes a serem solucionadas são: o que são dados propriamente ditos e como houve a supervalorização e mercantilização deles, assuntos estes que serão abordados adiante.

---

[9] MULHOLLAND, Caitlin. **A tutela da privacidade na internet das coisas (IoT).** Belo Horizonte: Casa do Direito; FGV – Fundação Getúlio Vargas, 2019 p. 482-490. Disponível em: <"https://igarape.org.br/wp-content/uploads/2019/06/Horizonte-presente-tecnologia-e-sociedade-em-debate.pdf">. Acesso em: 23 set. 2023. p 488.

[10] O estudo feito pelo site Quartz trouxe um dado alarmante: 55% dos brasileiros consideraram que o Facebook é a Internet. Ou seja, mais da metade dos entrevistados afirmou não perceber vida online fora da plataforma. VIDE: VALENTE, Jonas. **Internautas brasileiros acham que a internet se resume ao Facebook:** *Pesquisa revela que 55% dos brasileiros não percebem vida online fora da plataforma criada por Mark Zuckerberg,* jan. 2017. Disponível em: <"https://www.cartacapital.com.br/blogs/intervozes/internautas-brasileiros-acham-que-a-internet-se-resume-ao-facebook/">. Acesso em: 25 set. 2023.

[11] VENTURINI, J. [et al]. **Termos de uso e direitos humanos: uma análise dos contratos das plataformas on line.** No prelo. [S.l.: s.n.], 2016. p. 10.

2. BIG DATA: A ESPECIALIZAÇÃO DA TECNOLOGIA DA INFORMAÇÃO

Conforme já explicitado, a captação de dados tem se tornado cada vez mais frequente com o advento da IoT. Somados ao exponencial crescimento da nova sociedade digital, o barateamento de smartphones e o *cloud computing*[12] também contribuíram para o aperfeiçoamento das ferramentas de captação de dados.

O conjunto desses fatores propiciou o desenvolvimento do *big data*, que mesmo sem um consenso para sua definição, pode ser entendido como qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados que têm o potencial de ser explorados para obter informações[13]. Da mesma forma, o Instituto de Tecnologia & Sociedade do Rio traz uma concepção compreensível sobre a presente temática:

> "Podemos dizer que Big Data é, literalmente, o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores. Todas as ações e comunicações em plataformas digitais, como com telefones celulares, computadores ou mesmo transações de cartão de crédito e, mais recentemente, declarações de imposto de renda, ou ações que, em algum momento, são digitalizadas e assim transformadas em dados, como as câmeras de segurança associadas com software de reconhecimento facial ou de padrões, são passíveis de serem armazenadas, processadas, copiadas e distribuídas quase instantaneamente, possibilitando análises de dados que podem levar governos e empresas a tomar decisões supostamente melhor fundamentadas"[14]

Mayer e Padova[15] também definem o *big data* através da analogia de um quebra-cabeça: os dados, sozinhos, são desorganizados e não possuem valor. Quando distribuídos e combinados uns aos outros se tornam preciosos e até valiosas mercadorias.[16]

---

[12] Conforme elucidado por Cezar Taurion, é um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataformas, aplicações e serviços disponibilizados na internet. Para conferir o conceito, verificar: TAURION, Cesar. **Cloud computing: computação em nuvem transformando o mundo da tecnologia da informação.** Rio de Janeiro: Brasport, 2009, p. 02.

[13] IANE, Julia et al. (Ed.). **Privacy, big data and the public good: frameworks for engagement.** Nova York: Cambridge University Press, 2014.

[14] INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. **Big Data no Sul Global: Relatório sobre estudos de caso**. Rio de Janeiro: ITS, 2016, p. 9. Disponível em: <"https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf">. Acesso em: 30 set. 2023.

[15] MAYER-SCHANBERGER, Viktor; PADOVA, Yann. **Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation.** The Columbia Science & Technology Law Review, Columbia, Nova York, v. XVII, p. 320, Primavera 2016. Disponível em:<"https://researchgate.net/publication/303665079" >. Acesso em: 23 mai de 2023. No original: "*Moreover, the value of data can be greatly enhanced not only by having and analyzing more of it, but by combining it with other data sources. It is like a single puzzle piece that taken by itself offers little value, but when combined with others to complete an image is turned into something precious.*"

[16] Para alguns, os dados são o novo petróleo. Vide THIRANI, Vasudha; GUPTA, Arvind. **The value of data.** World Economic Forum, set. 2017. Disponível em: <"https://www.weforum.org/agenda/2017/09/the-value-

Contudo, a definição mais completa para *big data* é a de Doug Laney[17], analista da empresa META Group, que, em um relatório de pesquisa, criou a teoria dos três "Vs" do *big data*: volume, velocidade e variedade. O volume seria explicado pela grande quantidade de *megabytes*[18] que são produzidos diariamente através dos aparelhos eletrônicos dos quais utilizamos, a variedade, pela capacidade excedente de processamento desses dados (sejam fotos, vídeos ou texto), e a velocidade pois toda a captação é feita por ferramentas que trabalham com uma rapidez nunca vista.

Ainda, a doutrina jurídica ainda considera a existência de não três, mas, sim, seis "Vs":

> O modelo 6 Vs que descreve Big Data é: (i) volume (grande volume) geração e captura de dados em massa; (ii) velocidade (geração rápida, processamento de dados) - oportunidade de captura rápida de dados para maximizar sua utilidade; (iii) variedade (várias modalidades, tipos de dados) dos vários formatos de dados, nomeadamente, estruturados, semiestruturados e não estruturados; (iv) valor, que significa extrair valor de um grande volume de dados por meio de alta velocidade na captura e análise; (v) a veracidade, a confiabilidade dos dados obtidos para garantir a veracidade em suas análises para obter informações precisas; e (vi) validação, a capacidade de garantir que várias fontes de dados quando agrupadas façam sentido. (tradução livre) [19]

Nesse sentido, em complemento, é necessário diferenciar o *big data* (constituído, principalmente, por dados brutos) de informação. Dados necessitam de ferramentas para serem

---

ofdata">. Acesso em: 02 ago. 2023. Thirani e Gupta afirmam: "*To discuss and resolve these issues, it is imperative to be cognizant about the value of data. In this age of hyper connected consumers, data is definitely the new age 'oil*'" (em tradução livre: Para discutir e resolver esses problemas, é imperativo estar ciente sobre o valor dos dados. Nesta era de consumidores hiperconectados, os dados são definitivamente o novo "petróleo" da era). Para outros, os dados possuem valor superior ao do petróleo, vide: **The world's most valuable resource is no longer oil, but data:** the data economy demands a new approach to antitrust rules. The Economist, may. 2017. Disponível em: <"https://encurtador.com.br/mLP45">. Acesso em: 02 ago. 2023.

[17] LANEY, Doug. 3D data management: Controlling data volume, velocity and variety. Disponível em: <"https://studylib.net/doc/8647594/3d-data-management--controlling-data-volume--velocity--an…">. Acesso em: 10 de set. 2023.

[18] Megabyte se refere à unidade de medida de informação que equivale a 1.000.000 de bytes. Ele é usado para medir o tamanho da memória e do espaço de armazenamento de um hardware. VER: NASCIMENTO, Anderson. **O que é megabyte?** Canaltech, 01 de ago. 2014. Disponível em: <"https://canaltech.com.br/produtos/O-que-e-megabyte/">. Acesso em: 10 de set. 2023.

[19] BAGNOLI, Vicente. **The Big Data Relevant Market As a Tool for a Case by Case Analysis at the Digital Economy: Could the EU Decision at Facebook/WhatsApp Merger Have Been Different?** In: Ascola Conference. 2017. p. 8. No original: "*The 6 Vs model that describes Big Data is: (i) volume (great volume) generation and mass data capture; (ii) velocity (rapid generation, processing of data) the rapid data capture opportunity to maximize their usefulness; (iii) variety (various modalities, types of data) the various data formats, namely, structured, semistructured and unstructured; (iv) value, that means to extract value from a huge volume of data through highspeed in the capture and analysis; (v) veracity, the reliability of the data obtained to ensure the truth in their analysis to obtain accurate information; and (vi) validation, the ability to assure that multiple data sources when grouped make sense".*

captados e analisados em tempo hábil[20], enquanto a informação representa o subproduto dessa análise, gerando significado e conhecimento de algo ou alguém.

3. DADOS COMO MERCADORIA: UTILIZAÇÃO DO BIG DATA E DO DATAVEILLANCE POR AGENTES ECONÔMICOS

É inegável que o desenvolvimento das ferramentas de captação e aprimoramento do *big data* possuem grande valia tanto para corporações quanto para o Poder Público: seja para a formação de um perfil de consumo cada vez mais personalizado ou para a criação de políticas públicas menos custosas e convenientes, a informação é o subproduto mais valioso do atual sistema capitalista.

Assim como citado anteriormente, a real complexidade está entre a linha tênue entre privacidade, consentimento e compartilhamento de dados dos usuários que são reféns das atuais ferramentas digitais. Na atual sociedade da informação, disponibilizar o próprio *big data* incide o risco de ter seu direito à privacidade violado. Em contramão, não disponibilizar implicará na abdicação dos benefícios trazidos pela tecnologia.

A insegurança entre ceder ou não as próprias informações pessoais diante de um cenário oligárquico, somado à falta de uma legislação protetiva o suficiente ao usuário, acarretaram na criação de um movimento ativista pró-privacidade: o ciberativismo[21]. A fim de sanar a dúvida de quais informações estavam em posse da empresa *Facebook,* o ativista austríaco Max Schrems se surpreendeu com o resultado de sua solicitação: foram mais de mil e duzentas páginas de informações pessoais produzidas em três anos e com uso moderado da plataforma[22].

---

[20] MORAIS, Izabelly Soares de… [et al]. **Introdução a Big Data e Internet das Coisas (IoT).** – Porto Alegre: SAGAH, 2018. p. 14.

[21] QUEIROZ, Eliani de Fátima Covem Queiroz. **Ciberativismo: a nova ferramenta dos movimentos sociais.** Revista Panorama, Goiânia, v. 7, n. 1, p.5, jan./jun. 2017. Disponível em: <"https://seer.pucgoias.edu.br/index.php/panorama/article/view/5574/3064">. Acesso em: 03 de out. 2023.

[22] A informação repassada ao ativista incluía números de telefone e endereços de e-mail de amigos e familiares; o histórico de todos os dispositivos que ele usou para acessar o Facebook; todos os eventos a que ele tinha sido convidado; todo mundo que ele tinha adicionado como amigo (e posteriormente desfeito a amizade); e um arquivo com suas mensagens privadas e também havia transcrições de mensagens que ele tinha apagado. VIDE: CROSSLEY, Rob. **Como empresas de internet armazenam o que elas sabem sobre você?** 30 ago. 2016. Disponível em: <"https://www.bbc.com/portuguese/geral-37180722">. Acesso em: 03 out. 2023.

Em contramão, Kent Walker[23] defende o *trade-off*[24] (troca, em tradução livre) de privacidade com base na conveniência trazida pela tecnologia, dos quais apenas os malefícios são evidenciados pela mídia:

> É certamente mais fácil pintar um retrato simpático de Sandra Bullock capturada no filme A REDE, sobre roubo de identidade, do que avaliar os benefícios que milhões de pessoas estão tendo ao receberem produtos de forma mais barata e fácil, em função da manipulação ética e criteriosa de dados pessoais. Além disso, a privacidade é uma força romântica do individualismo heroico da oratória. Tais virtudes têm apelo junto a jornalistas, romancistas e articulistas. Mas os valores burgueses de conveniência, das comunidades, e da acessibilidade são também virtudes, pelo menos tão essenciais para o funcionamento da sociedade quanto à própria privacidade. Tais virtudes são tipicamente ignoradas pelos defensores da privacidade. (tradução livre)[25]

Nesse sentido, Mayer e Cukier[26] também defendem os aspectos positivos do recolhimento de dados, sejam eles a capacidade de personalizar experiências do usuário, oferecendo recomendações sob medida, ou até para obter diagnósticos, antes complexos, para relatórios médicos.

É fato: historicamente, a captação de dados para a formação de um perfil de consumo não é considerada como algo novo, tampouco a existência da assimetria de poder entre grandes empresas (hoje também chamadas de *Big Techs*) e usuários. O *big data* é para a sociedade da informação o que, no passado, foi o carvão para a sociedade industrial. Antes, aqueles que detinham as máquinas de produção era quem centravam e dominavam a economia. Agora, detém poder as empresas que possuem o aparato tecnológico-científico desenvolvido o suficiente para processar, armazenar e interpretar o *big data*, a fim de transformar em informação para detrimento e lucro próprio.

---

[23] WALKER, K. **Where Everybody Knows Your Name:** A Pragmatic Look at the Costs of Privacy and the Be nefits of Information Exchange. Stanford Technology Law Review. 2001.

[24] A título de entendimento, *trade-off*, em uma tradução mais completa, poderia ser definido como a escolha de uma opção em detrimento de outra.

[25] No original: "*It is certainly easier to paint a sympathetic portrait of Sandra Bullock captured in the film The Network, about identity theft, than to assess the benefits that millions of people are getting by receiving products more cheaply and easily, due to the ethical and judicious handling of personal data. Moreover, privacy is a romantic force of the heroic individualism of oratory. Such virtues appeal to journalists, novelists, and columnists. But the bourgeois values of convenience, communities, and accessibility are also virtues, at least as essential to the functioning of society as privacy itself. Such virtues are typically ignored by privacy advocates*." WALKER, K., op. cit. 2001. p. 04.

[26] MAYER-SCHONBERGER, Viktor; CUKIER; Kenneh. Big Data: **A revolution that will transform how we live, work and think**. New York: Houghton Mffin Hartcourt, 2013.

Embora tenham trazido conveniência para a vida cotidiana, muitas das ferramentas digitais fornecidas pelas *Big Techs* se aproveitam da falta de legislação regulamentadora em países menos desenvolvidos - e o próprio desconhecimento dos usuários - e capturam dados desenfreadamente, sem nenhum tipo de respeito aos direitos da privacidade e proteção de dados. Um exemplo pertinente e atual seria o caso do aplicativo *Face App*[27], dito gratuito, e que tinha a premissa de utilizar inteligência artificial para transformar as *selfies* fornecidas pelos usuários para a troca de gênero, torná-lo mais velho ou mais novo etc. No entanto, especialistas em segurança digital notaram que além da captura de imagem, o aplicativo também detinha a posse dos dados de navegação do celular. Sem que soubessem, os usuários tinham seus dados captados e vendidos para outras empresas a fim de gerar publicidade e propaganda.

Shoshana Zuboff explicita que a simples gratuidade dos aplicativos era um dos motivos de *trade-off* de privacidade e dados para grandes empresas, mesmo que isso custasse a concessão de dados pessoais:

> Por fim, as empresas começaram a explicar essas violações como um *quid pro quo* necessário em troca de serviços de internet "gratuitos". Segundo elas, privacidade era o preço a se pagar por abundantes prêmios de informação, conexão e outros bens digitais quando, onde e como fossem desejados. Essas explicações nos distraíram da mudança nas condições do mar que reescreveriam as regras do capitalismo e do mun do digital.[28]

No mesmo sentido, João Pedro Seefeld Pessoa[29] também aborda sobre o assunto, agregando a ideia de que a concentração de poder e capital é feita por meio da gratuidade dos aplicativos:

> Em outras palavras, o oferecimento de produtos e serviços, muitas vezes gratuitos, exige do usuário o fornecimento de dados pessoais, que não necessariamente servem para a própria existência do produto ou serviço que chega ao indivíduo, mas sim par a agregar valor à própria organização como nó social na malha do poder em rede.[30]

---

[27] TOLEDO, Giuliana de. **FaceApp rouba dados? Jogo volta à moda trocando gênero em fotos e reacende debate:** Entenda as críticas ao app que virou febre de novo na quarentena dos brasileiros: Procon-SP estuda notificar pela segunda vez Google e Apple, que oferecem o programa. O Globo. 17 de jun. 2020. Disponível em: <"https://oglobo.globo.com/cultura/faceapp-rouba-dados-jogo-volta-moda-trocando-genero-em-fotos-reacende-debate-24485207"> Acesso em: 04 de out. 2023.

[28] ZUBOFF, Shoshana. **A Era Do Capitalismo De Vigilância**: A Luta Por Um Futuro Humano Na Nova Fronteira Do Poder. Rio De Janeiro: Intrínseca, 2020. P.I, p. 72.

[29] PESSOA, João Pedro Seefeldt. **O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI**. Porto Alegre, RS: Editora Fi, 2020.

[30] Ibid. 2020, p. 92.

Para Shoshana Zuboff[31], esse interesse de obtenção de lucros a partir da captação de dados pessoais pelas *Big Techs* é o que pauta o capitalismo de vigilância. Considerada uma nova *commodity* do mundo moderno, a informação disponibilizada e captada pelos dispositivos eletrônicos, transformou-se em, além da análise e conjunto de dados, ativo comerciável. A vigilância de dados, também chamado *dataveillance*, pode ser definida pelo uso sistemático de dados pessoais na investigação e monitoramento de ações e comunicações de um ou mais indivíduos[32]

A autora destaca a participação fundamental da empresa Google como pioneira na disseminação do capitalismo de vigilância[33]. Depois de algum tempo tratando os dados providos das pesquisas dos usuários como verdadeiros resíduos digitais - chamados de *data exhaust* -, os engenheiros de computação criaram uma patente utilizada até hoje de utilizar as informações dos usuários para a realização de uma publicidade direcionada e personalizada[34].

Nas palavras da autora:

> [...] o Google não faria mais mineração de dados comportamentais estritamente para melhorar o serviço para seus usuários, e sim para ler as mentes destes afim de combinar anúncios com seus interesses, que, por sua vez, eram deduzidos dos vestígios colaterais do comportamento on-line. Com o acesso exclusivo do Google aos dados comportamentais, seria possível então saber o que um indivíduo específico, num tempo e espaço específicos, estava pensando, sentindo e fazendo. O fato de isso deixar de nos parecer surpreendente, ou talvez nem mesmo digno de nota, é prova do imenso entorpecimento psicológico que fez com que nos habituássemos a uma guinada audaz e sem precedentes nos métodos capitalistas.[35]

Ora, é evidente que a mineração[36] de dados feita pelas *Big Techs* é feita exclusivamente para a formação de melhores anúncios publicitários. O *big data*, antes considerado resíduo, hoje

---

[31] ZUBOFF, op. cit, p. 87.

[32] O termo *dataveillance* baseou-se na aglutinação das palavras *data (*dados, em tradução livre do inglês) e *surveillance* (vigilância, em tradução livre do inglês). VIDE: CLARKE, Roger. **Information technology and dataveillance**. Communications of the ACM, v. 31, n. 5, p. 498-512, maio 1988. Disponível em: <"https://dl.acm.org/doi/pdf/10.1145/42411.42413">. Acesso em: 09 de out. 2023. No original: "*Surveillance is the systematic investigation or monitoring of the actions or communications of one or more persons. Its primary purpose is generally to collect information about them, their activities, or their associates.*" (Tradução nossa).

[33] ZUBOFF, op. cit, p. 101.

[34] É possível conferir a informação na página "AdSense" da Google. VIDE: GOOGLE. **Como funcionam os anúncios personalizados.** Disponível em: <"https://support.google.com/My-Ad-Center-Help/answer/12155656?visit_id=638324756912080737-2456707626&rd=2#personalized-ads-on-google%20non-personalized-ads-on-google%20zippy=%2Ccom-o-adchoices%2Candroid-tv>". Acesso em: 09 de set. 2023.

[35] ZUBOFF, op. cit, p. 103.

[36] Para Zuboff, a mineração de dados, ou "*data mining*", inglês, foi uma operação realizada por Amit Pavel, funcionária da empresa Google, do qual eram analisadas as entradas de dados acidentais de usuários do Google, fazendo com que ela tivesse acesso a arquivos detalhados de cada usuário, como seus pensamentos, sentimentos, interesses; que podiam ser construídos a partir da navegação pelas buscas de pesquisa. VIDE: Ibidem. p. 87.

é armazenado de forma desenfreada, sendo inclusive protegido em salas com scanners biométricos de íris e equipes de segurança vigilantes 24h.[37]

É fato, o conjunto dos dados processados e analisados pelas ferramentas corretas produzem um capital tão valioso que parece compensar para as empresas a quebra de protocolos de segurança à própria privacidade do usuário e também um alto preço de custo para que haja a produção da publicidade direcionada (também chamado de "*data-driven marketing"*[38]*)*.

Resta claro que a gratuidade do usufruto do aplicativo ou serviço é mascarado pela coleta de dados, ou seja, a conclusão feita é que de fato não há nenhuma gratuidade pois o produto é o próprio usuário. "*Se algo não é de graça, você não é o consumidor, você é o produto*"[39].

Sob este contexto, o longa-metragem de 2017 "O Círculo"[40] (*The Circle*, no idioma original) explicita de forma clara através da personagem Mae Holland a complexidade do tema abordado. A jovem, atraída pelos benefícios concedidos pela maior empresa de tecnologia do mundo, entre eles ambientes de recreação exclusivos para funcionários, a boa remuneração, festas custeadas pela empresa etc., se depara com a ferramenta "*True You"*, que concentrava grande parte das informações dos usuários que utilizavam a plataforma. Entre as informações compartilhadas estavam fotos, e-mails, geolocalização precisa e até o histórico de votos para candidatos à política, já que a multinacional atuava em parceria com o Estado.

---

[37] É possível conferir a informação no próprio site da Big Tech Google. "*Nossos data centers contam com a proteção de diversas camadas de segurança para evitar qualquer tipo de acesso não autorizado aos seus dados. Usamos sistemas de defesa com perímetro seguro, uma cobertura abrangente de câmeras, autenticação biométrica e uma equipe de segurança 24 horas. Além disso, implementamos um controle de acesso e política de segurança rigorosos nos nossos data centers, garantindo um treinamento com foco em segurança para todos os funcionários*." VIDE: GOOGLE. **Dados e segurança: segurança é um assunto sério nos nossos data centers. Mantemos seus dados protegidos e seguros com o uso de diversos recursos de segurança**. Disponível em: <"https://www.google.com/intl/pt-BR/about/datacenters/data-security/">. Acesso em: 11 de out. 2023.

[38] MULVENNA, Maurice; NORWOOD, Marian; BUCHNER, Alex. **Data-Driven Marketing**. Electronic Markets.UK, v. 8:3, p. 32-35. 30 mar. 2006. Disponível em: <"https://www.tandfonline.com/doi/epdf/10.1080/10196789800000038?needAccess=true">. Acesso em: 11 de out. 2023.

[39] Em 1973, os artistas Richard Serra e Carlota Fay Schoolman divulgaram um curta-metragem chamado *Television Delivers People*, que critica a televisão como forma de comunicação para as massas. Originalmente, o slogan utilizado para a crítica do uso dos dados dos usuários era aplicado apenas ao serviço televisivo. KUNSTSPEKTRUM. **Richard Serra "Television Delivers People" (1973).** Youtube, 2 de fev. 2011. Disponível em: <"https://www.youtube.com/watch?v=LvZYwaQlJsg&ab_channel=KunstSpektrum"> Acesso em: 11 de out. 2023. No original, "*It is the consumer who is consumed. You are the product of T.V. You are delivered to the advertiser who is the customer. He consumes you. (minuto 1:09)*"

[40] **O CÍRCULO** (The Circle, no original). Filme. Direção: James Ponsoldt. Produção: Anthony Bregman. Intérpretes: Emma Watson, Tom Hanks, John Boyega e outros. Estados Unidos: STXFilms and EuropaCorp, 2017.

A principal crítica extraída no longa metragem é a relação de dualidade que a personagem principal vive de, além de ser vigiada e monitorada em tempo integral de trabalho, também convive com os mais íntimos dados de diversos usuários que utilizam a plataforma. O ponto ápice da violação à privacidade e proteção de imagem é demonstrado na transmissão em tempo real na morte de um dos personagens.

Em virtude disso, não restam dúvidas quanto ao valor de mercado do novo capital da sociedade da informação, o *big data,* e também sobre a constante vigilância por parte das grandes corporações. Tendo em vista todos os aspectos supramencionados, é de imprescritível a tutela da privacidade dos usuários, que não deve ser feita de forma branda, a fim de conter todos os aspectos negativos da coleta de dados, e ao mesmo tempo não protetiva demais, a fim de possibilitar a inovação da tecnologia, que, de certa forma, nos traz conveniência. De fato, são as corporações privadas que necessitam provar a imprescindibilidade, finalidade específica e legitimidade de coleta e tratamento de dados do indivíduo, e isso deve estar ainda mais claro em tempos de vigilância massiva.

4. DIREITO FUNDAMENTAL À PRIVACIDADE E À PROTEÇÃO DE DADOS: A ESCOLHA DE UM MODELO

Como já abordado, a privacidade é um direito fundamental que desempenha uma função cada vez mais crítica na era digital. Com o crescimento exponencial da coleta, armazenamento e análise de dados pessoais, o equilíbrio entre a proteção da privacidade dos usuários da Internet e as demandas legítimas por segurança na era do capitalismo de vigilância tornou-se um desafio.

A construção doutrinária sobre o direito à privacidade teve início, sobretudo, no artigo escrito pelos advogados Samuel D. Warren e Louis D. Brandeis[41] que conceituavam a privacidade como o direito de ser deixado só ("*right to be let alone",* no original). Ambos denunciavam como a fotografia, jornais e aparatos tecnológicos tinham invadido a vida privada e doméstica dos cidadãos norte-americanos, e que as "recentes invenções e novos métodos empresariais chamavam atenção para o próximo passo que precisa ser dado para a proteção da pessoa"[42].

[41] WAR–REN, Samuel; BRANDEIS Louis. **The right to privacy**, Harvard Law Review, v. 4, n. 5, p. 193-220, dez. 1890.
[42] Ibid, p. 195, tradução livre. ("*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'.*")

Contudo, o direito à privacidade apenas foi reconhecido como direito fundamental quando foi citado na Convenção para Proteção dos Direitos do Homem e das Liberdades Fundamentais em 1953, inspirada na Declaração Universal dos Direitos Humanos ocorrida em 1948. Fato é, conforme as tecnologias e a internet foram se desenvolvendo, também as legislações a respeito à proteção de dados e privacidade iam se aprimorando, chegando a passar por quatro gerações[43].

A primeira das quatro gerações de leis, composta por normas que refletiam o estado da tecnologia e a visão do jurista da época, tinha como objetivo regular um cenário de criação e gestão de bancos de dados (*data centers)* cujo Estado seria o principal atuante. Contudo, em decorrência da inexperiência do uso de tecnologias que ainda estavam em desenvolvimento, que ainda eram recentes demais para serem compreendidas, somadas à necessidade de permissões e autorizações constantes que deveriam ser solicitadas ao Estado, a primeira geração foi composta de princípios de proteção que foram considerados abstratos e rasos demais, pois se limitavam apenas aos aspectos computacionais, e não à tutela da proteção de dados do usuário em si.[44].

A constante criação de centros para processamento de dados tornou inviável que tais autorizações dependessem exclusivamente do poder estatal. Por conta disso, na segunda geração de leis, a estrutura dos bancos de dados teve a sua descentralização, ou seja, não é mais "fixada em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão"[45]. Em outras palavras, por conta da desconfiança dos cidadãos em fornecer as suas próprias informações ao controle estatal, foram criadas novas ferramentas para que o próprio cidadão controlasse a sua privacidade, e isso se daria com base no consentimento do uso das suas informações por terceiros.

Contudo, o modelo de leis da segunda geração tornou-se um complicado problema, pois o poder estatal, já descentralizado, considerava as informações pessoais dos cidadãos um requisito indispensável até para o próprio funcionamento, e a recusa do fornecimento dessas informações acarretaria em um colapso. Dessa forma, a terceira geração se preocupou em

---

[43] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Revista Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-
108, jul./dez. 2011. Disponível em:<"https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315". Acesso em: 17 out. 2023.

[44] Ibid. p. 96.

[45] Ibid. p. 97.

estabelecer que o cidadão revele seus dados, contudo, com determinada proteção jurídica, proporcionando o "*[...] o efetivo exercício da autodeterminação informativa [...]*"[46].

Por fim, a quarta e última geração de leis foi criada para superar as desvantagens da autodeterminação informativa trazida na terceira geração, pois esta era exercida apenas por um pequeno grupo de "indivíduos privilegiados que decidiam enfrentar os custos econômicos e sociais do exercício dessas prerrogativas"[47]. Dessa forma, com o intuito de aprimorar a proteção de dados de forma coletiva e idônea, foram criadas ferramentas jurídicas para que fosse substituída à autodeterminação informativa pela proteção de dados considerados sensíveis (por exemplo, relatórios médicos no setor de saúde ou sigilo para o crédito de consumo), independentemente do consentimento do detentor desses dados.

Doutrinariamente, para Stefano Rodotà[48], o direito à privacidade "*pode ser definido mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações*"[49]. Rodotà entende que o conceito de privacidade originado pelo conceito de "ser deixado só" está superado, haja vista que tal conceito se baseou no aspecto proteção à vida privada no sentido de proteção patrimonial, ou seja, havia uma inviolabilidade das informações presentes dentro da casa e estas necessitavam tutela para que não fossem compartilhadas com outras sem a própria autorização dos titulares desses dados.

Em destaque a respeito do direito à privacidade e ao direito à intimidade, disciplina Alexandre de Moraes:

> [...] o direito à privacidade ou à vida privada engloba o direito à intimidade. A intimidade relaciona-se às relações subjetivas e de trato íntimo de uma pessoa, suas relações familiares e de amizade, enquanto privacidade ou vida privada é mais ampla e envolve todos os relacionamentos sociais.[50]

Dessa forma, após uma breve exposição das premissas fundamentais do direito à privacidade, cabe prosseguir com a análise específica da legislação nacional relativo ao tema.

---

[46] Ibid. p. 98.
[47] *Ibidem*.
[48] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 92
[49] Ibid. p. 15.
[50] MORAES, Alexandre de. **Direito constitucional** - 13. ed. - São Paulo: Atlas, 2003. p. 53.

No ordenamento jurídico brasileiro, por sua vez, a tutela à privacidade dos indivíduos sob o aspecto de vista da esfera privada está presente na Constituição Federal, no rol dos direitos fundamentais elencados no art. 5°: o direito à inviolabilidade do sigilo da correspondência e das comunicações telegráficas, direito à informação, direito à garantia da inviolabilidade da intimidade e vida privada, direito ao habeas data.

Recentemente, houve a inclusão ao direito à proteção de dados pessoais na Constituição Federal com a Emenda Constitucional n° 115[51] em fevereiro de 2022, a inserção do inciso XXVI no artigo 21[52], fixando a competência de fiscalizar a proteção e tratamento de dados pe ssoais à União, e a adição do inciso LXXIX no artigo 5°[53].

O direito aos dados pessoais também foi citado de forma ainda que indireta no artigo 43 do Código de Defesa ao Consumidor ("CDC")[54], pois elenca o direito ao acesso do consumidor às próprias informações existentes em cadastros, fichas, registros e dados pessoais arquivadas e a garantia de retificação dessas informações caso seja necessário.

Carecendo de uma legislação própria a respeito do assunto, na gestão de Dilma Rousseff, o Brasil promulgou a Lei nº 12.965[55], datada de 23 de abril de 2014, que ficou amplamente reconhecida como o Marco Civil da Internet ("MCI"). Essa lei foi criada com a

---

[51] BRASIL. **Emenda Constitucional n° 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: <"https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais> Acesso em: 2 de out. 2023.

[52] BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: <" https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm">. Acesso em: 17 de set. 2023.

[53] "***Art. 21***. *Compete à União: XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei."* VIDE: BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: <" https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm">. Acesso em: 17 de set. 2023.

[54] *"**Art. 43**. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. **§ 1°** Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. **§ 3°** O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas"*. VIDE: BRASIL. **Lei Nº 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Diário Oficial da União, 1990. Disponível em: <"https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.html">. Acesso em: 2 de out. 2023.

[55] BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Dispõe sobre o Marco Civil da Internet no Brasil. Diário Oficial da União, Poder Executivo, Brasília, DF, 24 abr. 2014. Disponível em: <"https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html">. Acesso em: 17 out. 2023.

finalidade de estabelecer diretrizes para a utilização da Internet no país, estipulando princípios, garantias, direitos e responsabilidades para os usuários da rede, ao mesmo tempo que delineou as diretrizes para a intervenção do Estado nesse cenário.

Dois anos mais tarde, na União Europeia e no Espaço Econômico Europeu, foi implementado o Regulamento Geral sobre a Proteção de Dados ("RGPD"), que teve como propósito regulamentar a privacidade e a proteção de dados pessoais de todos os cidadãos e residentes nesta área geográfica. O RGPD permitiu que as pessoas tivessem maior controle sobre suas informações pessoais, ao mesmo tempo em que harmonizava as regulamentações de privacidade em toda a União Europeia.

O Brasil, seguindo uma trajetória semelhante, reconheceu que o Marco Civil da Internet já tratava de questões legais relacionadas ao ambiente virtual e crimes cibernéticos. No entanto, com a expansão do *big data* e seu compartilhamento, havia uma necessidade premente de abordar a questão do tratamento não só da informação, mas também de dados sensíveis dos usuários. Em resposta a essa demanda, a Lei nº 13.709[56], datada de 14 de agosto de 2018, foi promulgada, e ficou conhecida como a Lei Geral de Proteção de Dados ("LGPD").

5. LEI GERAL DE PROTEÇÃO DE DADOS COMO MEDIDA PROTETIVA DOS USUÁRIOS DE TECNOLOGIA NO BRASIL

A Lei Geral de Proteção de Dados, ou LGPD, é um marco significativo no cenário legal relacionado à privacidade e à proteção de dados pessoais no Brasil. Promulgada em 2018 e efetivada em setembro de 2020, a LGPD estabeleceu uma série de regras e diretrizes destinadas a garantir a segurança e o controle das informações pessoais dos cidadãos. Com o objetivo de regulamentar a proteção de dados e inspirada no modelo europeu de Regulamento Geral de Proteção de Dados ("GDPR"), a LGPD se preocupou em estabelecer alguns conceitos, dentre eles, o conceito de "dados pessoais" e de "dados sensíveis".

Nos termos do artigo 5°, inciso I, da LGPD, caracteriza-se como dado pessoal os dados com *"informação relacionada a pessoa natural identificada ou identificável"*[57] ou seja, trata-se dos dados que podem identificar um sujeito, podendo ser uma fotografia, nome, endereço,

[56] BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Poder Executivo, Brasília, DF, 15 ago. 2018. Disponível em: <"https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.html>". Acesso em: 17 out. 2023.
[57] Ibidem, art. 5°, inciso I.

geolocalização, CPF, etc. Rony Vainzof[58] destaca o fato da identificabilidade poder ser obtida também de forma indireta através do conjunto de outras informações, como é o caso do *Internet Protocol* (IP) que identifica apenas o número de rede de um computador, e isso, somado à outra informação, como, por exemplo, a idade daquele usuário, pode se tornar um fator identificável e, dessa forma, esse dado pessoal protegido pela LGPD.

Elencados no inciso II[59] do mesmo artigo, também estão os "dados sensíveis". São chamados desta forma pois possibilitam e revelam a origem étnica, etnia, convicção religiosa ou filosófica, opinião política, filiação sindical, questões genéticas, biométricas ou de saúde ou vida sexual do titular. Esses dados acabam recebendo uma maior tutela do legislador justamente por terem o potencial de, caso fossem compartilhados sem o consentimento do usuário, serem capazes de gerar estigmatizações e discriminações a determinados grupos sociais e causar danos não apenas à privacidade, mas também à imagem e direitos fundamentais do titular.

Contudo, embora elencadas as diferenças entre dado pessoal e dado sensível pela LGPD, entendemos que tais conceitos podem ser facilmente confundidos, uma vez que, embora se tratando de um dado pessoal comum, certamente o endereço de uma pessoa de grande relevância pública, se combinado e atrelado ao seu nome, outro dado pessoal comum, deverá se regido como um dado pessoal sensível. Ainda, a LGPD optou por não elencar como dado sensível o consumo de crédito e aspectos da personalidade do titular dos dados, o que entendemos que é um erro, visto que, a fins de exemplificação, a escolha de compras de artigos sacros pode revelar sobre convicções religiosas, filosóficas ou políticas; a compra de um medicamento que revela a condição médica e, mais além, a contratação de serviços ou a compra de produtos que revelem sobre a sexualidade de um sujeito.

Um dos principais exemplos dados por Bruno Ricardo Bioni[60] trata-se do caso *Target*[61], onde um senhor teve conhecimento da gravidez da sua filha adolescente com base nos cupons de desconto que ele recebia via correios. Utilizando o cadastro do pai, a adolescente alimentava

---

[58] VAINZOF, Rony; MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **COMENTÁRIOS AO GDPR: Regulamento Geral de Proteção de Dados da União Europeia.** 3ª ed. São Paulo: Thomson Reuters Brasil, 2021. P. 37-85.

[59] BRASIL, op cit, art. 5°, inciso II, 2018.

[60] BIONI, Bruno Ricardo**. Proteção De Dados Pessoais: A Função E Os Limites Do Consentimento** – 3. Ed. – Rio De Janeiro: Forense, 2021.

[61] DUHIGG, Charles. **How Companies Learn Your Secrets**. The New York Times Magazine. fev, 16. 2012. Disponível em: <" https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html">. Acesso em: 17 out. 2023.

o sistema de informação da loja realizando buscas no indexador sobre testes de gravidez e outros produtos para gestantes, inclusive realizando algumas compras via cartão de crédito.

Dessa forma, o algoritmo da empresa *Target*, a partir dos dados obtidos pelas buscas (dados inicialmente considerados como dados pessoais), acreditava que ali havia uma alta possibilidade de ter uma cliente gestante. Somado ao fator endereço, esses dados se transformaram em informação sensível, e resultaram na violação da privacidade da adolescente. Renato Leite Monteiro também discorre a respeito deste episódio:

> Desta forma, a empresa que convencer primeiro os pais a comprar em suas lojas terá clientes fiéis e que, consequentemente, lhe proporcionará lucros maiores. Por isso, em 2012, a empresa Target resolveu tentar descobrir quais de suas clientes estariam grávidas para que lhes fossem enviados cupons de desconto. Esse desafio foi dado a especialistas de marketing digital, que tinham acesso aos registros eletrônicos não só da página web da empresa, mas também coletados por serviços parceiros de propaganda direcionada e informações off-line, como localização geográfica, histórico empregatício, hábitos de leitura, etnia e outros dados que sozinhos não podem ter nenhum significado maior, mas quando agregados e interpretados, podem levar a conclusões de alto valor comercial. (...) A metodologia foi aplicada a cada compradora do sexo feminino, o que resultou em um enorme número de "possíveis grávidas", as quais receberam propaganda e descontos diferenciados. Por volta de um ano após a estratégia que começou a ser empregada pela Target, um homem adentrou em uma das lojas da cadeia questionando os motivos pelos quais a empresa estava enviando à sua filha cupons direcionados a mulheres grávidas. Afirmou que ela ainda era menor de idade e que não estaria carregando um bebê. Todavia, após retornar para casa e conversar com sua filha, esta afirmou estar grávida. Ou seja, a empresa soube da novidade antes mesmo que os pais da mãe por vir os informasse.[62]

Ainda, ressaltamos que não é necessário que o indivíduo seja completamente identificado para que haja a violação à privacidade. Como exemplo, temos um aplicativo de celular que coleta dados de localização GPS que pode rastrear os movimentos de um usuário, mesmo sem saber seu nome, ou até mesmo motores de busca como a empresa Google, que coletam informações de pesquisas na *web* e criam a publicidade direcionada mesmo sem saber a identidade de quem realizou as pesquisas.

Nesse sentido, o artigo 7° da LGPD discorre sobre as hipóteses de tratamento de dados: mediante consentimento do titular; para o cumprimento de obrigação legal ou regulatória por parte do controlador; pela administração pública para implementação de políticas públicas; realização de estudos por órgãos de pesquisa; para execução de contratos ou procedimentos preliminares do qual faça parte o titular e mediante seu pedido; para proteção da vida ou

---

[62] MONTEIRO, Renato Leite. D**a proteção aos registros, aos dados pessoais e às comunicações privadas**. In: DEL MASSO, Fabiano Dolenc; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (coord.). Marco Civil da Internet: Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. E-book.

incolumidade física do titular ou de terceiros; para a tutela quando for o caso de procedimento realizado por profissionais da saúde, serviços de saúde ou autoridade sanitária; para ao atendimento de legítima expectativa do controlador ou terceiro e desde que prevaleçam os direitos e liberdades do titular; e, finalmente, para a proteção do crédito.

Com destaque no inciso I do citado artigo, em relação ao tratamento fundamentado no consentimento, este deve ser concedido mediante uma manifestação de vontade livre, específica, informada e inequívoca do titular dos dados pessoais. Em outras palavras, o consentimento para o tratamento de dados é expresso pelo próprio titular.

Assim como verificado, a quarta geração de leis fez com que a autodeterminação afirmativa fosse equilibrada em relação ao próprio consentimento dado, pois a recusa deste acarretaria a falta de informações consideradas vitais para o funcionamento público. Da mesma forma ocorreu no inciso V do artigo 7°, pois este autoriza o tratamento de dados *"quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados*".

Vejamos, a partir da análise do inciso, é possível verificar que os dados são, de certa forma, essenciais para o contrato, tanto para o contratado quanto para o anuente. Para fins de exemplificação, em uma compra de mercadoria cuja entrega estabelecida é à domicílio, é preciso que o anuente forneça dados que sejam considerados necessários o suficiente para que ele seja identificado e a entrega seja feita. Contudo, há um juízo de valor inerente e apontado por Cíntia Rosa Pereira[63]. Seria lícito ao contratante condicionar o fornecimento de dados pessoais (ainda que considerados desnecessários) para o simples perfazimento do contrato?

> Havendo solicitação, no ato de contratar, de dados não necessários ao negócio, duas questões se levantam: primeiramente, se é lícito condicionar o perfazimento de um contrato, especialmente se de adesão ou de consumo, à concordância do aderente ou consumidor em fornecer dados pessoais desnecessários; em segundo lugar, como definir o quadro normativo que recai sobre esses outros dados.[64]

Em resumo, a LGPD, inspirada nas leis da quarta geração, opta pelo equilíbrio entre a livre concorrência e livre iniciativa ao decidir que o próprio usuário tenha a liberdade de

[63] DE LIMA, Cíntia Rosa Pereira. **Comentários à lei geral de proteção de dados**: Lei n° 13.709/2018, com alteração da lei n° 13.853/2019. São Paulo: Almedina, 2020. p. 144.
[64] Ibid. p. 145.

escolher entre fornecedores que lhe tomem os dados pessoais como parte de sua contraprestação, ou optar por outros que não exijam o *trade-off* de privacidade. O principal problema evidenciado por Cíntia Rosa[65] é a existência de setores oligárquicos da tecnologia, dos quais os principais atuantes (se não todos) apenas concederão o acesso ao serviço caso haja a entrega da própria informação pessoal (e, dependendo, informação sensível) do usuário. O *trade-off*, portanto, deixa de ser considerado uma escolha e passa a ser uma obrigação. A solução trazida pela autora para tal escolha legislativa seria a concessão de benefícios ao consumidor:

> Que benefícios o consumidor teria se, ao comprar uma geladeira, aceitasse fornecer informações não necessárias ao lojista? Ganhará bônus, descontos, brindes, pontos em programas de fidelização? Houvesse sido assegurado por lei o destaque e também a autonomia entre os dois negócios – a aquisição de bens e serviços, de um lado, e a entrega dos dados desnecessários, de outro – não haveria qualquer prejuízo à livre concorrência, pois daria margem a uma outra livre concorrência sobre o fornecimento dos dados extras. Desse modo, ao mesmo tempo em que a parte mais fraca se veria protegida contra eventuais abusos, para que possa adquirir produtos e serviços no mercado sem precisar fornecer dados pessoais desnecessários ao negócio, ela não estaria impedida de voluntariamente fornecê-los em troca de algum benefício que a interesse, proposto pelo fornecedor de forma individualizada e independente do negócio principal.

No que diz respeito à fiscalização, implementação e zelo ao cumprimento da Lei em território nacional, a LGPD determinou no artigo 5°, inciso XIX, e nos artigos 55-C em diante, a Autoridade Nacional de Proteção de Dados ("ANPD"). Tal como previsto no SERPRO[66], a finalidade inicial da ANPD é orientar, de forma preventiva, os agentes de tratamento de dados. Caso seja necessário, fiscalizar, advertir e, somente após o descumprimento completo, a penalização dos responsáveis caso a LGPD ainda continue sendo descumprida. Da mesma forma, também foi criado o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade ("CNPD") e, conforme expresso no artigo 58-B da LGPD, são competências exclusivas do CNPD, respectivamente, (i) propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD, (ii) elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (iii) sugerir ações a serem realizadas pela ANPD, (iv) elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais

---

[65] Ibidem.
[66] GOVBR. "**QUEM VAI REGULAR A LGPD?**". Disponível em:<"https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd">. Acesso em: 17 out. 2023.

e da privacidade e, por fim, (v) disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

Quanto às sanções administrativas previstas na LGPD, previstas no Capítulo VII, são elencadas entre advertências e multas com percentual de até 2% do faturamento da empresa ou R$50.000.000,00 (cinquenta milhões de reais) caso a porcentagem do faturamento ultrapasse esse valor. Embora a LGPD elenque como penalidade máxima o encerramento de atividades do tratamento de dados ao agente que cometer as ilicitudes previstas em lei, entendemos, aqui, que embora a LGPD elenque multas de alto valor, isso não representaria uma proporção justa ao direcionamento efusivo da proteção de dados. Qual seria valor determinante para um dado sensível compartilhado sem restrições? Somente o titular dos dados saberá.

Nesse sentido, é necessário ressaltar duas decisões judiciais brasileiras consideradas como marcos na conscientização sobre a proteção de dados pessoais. Uma delas é a Apelação Cível 1.0000.19.061299-4/001/MG[67], da qual a empresa Netshoes foi sentenciada pela 11ª Câmara Cível de Minas Gerais a pagar a quantia de R$500.000,00 (quinhentos mil reais) a título de indenização de danos morais coletivos por conta de um vazamento de dados internos dos consumidores. Foi firmado um Termo de Ajuste de Conduta a pedido do Ministério Público do Distrito Federal e Territórios (“MPDFT”). O caso, na época, ficou conhecido pelo número de clientes afetados: mais de 1 milhão de pessoas tiveram o nome, CPF, endereço e informações de compras disponibilizadas na internet. A outra decisão, também proferida pelo MPDFT, foi o Recurso Especial n° 1.652.187DF[68], cujo Recorrido tratava-se da Serasa Experian (SERASA). A empresa, que atua principalmente em soluções de crédito e negócios, foi sentenciada a proibição de venda de dados pessoais de seus consumidores. O principal produto

---

[67] MINAS GERAIS. Tribunal de Justiça de Minas Gerais (11ª Câmara Cível). **Apelação Cível 1.0000.19.061299-4/001/MG**. Ementa: APELAÇÃO CÍVEL - AÇÃO DE INDENIZAÇÃO - VIOLAÇÃO DE SIGILO DE DADOS POR ATAQUE CIBERNÉTICO - DANO MORAL CONFIGURADO - REDUZIR VALOR DA INDENIZAÇÃO. - As consequências que decorreram da invasão dos dados cadastrais da autora por terceiros desautorizados, causaram abalos moral, passíveis de reparação. - Em acordo com as peculiaridades do caso, entendo que o valor da indenização fixada pelo juiz sentenciante deve ser reduzido, O que proporciona a reparação pecuniária do dano à ofendida e o efeito pedagógico ao ofensor, evitando-se a reiteração de condutas dessa natureza, sem que haja enriquecimento ilícito sem causa. Relatora: Des.(a) Shirley Fenzi Bertão. Apelante: NS2.COM INTERNET S.A. - NETSHOES. Apelado: NELY REZENDE MILITAO DE ASSIS HORTA. DDJE: 14/08/2019. Data de publicação: 19/08/2019. Disponível em: <"https://www5.tjmg.jus.br/jurisprudencia/pesquisaPalavrasEspelhoAcordao.do?&numeroRegistro=1&totalLinhas=1&paginaNumero=1&linhasPorPagina=1&palavras=viola%E7%E3o%20sigilo%20dados%20ataque%20cibern%E9tico&pesquisarPor=ementa&orderByData=2&referenciaLegislativa=Clique%20na%20lupa%20para%20pesquisar%20as%20refer%EAncias%20cadastradas...&pesquisaPalavras=Pesquisar&'">. Acesso em: 30 de out. 2023.

[68] BRASIL. Superior Tribunal de Justiça. **RECURSO ESPECIAL Nº 1.652.187.** Disponível em: <"https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201700244268">. Acesso em: 30 de out. 2023.

comercializado pela empresa aos seus compradores era a “Lista Online de Prospecção de Clientes”, que fornecia os dados de mais de 150 milhões de pessoas com o valor de R$0,98 (noventa e oito centavos) por consumidor. O MPDFT alegou a violação de dispositivos da LGPD por conta da violação do consentimento dos consumidores em terem seus dados comercializados à demais empresas.

> DECISÃO: O MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS (MPDFT) propôs ação civil pública contra o SERASA EXPERIAN (SERASA), objetivando a declaração de abusividade da conduta da ré em não permitir que o consumidor exerça o direito de correção da informação, quando proveniente de compartilhamento de dados com outras instituições, e se abster de comunicar aos consumidores a qualificação dos bancos de dados com os quais compartilha suas informações. O Juízo de piso julgou parcialmente a ação para: Ao teor do exposto, JULGO PROCEDENTE EM PARTE o pedido formulado na petição inicial para condenar a requerida à obrigação de comunicar ao consumidor, por ocasião de sua notificação de inscrição negativa, a qualificação dos bancos de dados com os quais será compartilhada a informação, sob pena de multa de R$ 1.000,00, a cada descumprimento comprovado nos autos. Em razão da sucumbência recíproca equivalente, condeno as partes ao rateio das custas processuais e honorários advocatícios, estes fixados em R$ 2.500,00 (dois mil e quinhentos reais), compensando-se na forma do art. 21 do CPC/73 (e-STJ, fl. 320). O apelo do SERASA não foi provido, enquanto o apelo do MPDFT foi provido em acórdão assim ementado APELAÇÃO CÍVEL. AÇÃO CIVIL PÚBLICA. CONSUMIDOR. CADASTRO NEGATIVO. COMPARTILHAMENTO DE DADOS POR ESPELHAMENTO. INFORMAÇÃO AO CONSUMIDOR. PROIBIÇÃO DE DIVULGAR DADOS POR QUEM NÃO PODE RETIFICÁ-LOS. EFEITOS TERRITORIAIS DA SENTENÇA. 1. Não se exige o domínio sobre o registro da informação para caracterizar o compartilhamento (ato de compartilhar); basta passá-la adiante. O fato de que os registros constantes na base de dados da SERASA são informados aos que consultam o SPC por um método chamado "espelhamento", ou qualquer outro nome que se lhe dê, não descaracteriza a existência de um compartilhamento de informações, ainda que em um grau mais superficial do que aquele que seria visto caso uma instituição pudesse promover alterações no banco de dados da outra. 2. O e. Superior Tribunal de Justiça, sem debater a existência de eventual lacuna no Código de Defesa do Consumidor a exigir complementação por analogia, mais do que reconhecer a possibilidade, proclamou que a Lei do Cadastro Positivo "deve ter aplicação conjunta com o CDC, sempre na postura hermenêutica do diálogo das fontes e de uma análise sistemática do ordenamento jurídico, principalmente no tocante às normas mais vantajosas e protetivas ao consumidor" (REsp 1297044/SP, Rei. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 20/08/2015, DJe 29/09/2015 grifei). 3. Não se pode olvidar que a divulgação das informações contidas no banco de dados da requerida em outras entidades de mesmo viés, implica em maior publicidade de dados negativos relativos ao consumidor. Por esta razão, deve este ter ciência ampla e irrestrita do alcance que as informações inseridas no sistema da requerida podem atingir. 4. A divulgação do registro da inscrição em cadastro de inadimplentes e ato que gera constrangimento ao consumidor, razão pela qual só pode ser realizada por quem dispõe dos meios necessários para alterar as informações constantes do banco de dados. 5. Quem cria e administra banco de dados de inadimplemento responde pelos danos que podem ser causados por eventual equívoco dos registros. Não se pode admitir que determinada instituição atue apenas na "ponta da cadeia", comodamente divulgando informações de bancos de dados que não administra, e, quando confrontada com violação ao direito do consumidor, decorrente de propagação de informação inverídica, busque isentar-se de qualquer responsabilidade afirmando que apenas "espelhou" dados provenientes de outra instituição. 6. Mais do que impedir uma interpretação restritiva do alcance dos instrumentos de tutela coletiva, e acima de se conceder, cm causas envolvendo

> relações de consumo, primazia ao art. 103, inciso III, do CDC, sobre o art. 16 da LACP, o e. STJ já esclareceu que não há que se falar em sentença que não produza efeitos em determinada parte do território nacional. Neste sentido, "pode-se afirmar, com propriedade, que determinada sentença atinge ou não esses ou aqueles sujeitos (alcance subjetivo), ou que atinge ou não essa ou aquela questão fático-jurídica (alcance objetivo), mas é errôneo cogitar-se de sentença cujos efeitos não são verificados, a depender do território analisado" (REsp 1243887/PR, Rei. Ministro LUIS FELIPE SALOMÃO, CORTE ESPECIAL, julgado em 19/10/2011, DJe 12/12/2011 grifei). 7. Negou-se provimento ao apelo da ré. Brasília-DF, 30 de novembro de 2018. Ministro MOURA RIBEIRO. (REsp n. 1.652.187, Ministro Moura Ribeiro, DJe de 06/12/2018.)[69]

Por conseguinte, torna-se evidente que os objetivos da LGPD não se direcionam para a proibição ou restrição da circulação de dados. O propósito da lei é claramente contrário a essa premissa. Na realidade, a lei visa estabelecer mecanismos que regulamentem a proteção de dados de acordo com os princípios da autodeterminação informativa, permitindo assim que os titulares de dados pessoais tenham uma efetiva oportunidade de questionar a legitimidade do tratamento de seus dados.

6. CASOS RELEVANTES

Precedentemente, é notório estabelecer que os casos que serão discutidos a seguir constituem apenas uma seleção específica feita com o propósito de exemplificar o contexto apresentado nos capítulos anteriores, sendo que de forma alguma busca-se o esgotamento das ocorrências enfrentadas pela violação da proteção de dados e direito à privacidade.

Os dois casos foram escolhidos por conta do seu impacto midiático, tanto no território nacional quanto de forma internacional. O primeiro caso trata-se de um dos maiores vazamentos de dados com influência política dos Estados Unidos; já o segundo, refere-se à violação de dados sensíveis a uma criança no Brasil, cujo viés político também foi considerado um fator relevante.

6.1 CAMBRIDGE ANALYTICA

Um dos principais casos relacionados ao vazamento de dados foi o caso da empresa Cambridge Analytica, cuja principal especialidade tratava-se da análise de dados para fins de estratégia política. De acordo com uma denúncia feita pelos jornais The New York Times e The

[69] Ibidem.

Guardian[70], a empresa teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas.

Os dados foram coletados por meio de um aplicativo denominado *"This is Your Digital Life" (*essa é a sua vida digital, em tradução livre em português) que, por meio de um pequeno questionário, tinha o algoritmo programado para criar um perfil de personalidade dos usuários. No início do teste, o aplicativo solicitava permissão para coletar os dados pessoais do participante, mas também solicitava a coleta dos dados dos amigos do participante sem o consentimento destes, o que era permitido pelo Facebook, desde que para fins acadêmicos. Foi descoberto que a empresa havia obtido ilegalmente dados pessoais de 50 milhões de usuários[71] do Facebook, cujos dados foram usados para criar perfis psicográficos e direcionar mensagens políticas altamente personalizadas durante a campanha presidencial dos Estados Unidos em 2016, entre outros eventos políticos, como o "Brexit" (Saída do Reino Unido da União Europeia), na Inglaterra.

O escândalo gerou preocupações significativas sobre a privacidade dos dados dos usuários do Facebook e levou a uma série de investigações e audiências no Congresso dos EUA. Estima-se que dois dias após a publicação feita pelos jornais, o valor do Facebook teve a redução de US$ 35 bilhões (ou aproximadamente R$ 115,5 bilhões) na bolsa de valores de tecnologia dos EUA. Como resultado, a Cambridge Analytica fechou suas operações e o Facebook implementou mudanças em suas políticas de privacidade e acesso a dados de terceiros.

6.2 VAZAMENTO DE DADOS DE PACIENTE NO ESPÍRITO SANTO

No Brasil, um dos casos mais dramáticos envolvendo o vazamento de dados é a de uma menina de dez anos, grávida em decorrência de um estupro (cujos abusos começaram no auge

---

[70] CONFERIR: CADWALLADR, Carole; HARRISON-Graham, Emma. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach:** Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters. The Guardian, USA, 17 de mar. 2018. Disponível em: <"https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election">. Acesso em: 10 de out. 2023. E também: ROSENBERG, Mattew. **Cambridge Analytica and Facebook: The Scandal and the Fallout So Far**. The New York Times, USA. 2018. Disponível em: <"https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html">. Acesso em: 10 de out. 2023.

[71] **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de a utoridades**. G1, 20 de mar. 2018. Disponível em: <"https://abrir.link/jlQjJ">. Acesso em: 10 de out. 2023.

dos seus seis anos pelo seu próprio tio) no Espírito Santo[72]. Em 16 de agosto de 2020, por meio da rede social Twitter, a ativista de extrema-direita Sara Giromini (conhecida como Sara "*Winter*") expôs diversos dados sensíveis da paciente, como nome completo, idade, e até mesmo o endereço do novo hospital do qual seria realizado o procedimento abortivo, este em conformidade com a decisão proferida pelo Tribunal de Justiça do Espírito Santo[73].

Dentre as violações causadas, podemos citar o inciso II, do artigo 2° da Lei n° 12.965/14 (Marco Civil da Internet), que dispõe que o uso da internet no Brasil deve ter como um de seus fundamentos "*os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais*"; o artigo 325 do Código Penal, a respeito do crime de violação de sigilo funcional, além de diversos dispositivos do Estatuto da Criança e do Adolescente, em destaque os artigos 5°, 17 e 143.

Além da quebra do anonimato, houve também a violação da proteção de dados sensíveis da criança que, em seu momento de maior vulnerabilidade em decorrência de um crime grave, necessitou de amparo da equipe médica em decorrência do grande volume de pessoas reunidas na porta do hospital em uma tentativa de impedir o procedimento. Dentre essas pessoas estava a imprensa, dois representantes do Ministério da Mulher, da Família e dos Direitos Humanos (ministério, na época, sob responsabilidade da então ministra Damares Alves) e também membros de grupos de extrema-direita e fanáticos religiosos[74].

CONCLUSÃO

No presente artigo, foi verificado que a sociedade da informação é constantemente impulsionada pela disseminação de novas tecnologias. Seja na indústria, nas ferramentas de comunicação, na área médica e até na maneira de como os objetos são enxergues através da Internet das Coisas; é impossível criar uma barreira ou empecilho para o desenvolvimento. É inegável: a tecnologia torna a vida humana conveniente. Entretanto, o preço pago por essa

[72] SOUSA, Thaís. **Ministério Público instaura inquérito sobre vazamento de dados de menina de 10 anos vítima de estupro.** O Globo. 06 de nov. 2023. Disponível em: <"https://oglobo.globo.com/brasil/ministerio-publico-instaura-inquerito-sobre-vazamento-de-dados-de-menina-de-10-anos-vitima-de-estupro-24590864">. Acesso em: 10 de out. 2023.
[73] DALVI, Bruno; MARCONDES, Luiza. **Justiça autoriza interrupção de gravidez de criança estuprada no ES**. G1. 15 de out. 2020. Disponível em: <"https://g1.globo.com/es/espirito-santo/noticia/2020/08/15/justica-autoriza-interrupcao-de-gravidez-de-crianca-estuprada-em-sao-mateus-no-norte-do-es.ghtml">. Acesso em: 10 de out. 2023.
[74] Ibidem.

conveniência tecnológica são os rastros deixados ao serem utilizadas tais ferramentas. O ser humano é uma fonte inesgotável de *big data* e informação, e cada vez mais é regido por algoritmos que analisam, compreendem e tomam decisões.

Sob esse contexto, este artigo verificou que o simples fato do ser humano ser produtor de informação faz parte de sua própria natureza. Desde a pré-história por meio de artes rupestres; aos autorretratos por meio de pinturas ou esculturas renascentistas e até à invenção da câmera fotográfica - hoje, aperfeiçoada e com melhores resoluções - o ser humano, em si, vive para ser lembrado e retratar o que vive.

Por outro lado, a partir do quarto capítulo, este artigo verificou o quanto o *big data*, quando processado e analisado pelas ferramentas corretas, se torna valioso quando transformado em informação. Somado ao exponente comercial e econômico, as principais oligarquias digitais se aproveitam de fragilidades do usuário, mesmo que custe a violação de direitos à privacidade, a troco de um mercado cada vez mais lucrativo.

Por meio deste trabalho foi verificado que os desafios perante o capitalismo de vigilância não são tão fáceis de serem solucionados. A disparidade de poder entre as oligarquias, *Big Techs* e usuários é tamanha que foram necessários anos de produção legislativa a fim de proteger o usuário, resultando na criação da Lei n° 13.709/18, inspirada nos moldes europeus, e que revolucionou a forma como tratamos os direitos à intimidade, imagem, proteção de dados e privacidade.

No entanto, o atual trabalho verificou que apenas a proteção legislativa não é suficiente, haja vista que a revolução tecnológica e a produção normativa andam em velocidades completamente distintas. A cibersegurança não depende apenas da anuência das empresas e oligarquias, mas também da própria conscientização do usuário a partir do momento em que ele consente em disponibilizar os seus dados. Para Shoshana Zuboff, o sucesso de normas regulatórias depende da interpretação e atuação das sociedades por movimentos populares. Da mesma maneira que antes, em meio à Revolução Proletária, trabalhadores buscavam melhores condições de trabalho e salários justos, hoje, "*os usuários terão que se mobilizar para reiterar as condições de existência humanas no presente século*"[75].

[75] ZUBOFF, op cit. 2020. p. 570.

Por meio deste artigo também foram verificados alguns artigos e incisos da LGPD, ressaltando a sua relevância como principal fonte normativa de proteção de dados dos usuários de internet no Brasil em 2023. Em complemento, analisou-se o fato da LGPD não ter tomado o caminho de proibir ou limitar a inovação tecnológica, pelo contrário, esta determinou a proteção de privacidade com base na instituição de princípios e mecanismos que asseguram aos usuários a proteção de suas próprias informações, respeitando a autodeterminação afirmativa do titular de dados.

Em contramão, foram encontradas algumas disparidades normativas quanto à definição de conceitos e às sanções impostas ao cometimento de ilicitudes. Cabe questionar ao leitor: seria possível quantificar o valor de proteção de um dado sensível espalhado, publicado e viralizado em redes sociais sem o consentimento do usuário, ainda mais sob o contexto de oligarquias que dominam a economia mundial? Qual seria o preço justo e quantificado a fim de determinar a responsabilidade em reparação de evidente dano? Estas são questões que este artigo não consegue alcançar.

Por tudo pelo que foi exposto acima, e em respeito ao questionamento inicial produzido por este artigo, é possível definir que o usuário de internet no Brasil, atualmente, em 2023, não está completamente protegido, haja vista o constante monitoramento de dados e a própria existência de um *trade-off* de privacidade para que este mesmo usuário consiga ter sua parcela de participação na era digital.

Em contraponto, também foi compreendido por meio deste trabalho que a reclusão digital não é a melhor opção a ser tomada e, mais do que isso, o conceito de união da própria sociedade e usuários, abordado anteriormente por Shoshana Zuboff, torna-se imprescindível para que as discussões sobre a privacidade e proteção de dados dos usuários sejam mais bem compreendidas.

REFERÊNCIAS BIBLIOGRÁFICAS

ANGELONI, Maria Terezinha. **ELEMENTOS INTERVENIENTES NA TOMADA DE DECISÃO**. Ci. Inf., Brasília, v. 32, n. 1, p. 17-22, Apr. 2003. Disponível em: <"http://www.scielo.br/scielo.php?script=sci_arttext&pid=S010019652003000100002&lng=en&nrm=iso">. Acesso em 25 set. 2023.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. **STATE SURVEILLANCE OF COMMUNICATIONS IN BRAZIL AND THE PROTECTION OF FUNDAMENTAL RIGHTS**. Electronic Frontier Foundation/ Internetlab, 2016. Disponível em: <"https://necessaryandproportionate.org/country-reports/brazil/twenty-sixteen/"> Acesso em: 5 maio. 2023

BAGNOLI, Vicente. T**HE BIG DATA RELEVANT MARKET AS A TOOL FOR A CASE-BY-CASE ANALYSIS AT THE DIGITAL ECONOMY: COULD THE EU DECISION AT FACEBOOK/WHATSAPP MERGER HAVE BEEN DIFFERENT?** In: Ascola Conference. 2017.

BAUMAN, Zygmunt. **VIGILÂNCIA LÍQUIDA**. Diálogos com David Lyon. Zahar Editora, 2014.

BIONI, Bruno Ricardo**. PROTEÇÃO DE DADOS PESSOAIS: A FUNÇÃO E OS LIMITES DO CONSENTIMENTO** – 3. Ed. – Rio De Janeiro: Forense, 2021.

BRASIL. **CONSTITUIÇÃO (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **EMENDA CONSTITUCIONAL N° 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: <"https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais"> Acesso em: 2 de out. 2023.

BRASIL. **LEI 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DE. 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.html>. Acesso em: 23 de abril de 2023.

BRASIL. **LEI 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 23 de abril de 2014. Disponível em: <"https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm">. Acesso em: 05 de maio de 2023.

BRASIL. **LEI Nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Poder Executivo, Brasília, DF, 15 ago. 2018. Disponível em: <"https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>". Acesso em: 17 out. 2023.

BRASIL. **LEI Nº 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Diário Oficial da União, 1990. Disponível em: <"https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm">

BRASIL. **PROJETO DE LEI Nº 4.060/2012**, de 13 de junho de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 23 de abril de 2023.

BRASIL. **PROJETO DE LEI Nº 5.276-A/2016**, de 24 de maio de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=3722DA20DAD%C2%A0%20A5FA1763A410EA5E11273.proposicoesWeb2?codteor=1470541&filename=Avulso+-%20PL+5276/2016>. Acesso em: 23 de abril de 2023.

CADWALLADR, Carole; HARRISON-Graham, Emma. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach:** Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters. The Guardian, USA, 17 de mar. 2018. Disponível em:

<"https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election">. Acesso em: 10 de out. 2023.

CASTELLS, Manuel. **A SOCIEDADE EM REDE**. Rio De Janeiro: Paz E Terra, 2018

CERNEV, A. K.; DINIZ, E. H. **PALMAS PARA O E-DINHEIRO! A EVOLUÇÃO DIGITAL DE UMA MOEDA SOCIAL LOCAL. REVISTA DE ADMINISTRAÇÃO CONTEMPORÂNEA**, v. 24, n. 5, p. 487–506, set. 2020.

CLARKE, Roger. **INFORMATION TECHNOLOGY AND DATAVEILLANCE**. Communications of the ACM, v. 31, n. 5, p. 498-512, maio 1988.

CROSSLEY, Rob. **COMO EMPRESAS DE INTERNET ARMAZENAM O QUE ELAS SABEM SOBRE VOCÊ?** *30* ago. 2016. Disponível em: <"https://www.bbc.com/portuguese/geral-37180722">. Acesso em: 03 out. 2023.

DAHLMANN, A; Venturin Dickow, M.; Maciel, M. **PRIVACY AND SURVEILLANCE IN THE DIGITAL AGE: A COMPARATIVE STUDY OF THE BRAZILIAN AND GERMAN LEGAL FRAMEWORKS**, mar. 2016. Ino Prelo.

DALVI, Bruno; MARCONDES, Luiza. **Justiça autoriza interrupção de gravidez de criança estuprada no ES**. G1. 15 de out. 2020. Disponível em: <"https://g1.globo.com/es/espirito-santo/noticia/2020/08/15/justica-autoriza-interrupcao-de-gravidez-de-crianca-estuprada-em-sao-mateus-no-norte-do-es.ghtml">. Acesso em: 10 de out. 2023.

DE LIMA, Cíntia Rosa Pereira. **COMENTÁRIOS À LEI GERAL DE PROTEÇÃO DE DADOS**: Lei n° 13.709/2018, com alteração da lei n° 13.853/2019. São Paulo: Almedina, 2020. p. 144.

DENT, Steve. **SAMSUNG'S LATEST SMART FRIDGE HAS CAMERAS AND A HUGE DISPLAY: SEE YOUR FOOD WITHOUT THE HASSLE OF OPENING THE REFRIGERATOR DOOR**. Disponível em: <"https://www.engadget.com/2016-01-04-samsung-family-hub-smart-fridge.html">. Acesso em: 3 out. 2023.

DONEDA, Danilo. **A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL**. Revista Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

Disponível em: <”https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315”. Acesso em: 17 out. 2023.

DUFF, Alistair A. **INFORMATION SOCIETY STUDIES.** Londres: Routledge: 2000; MASUDA, Yoneji. **THE INFORMATION SOCIETY AS POST-INDUSTRIAL SOCIETY.** Tóquio: Institute for the Information Society, 1980;

DUHIGG, Charles. **HOW COMPANIES LEARN YOUR SECRETS**. The New York Time s Magazine. fev, 16. 2012. Disponível em: <” https://www.nytimes.com/2012/02/19/magazine /shopping-habits.html”>. Acesso em: 17 out. 2023.

EFF; Internetlab. **QUEM DEFENDE SEUS DADOS?** Disponível em: <”https://internetlab.org.br/pt/projetos/quem-defende-seus-dados”>. Acesso em: 5 maio. 2023.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o coloco u na mira de autoridades. G1, 20 de mar. 2018. Disponível em: <"https://abrir.link/jlQjJ”>. Acesso em: 10 de out. 2023.

FILHO, A.5.; Schwartz, D.; André. G. Big Data — **BIG PROBLEMA! PARADOXO ENTRE O DIREITO À PRIVACIDADE E O CRESCIMENTO SUSTENTÁVEL**. Conpedi Law Review, V. 2, N. 3, P. 311-331, jun. 2016. Disponível Em:<”https://portaltutor. com/Index.Php/Conpedireview/Article/View/314”>, Acesso em: 5 maio. 2023.

GAZOLLA, Frederico. **DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO E O PÓS-PANOPTISMO: UMA ANÁLISE SOBRE PRIVACIDADE E REGULAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS** - São Paulo: Editora Dialética, 2021.

GOOGLE. **COMO FUNCIONAM OS ANÚNCIOS PERSONALIZADOS.** Disponível em: <”https://support.google.com/My-Ad-Center-Help/answer/12155656?visit_id=638324756912 080737-2456707626&rd=2#personalized-ads-on-google%20non-personalized-ads-on-google%20zippy=%2Ccom-o-adchoices%2Candroid-tv”>. Acesso em: 09 de set. 2023.

GOOGLE. **DADOS E SEGURANÇA: SEGURANÇA É UM ASSUNTO SÉRIO NOS NOSSOS DATA CENTERS. MANTEMOS SEUS DADOS PROTEGIDOS E SEGUROS COM O USO DE DIVERSOS RECURSOS DE SEGURANÇA**. Disponível em:

<”https://www.google.com/intl/pt-BR/about/datacenters/data-security/”>. Acesso em: 11 de out. 2023.

GOVBR. “**QUEM VAI REGULAR A LGPD?**”. Disponível em: <”https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd”>. Acesso em: 17 out. 2023.

IANE, Julia et al. (Ed.). **PRIVACY, BIG DATA AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT.** Nova York: Cambridge University Press, 2014.

INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. **BIG DATA NO SUL GLOBAL: RELATÓRIO SOBRE ESTUDOS DE CASO.** Rio de Janeiro: ITS, 2016, p. 9. Disponível em: <”https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf”>. Acesso em: 30 set. 2023.

KIRA, B; Tambelll, C. N. **DATA PROTECTION IN BRAZIL: CRITICAL ANALYSIS OF THE BRAZILIAN LEGISLATION.** Internetlab, 2016. Disponível Em: <”https://internetlab.org.br/WpContent/Uploads/2017/03/Legal-Framework-Analysis-Brazil.Pdf”>. Acesso em: 5 maio. 2023.

KUNSTSPEKTRUM. **RICHARD SERRA "TELEVISION DELIVERS PEOPLE" (1973)**. Youtube, 2 de fev. 2011. Disponível em: <”https://www.youtube.com/watch?v=LvZYwaQlJsg&ab_channel=KunstSpektrum”>.

LANEY, Doug. **3D DATA MANAGEMENT: CONTROLLING DATA VOLUME, VELOCITY AND VARIETY.** Disponível em: <”https://studylib.net/doc/8647594/3d-data-management--controlling-data-volume--velocity--an…”>. Acesso em: 10 de set. 2023.

MACHLUP, Fritz. **THE PRODUCTION AND DISTRIBUTION OF KNOWLEDGE IN THE UNITED STATES**. Nova Jersey: Princeton University Press, 1962; DIJK, Jan van. The network society. 3. rd. Londres: Sage Publications, 2012;

MAGRANI, Eduardo. **A INTERNET DAS COISAS.** — Rio de Janeiro: FGV Editora, 2018.

MAYER-SCHANBERGER, Viktor; PADOVA, Yann. Cukier; Kenneh. **BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK AND THINK**. New York: Houghton Mffin Hartcourt, 2013.

MAYER-SCHANBERGER, Viktor; PADOVA**, YANN. REGIME CHANGE? ENABLING BIG DATA THROUGH EUROPE'S NEW DATA PROTECTION REGULATION.** The Columbia Science & Technology Law Review, Columbia, Nova York, v. XVII, p. 315-335, Primavera 2016. disponível em: <"https://researchgate.net/publication/303665079">. Acesso em: 23 mai. de 2023.

MENEZES NETO, Elias Jacob De; Bolzan De Morais, José Luis. **A FRAGILIZAÇÃO DO ESTADO-NAÇÃO NA PROTEÇÃO DOS DIREITOS HUMANOS VIOLADOS PELAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO.** Revista Direitos Fundamentais & Democracia, [S. L.], V. 23, N. 3, P. 187-188, 2018. Disponível em: <"https://revistaeletronicardfd.unibrasil.com.br/Index.Php/Rdfd/Article/View/1135">. Acesso em: 25 ago. 2023.

MINAS GERAIS. Tribunal de Justiça de Minas Gerais (11ª Câmara Cível). **Apelação Cível 1.0000.19.061299-4/001/MG**. Ementa: APELAÇÃO CÍVEL - AÇÃO DE INDENIZAÇÃO - VIOLAÇÃO DE SIGILO DE DADOS POR ATAQUE CIBERNÉTICO - DANO MORAL CONFIGURADO - REDUZIR VALOR DA INDENIZAÇÃO. - As consequências que decorreram da invasão dos dados cadastrais da autora por terceiros desautorizados, causaram abalos moral, passíveis de reparação. - Em acordo com as peculiaridades do caso, entendo que o valor da indenização fixada pelo juiz sentenciante deve ser reduzido, O que proporciona a reparação pecuniária do dano à ofendida e o efeito pedagógico ao ofensor, evitando-se a reiteração de condutas dessa natureza, sem que haja enriquecimento ilícito sem causa. Relatora: Des.(a) Shirley Fenzi Bertão. Apelante: NS2.COM INTERNET S.A. - NETSHOES. Apelado: NELY REZENDE MILITAO DE ASSIS HORTA. DDJE: 14/08/2019. Data de publicação: 1 9/08/2019. Disponível em: <"https://www5.tjmg.jus.br/jurisprudencia/pesquisaPalavrasEspelhoAcordao.do?&numeroRegistro=1&totalLinhas=1&paginaNumero=1&linhasPorPagina=1&palavras=viola%E7%E3o%20sigilo%20dados%20ataque%20cibern%E9tico&pesquisarPor=ementa&orderByData=2&referenciaLegislativa=Clique%20na%20lupa%20para%20pesquisar%20as%20refer%EAncias%20cadastradas...&pesquisaPalavras=Pesquisar&">. Acesso em: 30 de out. 2023.

MONTEIRO, Renato Leite. D**A PROTEÇÃO AOS REGISTROS, AOS DADOS PESSOAIS E ÀS COMUNICAÇÕES PRIVADAS**. In: DEL MASSO, Fabiano Dolenc;

ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (coord.). Marco Civil da Internet: Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. E-book.

MORAES, Alexandre de. **DIREITO CONSTITUCIONAL** - 13. ed. - São Paulo: Atlas, 2003. p. 53.

MORAIS, Izabelly Soares de… [et al]. **INTRODUÇÃO A BIG DATA E INTERNET DAS COISAS (IOT).** – Porto Alegre: SAGAH, 2018.

MULHOLLAND, Caitlin. **A TUTELA DA PRIVACIDADE NA INTERNET DAS COISAS (IOT).** Belo Horizonte: Casa do Direito; FGV – Fundação Getúlio Vargas, 2019 p. 482-490. Disponível em: <"https://igarape.org.br/wp-content/uploads/2019/06/Horizonte-presente-tecnologia-e-sociedade-em-debate.pdf">. Acesso em: 23 set. 2023.

MULVENNA, Maurice; NORWOOD, Marian; BUCHNER, Alex. **DATA-DRIVEN MARKETING.** Electronic Markets.UK, v. 8:3, p. 32-35. 30 mar. 2006. Disponível em: <https://www.tandfonline.com/doi/epdf/10.1080/10196789800000038?needAccess=true>. Acesso em: 11 de out. 2023.

NASCIMENTO, Anderson. **O QUE É MEGABYTE?** Canaltech, 01 de ago. 2014. Disponível em: <"https://canaltech.com.br/produtos/O-que-e-megabyte/">. Acesso em: 10 de set. 2023.

O CÍRCULO (The Circle, no original). Filme. Direção: James Ponsoldt. Produção: Anthony Bregman. Intérpretes: Emma Watson, Tom Hanks, John Boyega e outros. Estados Unidos: STXFilms and EuropaCorp, 2017.

OLIVEIRA, Marcos de. **(IOT): 41,76 BILHÕES DE DISPOSITIVOS ATIVOS CONECTADOS GLOBALMENTE EM 2023**. Monitor Mercantil, maio. 2023. Disponível em: <"https://monitormercantil.com.br/iot-4176-bilhoes-de-dispositivos-ativos-conectados-globalmente-em-2023/>". Acesso em: 23 de set. 2023.

ORWELL, George. **1984**. São Paulo: Companhia Das Letras, 2009.

PESSOA, João Pedro Seefeldt. **O EFEITO ORWELL NA SOCIEDADE EM REDE: CIBERSEGURANÇA, REGIME GLOBAL DE VIGILÂNCIA SOCIAL E DIREITO À PRIVACIDADE NO SÉCULO XXI**. Porto Alegre, RS: Editora Fi, 2020.

QUEIROZ, Eliani de Fátima Covem Queiroz. **CIBERATIVISMO: A NOVA FERRAMENTA DOS MOVIMENTOS SOCIAIS.** Revista Panorama, Goiânia, v. 7, n. 1, p. 2-5, jan./jun. 2017. Disponível em: <"https://seer.pucgoias.edu.br/index.php/panorama/article/view/5574/3064">. Acesso em: 03 de out. 2023.

REIS, E. V. B. Naves, B. T. O. **O MEIO AMBIENTE DIGITAL E O DIREITO À PRIVACIDADE DIANTE DO BIG DATA**. Veredas Do Direito, Belo Horizonte, V. 17, N. 37, P. 145/167, Abr. 2020. Disponível em: <"https://revista.domhelder.edu.br/index.php/veredas/article/view/1795">. Acesso em: 10 abril. 2023.

RODOTÀ, Stefano. **A VIDA NA SOCIEDADE DA VIGILÂNCIA: A PRIVACIDADE HOJE**. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 92

ROSENBERG, Mattew. **Cambridge Analytica and Facebook: The Scandal and the Fallout So Far**. The New York Times, USA. 2018. Disponível em: <"https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html">. Acesso em: 10 de out. 2023.

SILVERBERG, David. **HOW COVID TURBOCHARGED THE QR REVOLUTIO**n, Jan 2021. Disponível em: <"https://bbc.com/News/Business-55579480">. Acesso em: 25 set. 2023.

SOUSA, Thaís. **Ministério Público instaura inquérito sobre vazamento de dados de menina de 10 anos vítima de estupro.** O Globo. 06 de nov. 2023. Disponível em: <"https://oglobo.globo.com/brasil/ministerio-publico-instaura-inquerito-sobre-vazamento-de-dados-de-menina-de-10-anos-vitima-de-estupro-24590864">. Acesso em: 10 de out. 2023.

TAURION, Cesar. **CLOUD COMPUTING: COMPUTAÇÃO EM NUVEM TRANSFORMANDO O MUNDO DA TECNOLOGIA DA INFORMAÇÃO**. Rio de Janeiro: Brasport, 2009

THIRANI, Vasudha; Gupta, Arvind. **THE VALUE OF DATA. WORLD ECONOMIC FORUM**, Set. 2017. Disponível em: <"https://weforum.org/Agenda/2017/09/The-Value-Ofdata">. Acesso em: 2 ago. 2023.

TOLEDO, Giuliana de. **FACEAPP ROUBA DADOS? JOGO VOLTA À MODA TROCANDO GÊNERO EM FOTOS E REACENDE DEBATE:** Entenda as críticas ao app que virou febre de novo na quarentena dos brasileiros: Procon-SP estuda notificar pela segunda vez Google e Apple, que oferecem o programa. O Globo. 17 de jun. 2020. Disponível em: <"https://oglobo.globo.com/cultura/faceapp-rouba-dados-jogo-volta-moda-trocando-genero-em-fotos-reacende-debate-24485207"> Acesso em: 04 de out. 2023.

TORRES JUNIOR, Paulo Fernandes Moreira. **O DIREITO À PRIVACIDADE E À INTIMIDADE NA INTERNET.** Repositório Institucional Tiradentes, Jul. 2016. Disponível em: <"https://openritgrupotiradentes.com/Xmlui/Handle/Set/1172">. Acesso em: 5 Maio 2023.

VAINZOF, Rony; MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **COMENTÁRIOS AO GDPR: Regulamento Geral de Proteção de Dados da União Europeia.** 3ª ed. São Paulo: Thomson Reuters Brasil, 2021. P. 37-85.

VALENTE, Jonas. ***Internautas brasileiros acham que a internet se resume ao Facebook:*** *Pesquisa revela que 55% dos brasileiros não percebem vida online fora da plataforma criada por Mark Zuckerberg*, jan. 2017. Disponível em: <"https://www.cartacapital.com.br/blogs/intervozes/internautas-brasileiros-acham-que-a-internet-se-resume-ao-facebook/">. Acesso em: 25 set. 2023.

VALENTE, Luiz Guilherme Veiga. direito, **ARTE E INDÚSTRIA: O PROBLEMA DA DIVISÃO DA PROPRIEDADE INTELECTUAL NA ECONOMIA CRIATIVA.** 2019. Tese (Doutorado) – Universidade De São Paulo, São Paulo, 2019. Disponível Em: <"https://teses.usp.br/Teses/Disponiveis/2/2132/Tde-08092020-004314/Pt-Br.Php">. Acesso em: 2 maio. 2023.

VENTURINI, J.; LOUZADA, L.; MACIEL, M.; ZINGALES, N.; STYLIANOU, K.; BELLI, L. **TERMOS DE USO E DIREITOS HUMANOS: UMA ANÁLISE DOS CONTRATOS DAS PLATAFORMAS ONLINE.** No prelo. [S.l.: s.n.], 2016.

WALKER, K. **WHERE EVERYBODY KNOWS YOUR NAME: A PRAGMATIC LOOK AT THE COSTS OF PRIVACY AND THE BENEFITS OF INFORMATION EXCHANGE**. Stanford Technology Law Review. 2001.

WARREN, Samuel; BRANDEIS Louis. **THE RIGHT TO PRIVACY**, Harvard Law Review, v. 4, n. 5, p. 193-220, dez. 1890.

WERTHEIN, J.. **A SOCIEDADE DA INFORMAÇÃO E SEUS DESAFIOS**. Ciência Da Informação, V. 29, N. 2, P. 71–77, Maio 2000.

ZUBOFF, Shoshana. **A ERA DO CAPITALISMO DE VIGILÂNCIA: A LUTA POR UM FUTURO HUMANO NA NOVA FRONTEIRA DO PODER.** Rio De Janeiro: Intrínseca, 2020.

ZUBOFF, Shoshana**. BIG OTHER: SURVEILLANCE CAPITALISM AND THE PROSPECTS OF AN INFORMATION CIVILIZATION.** Journal of Information Technology, 04 abr. 2015, p. 77. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754>. Acesso em: 10 out. 2023.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, **MELYSSA SANTOS**, discente regularmente matriculado(a) na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº **31909493**, período **NOTURNO**, turma **R**, tendo realizado o TCC com o título: "***ANÁLISE DA CIBERSEGURANÇA DE USUÁRIOS DA INTERNET NO BRASIL:*** *Um desafio na era do big data e dataveillance versus a privacidade e proteção de dados dos usuários sob a ótica da Lei n° 13.709/18*", sob a orientação da Professora **RUTH CAROLINA RODRIGUES SGRIGNOLLI,** declaro, para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 06 de novembro de 2023.

melyssa Santos

Assinatura do discente