CENTRO UNIVERSITÁRIO BRASILEIRO CURSO DE BACHARELADO EM DIREITO

MATHEUS SANTOS TORRES HOMEM

LEI GERAL DE PROTEÇÃO DE DADOS: aplicabilidade de efetividade em meio ao âmbito empresarial

RECIFE/2022

MATHEUS SANTOS TORRES HOMEM

LEI GERAL DE PROTEÇÃO DE DADOS: aplicabilidade de efetividade em meio ao âmbito empresarial

Monografia apresentada ao Centro Universitário Brasileiro - UNIBRA, como requisito parcial para a disciplina de Orientação Monográfica 2
Professor/a orientador/a: Candida Bonfim

RECIFE/2022

Ficha catalográfica elaborada pela
bibliotecária: Laís Cardoso, CRB-4/PE-1753/P.

H765l Homem, Matheus Santos Torres.
Lei geral de proteção de dados: aplicabilidade de efetividade em meio ao âmbito empresarial / Matheus Santos Torres Homem. - Recife: Edição do autor, 2022.
40 p. : il. color.

Orientador(a): Me. João Roberto da Conceição.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – Unibra. Bacharelado em Direito, 2022.
Inclui Bibliografia.

1. Lei. 13709/2018. 2. LGPD. 3. Proteção. 4. Dados. I. Centro Universitário Brasileiro - Unibra. II. Título.

CDU: 34

Dedico esse trabalho a minha mãe, que lutou muito pelas minhas conquistas

RESUMO

Na sociedade da informação, os direitos de proteção de dados pessoais estão em sérios riscos. Embora tenha influência direta na privacidade e na vida privada, este direito opera sob um mecanismo diferente dos demais. Deve ser analisado, para o seu melhor enquadramento, como direito da personalidade uma vez que está presenteem todos os âmbitos da sociedade e tem impacto em vários aspetos que regem a vidade milhões de indivíduos. As ferramentas de coleta e processamento de dados são de interesse de muitas empresas e organizações que desejam aproveitá-las ao máximo para atingir seus objetivos. O desenvolvimento tecnológico é motivo de preocupação devido à imprevisibilidade das consequências de uso sem limites desses dados, sendo o principal propulsor de mudanças sobre o tema no campo jurídico. Este trabalho tem por objetivo analisar a natureza jurídica e os limites da responsabilidade civil dos agentes de proteção de dados no Brasil, com base na lei Geral de Proteção de Dados (lei nº 13.709/18). Para tal, com base na exploração da legislação em vigorem meio a um raciocínio dedutivo e analises bibliográficas e documentais, além da opinião de alguns juristas, esta monografia vem a tratar de: no primeiro capítulo, a evolução da fundamentação que levou a formação dos conceitos de privacidade e personalidade no digital; logo após, no segundo capítulo, demonstrar os dados como forma de comercio; e, no ultimo capitulo, demonstrara responsabilidade pela titularidade de natureza jurídica e civil dos agentes de dados e seus tratamentos subjetivos, bem como a possibilidade e a devida oportunidade efetuar uma devida ação de ressarcimento indenizatório, por prejuízos causados pela má gestão de dados pelos detentores deles.

Palavras-chave: Lei. 13709/2018. LGPD. Proteção. Dados.

ABSTRACT

In the information society, personal data protection rights are at serious risk. Although it has a direct influence on privacy and private life, this right operates under a mechanism different from the others, which must be analyzed for its best framing as a personality right since it is present in all areas of society and has an impact on several aspects that govern the lives of millions of individuals. Data collection and processing tools are of interest to many companies and organizations that want to make the most of them to achieve their goals. Technological development is a matter of concern due to the unpredictability of the consequences of unlimited use of these data, being the main driver of changes on the subject in the legal field. This work aims to analyze the legal nature and limits of civil liability of data protection agents in Brazil, based on the General Data Protection Law (law nº 13.709/18). To this end, based on the exploration of the legislation in force, bibliographical and documental analysis, in addition to the opinion of some jurists to base the concepts that led to this monograph comes to deal with; in the first chapter, the evolution of the reasoning that led to the formation of the concepts of privacy and personality in the digital world, soon after demonstrating data as a form of commerce, and in the last chapter to demonstrate the responsibility for the legal and civil ownership of data agents and their subjective treatments, as well as demonstrating the possibility and due opportunity to carry out a due action for indemnity reimbursement, for damages caused by poor data management by their holders.

Keywords: Law. 13709/2018. LGPD. Protection. data.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) é uma lei brasileira que define o que pode ser feito com os dados dos cidadãos e também prevê penalidades para o descumprimento dessas decisões, e não se trata de um assunto recente, mas veio ganhando uma maior atenção na última década, quando o tema foi lançado para consulta pública pelo Ministério da Justiça, por meio de uma plataforma *online*. Ao longo desses anos, foram vários os fatores políticos e também econômicos que impulsionaram a criação de três principais projetos de lei.

A LGPD impõe normas que modificaram as relações entre grandes corporações como Twitter, Amazon e os usuários desses serviços, ou seja, os consumidores desses produtos, já que em comparação são os mais vulneráveis a abusos por parte de megacorporações.

Os direitos fundamentais eram, basicamente, liberdade, igualdade e fraternidade, e nem se cogitaria pensar na possibilidade de uma revolução de novos tipos defundamentos que hoje se tornaram pilar a sociedade, como a defesa as etnias, aos sexos, meio ambiente, e ambiente digital.

Em suma, a problemática ficou visível visto que as empresas brasileiras e estrangeiras que venham a coletar e processar dados no Brasil devem se adequar à Lei Geral de Proteção de Dados. Diante desse cenário, é um grande repto para as empresas não apenas se comprometerem a investir em tecnologias que auxiliem o processo de segurança da informação, mas também mudar sua cultura e o paradigma de coleta de dados não essenciais para o negócio. Para os dados essenciais que serão recolhidos pelas empresas, como os dados essenciais para a emissão de um documento de comprovação, a lei exige que estes sejam protegidos contra intrusões e que não sejam aplicados a uma finalidade diferente daquela para o qual foram coletados (SERPRO, 2019). As medidas que todas as empresas e órgãos públicos devem adotar vão desde a garantia da segurança dos dados até a pseudonimização ou anonimização dos dados para ajudar a reduzir o risco aos usuários, entre outras que serão discutidas ao longo deste artigo.

Um ponto crucial a ser observado é que os dados privados dos usuários são de forma indiscriminada coletados e utilizados por todo tipo de empresa, portanto essa a Lei Geral de Proteção de dados (LGPD), terá um grande impacto em todos os tipos de negócio e em toda a sociedade. Assim, pode-se afirmar que o conhecimento da lei é

necessário para as empresas evitarem sanções administrativas, judiciais e multas. Também é de suma importância para o cidadão comum conhecer seus novos direitos e todas as regras sobre como as empresas terão que comportar-se no que diz respeito à coleta e tratamento dos seus dados pessoais.

O presente trabalho tem como objetivo apresentar, de forma simples e de fácil compreensão para o cidadão comum, uma análise da Lei Geral de Proteção de Dados, seus aspectos e implicações para as empresas instituições públicas e sociedade em geral. Visa discutir também a importância dos dados e a transformação da economia na era digital e sua consequente dependência de bancos de dados. Para a elaboração desta monografia, foi utilizada a metodologia de raciocínio dedutivo com uma exploração Documental e bibliográfica para trazer luz aos fatos. O método documental é muito útil para a análise do direito, tema principal deste trabalho.

2 FUNDAMENTOS DA PRIVACIDADE

2.1 PROTEÇÃO DE DADOS

Em uma constante evolução tecnológica da humanidade, novos desafios foram sendo criados em decorrência das inovações da época. Novos desafios a privacidade de dados também foram sendo colocados à prova e, por um período de tempo, as regras que asseguravam a segurança dos dados se tornavam inadequadas mediante os meios de evolução tecnológicas, outrora sem regras ou revisão adequada.

Em meio a isto, o direito à privacidade se viu consagrado como direito fundamental segundo o artigo 5º, incisos X, XI e XII da Constituição Federal (BRASIL,1988). Porém, para entender como nasceu a segurança de dados é preciso analisar como ocorreu sua evolução à medida foram surgindo problemas advindos dos avanços tecnológicos.

Desde já, no que se refere ao tema proposto neste tópico, cabe observar que a legislação brasileira não adotou os termos “privacidade”, mas sim “vida privada” e “intimidade”, sem concebê-los de forma específica. Não obstante, o debate termológico se mostra infrutífero para os intentos do estudo proposto neste trabalho, possibilitando o uso da palavra “privacidade” para abordar as questões levantadas quanto à proteção do direito à privacidade.

Elegemos o significado primário da palavra “privacidade” para nos concernir à intimidade. O conceito de privacidade está ligado às transformações ocorridas ao longo da história e à relação entre as pessoas e os espaços que habitam. É possível observar, portanto, que o exercício desse direito está vinculado a uma estrutura que o possibilita, pois se relaciona, mesmo que indiretamente, com o espaço onde vive e edifica sua existência.

Dito isto, com o crescimento dos progressos tecnológicos, as pessoas como forma de entretenimento em redes sociais, começaram a divulgar fatos da vida pessoal e “fofocas” de forma empolgante e as vezes até imediata comparada a meios convencionais. Portanto, foi preciso ver a necessidade de direitos extensos em se tratando da privacidade individual e coletiva, em meio a ideia de um direito privado.

Em 1890 foi publicado um artigo na *Harvard Law Review*, redigido por dois colegas, Samuel Warren e Louis Brandeis, chamado “*The right to privacy*”, bastante representativo, sendo destaque como um dos precursores do direito à privacidade,

percebendo que esse direito das pessoas deveria ser o direito de “deixar em paz” (CANCELIER, 2017, p. 9).

Warren e Brandeis (1890) levantam a ideia de existir algum limite para que seja garantida de forma legal a segurança ao tentar exprimir alguma informação a outrem. O direito à privacidade era cabido apenas como uma prerrogativa de respeitar a individualidade ou o Espaço do indivíduo, longe da curiosidade dos outros. Na verdade, o direito à privacidade é cabido como uma necessidade de solidão, de se permitir que uma pessoa se retire para um espaço privado sem ser perturbado.

Quando se trata do conceito de privacidade, contudo, o ímpeto dado por esses dois advogados, Warren e Brandeis, sugere que esse direito em formação deve ser protegido e tutelado de forma independente. Inspirado na publicação não autorizada em jornais de alguns fatos íntimos sobre o casamento da filha de Thomas McIntyre Cooley elaborando assim em 1888 “o direito de estar só”. Com a relação dos fatos acima, tornou-se obvia a necessidade de proteção reforçada para proteger os direitos aos dados pessoais.

Em 1948, com a declaração Universal dos direitos humanos, o direito àprivacidade foi consagrado como um direito fundamental do ser humano, conforme mencionado no art.12, e válido até hoje: “Art.12: Ninguém sofrerá intromissões arbitrários ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência” (UE, 1948).

Desde então, o pensamento de privacidade foi alterado diversas vezes. No passado, incluía apenas a inviolabilidade do domicílio e o sigilo das comunicações. A definição sofreu uma mudança profunda, abordando outros aspectos em uma perspectiva mais ampla.

A privacidade ajuda a limitar quem pode acessar dados ou informações, por exemplo, sobre sua localização por meio de gps em dispositivos, itens de preferência e comunicações, até o estado corporal e suas funções monitorados através de aplicativos.

As leis de proteção de dados pessoais compartilham características comuns, como independência e clareza. Em 1970, a Alemanha aprovou a primeira lei de proteção de dados pessoais do mundo. Mendes (2011) apontou a necessidade de aumentar onível de proteção de dados pessoais, defendendo que a proteção de dados pessoais, pois trata-se de uma projeção da individualidade do indivíduo cabendo assim receber o devido respaldo jurídico.

Foi em 1980 que a organização para Cooperação e Desenvolvimento

Econômico(OCDE) criou um comité de ministros da OCDE e publicou diretrizes que estabelecem os princípios básicos sobre proteção de dados e o fluxo de informações entre países, que possuem leis próprias, de acordo com os princípios estabelecidos nas diretrizes, No entanto, essas diretrizes ainda não se aplicam à implementação do padrão que muitas vezes é interpretado de forma ampla.

Isso acabou levando a várias disposições legais em muitos países. Cada país tem sua própria interpretação de proteção de dados (OCDE, 2002). Em 1981, a delegação Europeia ratificou e proibiu o processamento de dados confidenciais sobre raça, política, saúde, religião, vida sexual, ficha criminal e outras informações de um indivíduo. Também estabeleceu o direito dos indivíduos de saber quais informações são mantidas sobre eles e de corrigi-las, se necessário (OCDE, 1981).

Uma decisão mais relevante veio em 1983, com o Tribunal Constitucional alemão que reconheceu o direito à autodeterminação da informação e declarou que a lei censitária era inconstitucional ao obrigar os cidadãos a fornecer dados, aplicando-lhes mesmo multas e permitindo até que fossem compartilhados entre os órgãos públicos federais. Segundo Mendes (2008):

> A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subsequentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados. Dessa forma, o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais se baseia em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação (MENDES, 2008).

No Brasil, em meados da década de 1990, começaram a emergir instrumentos legais sobre a proteção do uso de dados, criando assim novas percepções sobre a real importância desses dados. Como exemplo, cita-se o Código de Defesa do Consumidor, que regulamenta o uso de bancos de dados de consumidores.

A legislação consumerista, Lei nº 8.078/90, prevê regras de acesso às "informações contidas em arquivos, cadastros, registros de dados pessoais e de consumo, arquivados a seu respeito", porém, permite a retificação em caso de ambiguidade e, embora não tenha previsto tal consentimento para a coleta desses dados, defendeu-se que o consumidor seja informado da abertura do cadastro.

Em 1996, a lei de interceptação de telefônica, Lei nº 9.296/96, caracterizou o

direito à privacidade ao limitar o uso desse recurso tornando as possibilidades de uso sempre sob a proteção de ordem judicial. Em 1997, foi promulgada a lei de *Habeas Data*, Lei nº 9.507/97, que regulamentou o direito constitucional e o rito deacesso e correção de informações pessoais.

Na Europa, após sancionada a diretiva nº 46, A diretiva à proteção de dados pessoais foi um dos mais difundidos no mundo até a *promulgação do General data protection regulation* (GDPR). A diretiva, embora não tenha força de lei perante os países membros, serviu de baliza para 13 legislações nacionais, bem como a manutenção de seus princípios mais relevantes no GDPR.

Uma vez que os princípios de proteção devem ser aplicados a qualquer processamento de dados pessoais, as atividades do controlador serão regidas pelo direito comunitário. Outra ponto a ser considerado diz respeito ao princípio de que devem ser excluídos os tratamentos de dados efetuados por pessoas singulares apenas no âmbito de atividades pessoais ou domésticas, tais como correspondência ou endereços pessoais (UNIÃO EUROPEIA, 1995); pontos sobre direitos de privacidade,que diz respeito à privacidade e ao fornecimento de ferramentas para controlar as violações desse direito.

O destaque dessa adição é a ênfase lenta, mas enfática, na privacidade comoum direito subjetivo, não um direito de propriedade, tendo uma adição importantecomo a lei de acesso à informação concebida em 2011, Lei nº 12.527/11, tendo como o seu art. 4, em seu inciso IV e art.6, em seu inciso lll, reforça que se considera informação pessoal: “Art. 4º Para os efeitos desta Lei, considera-se: IV - Informaçãopessoal: aquela relacionada à pessoa natural identificada ou identificável”. (BRASIL, 2011). Ademais devemos reforçar também o que foi dito no Art. 6:

> Art. 6º Cabe aos órgãos e entidades do poder público, observadas asnormas e procedimentos específicos aplicáveis, assegurar a: III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. (BRASIL, 2011)

Deixando expresso que é uma forma assentir a conexão de responsabilidade dos órgãos públicos, onde diz expressamente no art. 6, que cabe aos órgãos públicos seguindo os requisitos da lei, garantir a proteção de informação sigilosa ou de informações pessoais.

Os demais elementos destacam alguns princípios fundamentais, como a

liberdade e as garantias individuais, também consagrados na lei Geral de Proteçãode Dados, como os princípios da transparência, privacidade, honra, respeito à privacidade e à imagem da pessoa humana. Merece destaque, ainda, a Lei Carolina Dieckman, lei nº 12.737/12, que foi destaque em 2012 após o caso de vazamento de imagens intimas da atriz. A lei reconheceu como crime, delitos exercidos com uso de dispositivos eletrônicos estando disposto em seu Art. 154-A, § 3º.

No primeiro período de 2013, alguns itens foram regulamentados na lei do consumidor que estabeleceu medidas efetivas de segurança para que o fornecedor garantisse a segurança no pagamento e tratamento dos dados do consumidor. Devido a uma tão forte dinamização da velocidade relacionada com a renovação dalegislação de proteção de dados, em vários países do mundo tem-se verificado a necessidade de proteger os dados pessoais em uma velocidade cada vez mais alarmante em meio a novos avanços tecnológicos e novas espécies de serviços digitais.

O analista da agência de Segurança Nacional (NSA), Edward Snowden, veio à tona revelando o uso de um *software* chamado "PRISM" que é usado para monitorar e rastrear, de forma global, todas as informações trazidas na rede de 14 computadores. O programa coletava informações em massa, monitorava não apenas os terroristas, mas todas as transmissões feitas por indivíduos na internet e também era uma forma de espionar países e empresas influentes. Entre as inúmerasvítimas, pode-se citar a então presidente do Brasil, Dilma Rousseff, cuja conta foi monitorada. Com isso, mostrou-se ao mundo inteiro o quão vulnerável é a privacidadena rede de computadores.

No final de 2013, após a presidente e seus assessores serem espionados pela agência de espionagem dos Estados Unidos, o governo brasileiro, após a conclusão da CPI da espionagem, solicitou a implementação do projeto de Lei nº 2.126/11, conhecido como Marco civil da internet que foi votado e sancionado em caráter de urgência, promulgado em 2014. Neste dispositivo legal a palavra "privacidade" é mencionada pela primeira vez, destacando a necessidade de proteção de dados, consagrando-a ou como um direito humano fundamental.

Não se deve esquecer que os incisos VII, VIII, X do art 7 e art. 3 do Marco civil, alegislação de proteção de dados prevê uma série de outros princípios e outras regras, que posteriormente serão aplicados também na LGPD.

Em 2016, muitas disputas surgiram na associação Europeia, que resultaram na criação da proteção de dados pessoais da Europa, Lei nº 679/16, mantendo relações

comerciais com a associação Europeia, criar a legislação no mesmo âmbito que a *General data protection regulation* (UE, 2016).

A lei estabelece uma série de pré-condições para o controle técnico e gestão da segurança da informação. O objetivo da União Europeia ao aprova-la era: (I) Contribuir para um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem estar das pessoas físicas; (II) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União, e evitar que as divergências sejam um obstáculo à livre circulação de dados pessoais no mercado interno; (III) garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo; (IV) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais; (V) possibilitar uma cooperação efetiva entre as autoridades de controle dosdiferentes Estados-Membros.

A criação de leis de proteção de dados pessoais elaborada em processos situacionais de época, para alguns juristas consistem em normas que refletem o estado da tecnologia e a visão dos juristas da época. Para outros, têm como propositura um centro de mudança no sistema regulatório. Para os juristas mais modernos voltou-se à procura de melhorar a proteção de dados pessoais, buscando sanar os vícios que prejudiquem os indivíduos, demonstrando a necessidade estatal para o resguardo efetivo dos dados com segurança, eregulando as possibilidades que danifiquem o direito individual ou coletivo.

2.2 PROTEÇÃO DE DADOS E DIREITO A PERSONALIDADE

Há implacabilidade na formação e no estabelecimento permanente de todos os direitos fundamentais do indivíduo na proteção qualitativa que o sujeito do Estado deve prestar no cumprimento de suas obrigações (OLIVEIRA JUNIOR, 2013).

Isto significa que num Estado Democrático de Direito, com obrigações mais ou menos razoáveis, será possível ampla defesa da pessoa através do reconhecimento da sua personalidade, que deve ser eficaz também no domínio da proteção de dados. Desse ponto de vista, esta necessidade de proteção real é, portanto, importante. A existência de uma entidade estatal é valorizada pela manifestação de todos aqueles

mecanismos de coerção social que a determinam.

É impossível em um país democrático agir de outra forma, pois a imposição de deveres tem um valor protegido quase equivalente. É uma indicação clara de que algo não se baseia na preservação qualitativa do interesse coletivo.

Tudo isso, claro, pode e deve aplicar os 16 dispositivos de proteção de dados pessoais previstos na Lei Geral de Proteção de Dados pessoais (LGPD), incluindo as esferas públicas que tratam de informações privadas de alto valor.

Tanto no campo doutrinário quanto no jurídico, associam-se as criações de ser humano e de personalidade. Essa similitude fica exatamente mais clara quando se trata de assuntos privados,portanto da órbita do direito civil, pois é por meio do instituto da personalidade jurídica que a pessoa passa a se configurar como sujeito de direitos e deveres no entanto, a permanência adotada de uma personalidade não importa no usufruto prévio de um direito delimitado.

Em se falando de direitos da personalidade, ter acesso ao exercício de direitos revela um demanda por uma visão panorâmica de deveres sociais em consonância com a legislação, Como seria de se esperar das instituições da administração pública baseadas no conhecimento da LGPD.

Sendo assim a personalidade jurídica é uma característica que decorre da divisão de direitos e deveres imposta pelo ordenamento jurídico.

No campo jurídico, pode-se notar que a personalidade jurídica do indivíduo pode ser utilizada sem qualquer requisito, expressando apenas o caso de ser um pessoa física ou jurídica, tem o direito de gozar de uma série de direitos razoáveis, tendo como dever respeitar essas obrigações impostas pelo bem coletivo. Atualmente a LGPD se dedica à proteção de informações e dados disponíveis em bases de dados como a base de direitos dapersonalidade.

2.3 A CARACTERIZAÇÃO DA DIGNIDADE DA PESSOA HUMANA NO DIGITAL

Importa dizer que precisa que a personalidade em causa neste estudo é aquela cuja proteção é canalizada para o desenvolvimento da pessoa humana, pelo que não se trata da (in)aptidão de um sujeito para ser o titular de direitos e obrigações.

Com o devido reconhecimento da dignidade da pessoa humana segundo constante no art.1º, inciso III,(BRASIL, 1988), tornou-se um verdadeiro marco normativo para a proteção dos direitos da personalidade e também trouxe outras

garantias, como a liberdade de expressão no art 5º, inciso IX e o direito à informação no art. 5º, XV.

No código civil, podemos observar que a dignidade da pessoa humana se tornoucentral para a proteção legal, especialmente no contexto do capítulo sobre direitos de privacidade. O sujeito, antes lidado como neutro, passou a ser entendido como uma pessoa sobre a qual se voltam as atenções do ordenamento jurídico como um todo.

Entre o exemplo mais comum encontra-se no art. 11, do Código Civil, que diz: "Art 11. com exceção dos casos previstos lei, os direitos dapersonalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária."

No entanto, os direitos da personalidade não se limitam à situação mencionada na hipótese do código civil acima citado e não podem ser considerados limitantes,mas sim amplos, o que permite o reconhecimento do direito à proteção de dados como um novo direito da personalidade (BIONI 2020, p. 50).

Na era da informação O fenômeno da manipulação da informação apresenta umanova situação desafiadora para a proteção da personalidade humana, a maioria daspessoas acredita que a sociedade e a economia são regidas pelas atividades de controle e armazenamento de dados pessoais, O efeito da economia da informação para mapear e categorizar os perfis dos detentores de dados.

Portanto, as informações pessoais são concebidas como extensão da personalidade e elementos essenciais da singularidade de cada indivíduo, capazes de identificá-los em suas particularidades como indivíduos sociais. Daí a importância de elevar o nível de proteção de dados pessoais ao patamar de direito humano.

Em todas as normativas estrangeiras, esse mesmo debate vem florescendo, sobretudo na Carta Europeia de Direitos Fundamentais, que inscreveu a proteção de dados como um direito fundamental e cuja proteção deve se dar por aplicação e interpretação de uma autoridade independente.

Muitos países, ao pensar em acordos internacionais nesse sentido, procuram nãoapenas analisar se determinado país possui uma lei de proteção de dados e se existe uma autoridade nacional relacionada ao assunto, mas principalmente estudar como funciona o sistema judiciário de proteção de dados. Portanto, é uma vantagem mencionar a proteção de dados na constituição como um direito fundamental.

pois tornaria um ambiente mais propicio ao Supremo Tribunal em um debate queprocure abordar a pauta no dia a dia, recorde-se que o mesmo Tribunal judiciário

já reconheceu a importância da questão e definiu a elevação da proteção de dados e do direito à autodeterminação informativa como direito fundamental autónomo em decisão histórica.

com base na decisão do então Tribunal Constitucional Federal da Alemanha Ocidental de 1983 (Volkszählungsurteil), em que a inconstitucionalidade dos dispositivos de uma lei que criou um censo estadual semelhante ao caso brasileiro e estabeleceu a coleta de dados pessoais dos cidadãos para a otimização da ordem pública.

A decisão do Tribunal proferida em 8 de maio de 2020, por votação quase unânime (10 votos a 1), homologou a medida cautelar deferida pela Ministra do STF Rosa Weber no âmbito de cinco ações diretas de inconstitucionalidade, suspendendo assim a eficácia da medida provisória nº954, de 17 de abril de 2020,que compõe a seguinte disposição:

> O compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência pública de importância internacional decorrentedo coronavírus (covid19), de que trata a Lei nº 13.979, de 6de fevereiro de 2020 (BRASIL. 2020).

Aludindo a uma ameaça à própria democracia constitucional, a decisão referendada pelo plenário do STF, pela ministra do STF, Rosa Weber, confirma que não há mais nenhum dado neutro ou indesejável, pois qualquer dado que possa identificar uma pessoa pode ser utilizado para formar perfis que as empresas e o Estado irão utilizar, razão pela qual qualquer dado que permita a identificação de uma pessoa merece proteção constitucional.

A importância de regulamentar a matéria deve abranger a proteção da personalidade o mais amplamente possível, uma vez que a exploração de dados pessoais vai além de um simples sentimento de invasão de privacidade, especialmente se for levada em conta a concepção clássica de privacidade, de “ser deixado sozinho”.

As infrações que podem ocorrer no âmbito da gestão irregular e ilícita dos dados pessoais afetam muitos outros domínios da vida dos cidadãos, expondo o mesmo aoperigo e sua autonomia e individualidade (TEPEDINO; FRAZÃO; OLIVA, 2019).

Conclui-se, assim, que a proteção de dados pessoais está incluída como categoria autónoma dos direitos da personalidade sendo essencial para a lei geral de proteção de dados que todos os responsáveis pelo tratamento e operadores dedados sejam supervisionados para que os titulares dos dados saibam claramentecomo os seus dados serão tratados. A LGPD, ao homogeneizar essas questões, conseguiu estabelecer uma relação de confiança entre os diferentes sujeitos que tratam de Tecnologia da Informação (TI).

3 DESTRINCHANDO A LGPD

3.1 ASPECTOS IMPORTANES DA LGPD

Para melhor entendimento e fluxo no trabalho, devemos destrinchar a LGPD. Sendo assim, no que diz respeito à proteção de dados, a lei nº 13.709/2018, da LGPD, que veio como precursora da legislação europeia *General Data Protection Regulantion* - (GDPR), sendo assim a LGPD surgiu em 25 de maio de 2018, sendo criada para suprir as lacunas existentes etrazer melhorias no tratamento de dados pessoais no ordenamento jurídico brasileiro.

A LGPD é espelhada nos progressos e evoluções dos recursos tecnológicos contemporâneos. Com o surgimento das redes sociais e popularização de compras online, a transmissão de dados pessoais atingiu níveis nunca antes vistos. Assim, para evitar o tratamento injustificado de dados por parte de instituições públicas e Corporações, iniciou-se no Brasil a regulamentação desta matéria.

Releva-se que esta lei prevê que as pessoas singulares ou coletivas de direito público ou privado tratem dados pessoais, incluindo os contidos em suportes digitais, com o objetivo de proteger os direitos básicos e fundamentais de um Estado Democrático de direitos, como, por exemplo, liberdade e privacidade, alcançando assim o livre desenvolvimento das pessoas físicas. O tratamento de dados pessoais pode ser realizado por órgãos ou entidadesdesde que se enquadre em uma das hipóteses previstas na LGPD. Estes pressupostos podem ser entendidos como condições necessários para verificar se otratamento de dados pelo controlador e operador é autorizado. Os casos de tratamento de dados pessoais e de dados pessoais sensíveis estão elencados,respectivamente, no art. 7º em seus incisos II, III,

lV, V e por fim o lX, e no art. 11 em seu inciso ll, da LGPD. Assim, é necessário averiguar,previamente, qual é a hipótese facultativa aplicável ao tratamento de dados pessoaisque o serviço irá efetuar. Além disso, sempre que a administração pública realizaratividade de tratamento de dados pessoais, deverá notificar ao titular os casos de tratamento de dados pessoais aprovados pela LGPD, bem como sua disposição legal. Assim, o fundamento da LGDP está vinculado ao disposto previamente listados e citados, é claro que a lei de proteção e desenvolvimento da população se baseia maisuma vez na proteção e garantia da privacidade liberdade, segurança, justiça e desenvolvimento econômico e social das pessoas, garantindo assim a segurança jurídica da população país.

Em 14 de agosto de 2018, foi sancionado o congresso Nacional do PLC 53/2018, que dispõe sobre a proteção de dados pessoais e modifica o Marco civil da internet consolidando-se assim como a lei Geral de Proteção de Dados do Brasil. Logo em seguida, vindo através da promulgação da lei nº 13.853/2019, o prazo para entrar em vigor da LGPD foi estendido para 24 meses, determinando assim, que a lei entraria em vigor em 16 de agosto de 2020.

No entanto, a LGPD substituir ou complementar esse marco regulatório setorial, por vezes contraditório, que tem gerado insegurança jurídica e tornado o Estado menos competitivo no contexto de uma sociedade cada vez mais conectada distribuidora de dados.

Assim, a LGPD ocasiona verdadeira mudança de paradigma na gestão de dados, destacando a necessidade de erigir uma cultura de proteção de dados no país. A lei, portanto, cria uma nova regulamentação para o uso de dados pessoais no Brasil, tanto online quanto offline, nos setores privado e público, além de colocar o país na lista de mais de 100 países considerados adequados para privacidade e uso de dados. A estrutura da LGPD é composta pelos tópicos a seguir; (1) Pré-requisitos (fins e definições legais); (2) Processamento de dados (quando aplicável, finalidade e rescisão); (3) Direitos dos titulares de dados (questões tributárias do processamento); (4) Processamento de dados por autoridades públicas (Termos específicos da transparência e responsabilidade); (5) Transferências internacionais de dados. (nos casos que houver essa possibilidade); (6) Agentes de processamento de dados (Sujeito ativo do processamento de dados - definições e responsabilidades); (7) Segurança e boas práticas (Tarefas voluntárias); (8) Superintendência (autoridade de supervisão); (9) Dados nacionais supervisão. (regime de controle); (10) Manejo final.

Mesmo os regulamentos europeus têm uma estrutura semelhante.(UNIÃO EUROPEIA, 2016).

3.2 CICLO DE TRATAMENTO DE DADOS

A relação de tratamento e qualquer operação realizada com dados pessoais, como os referentes aos dados são as seguintes: coleta, processamento, recepção, classificação, uso, acesso, reprodução, transmissão, distribuição, tratamento, arquivamento, armazenamento, eliminação, avaliação ou controle de informações., modificação, comunicação, cessão, difusão ou extração.

Os representantes que devem ser mencionados são titulares, controladores, operadores e encarregados; as figuras abaixo referem-se diretamente à relação de tratamento de dados pessoais.

Figura 1 – Ciclo de tratamento de dados

Fonte: Confluence; Informativo, Entenda a finalidade da Lei geral de proteção de dados

Os encarregados, definidos no inciso Vlll da LGPD, tem o dever de preencher a lacuna entre o controlador de dados, o agente responsável pela gestão de dados e aautoridade nacional. Incluído na autoridade devida, inclui a aceitação de reclamações de proprietários e pedidos de esclarecimento e comunicação com a autoridade nacional, vindo a fornecer orientações sobre medidas e práticas cautelares a adotar na área da proteção de dados pessoais, devendo, conforme o art. 41, ao controlador definir os encarregados pelos dados e deixar suas informações expressas de forma pública.

Operador foi definido no inciso Vll do artº 6 da LGPD, também podendo ser

pessoanatural ou jurídica, de direito público ou privado. É a pessoa que irá executar todos os procedimentos de processamento de dados sob as formações do controlador, devendo ressaltar que na LGPD fica claro em seu Art. 6º, que o Operador estará sob o princípio da transparência, sendo de suma importância repassar informações clarase objetivas ao titular da informação.

O Controlador, de acordo com a definição legal em seu art 5º, inciso Vl, é a pessoa natural ou jurídica, podendo ser de direito público ou privado, responsável pela tomada de decisões relacionadas ao gerenciamento de dados pessoais, devendo, com base no art. 9º, inciso lll, permitir o direito do titular dos dados o acesso às informações relacionadas ao mesmo.

Atendendo às normas legais, define as modalidades de tratamento dos dados pessoais, uma vez que compete ao responsável pelo tratamento designar o responsável e elaborar relatórios de impacto, incluindo dados pessoais confidenciais, relacionados com operações de processamento.

O Titular é o principal beneficiário da cobertura protetora oferecida pela LGPD. Oprincipal objetivo da lei é garantir sua liberdade, sua privacidade e a livre expressão de sua personalidade. De acordo com a definição legal, o titular é a pessoa singular a quem dizem respeito os dados pessoais a tratar, consequentemente, a LGPD não tem interesse no tratamento de dados de pessoas jurídicas;

Autoridade Nacional de Proteção de Dados (ANPD) é o terceiro envolvido no tratamento de dadospessoais. De acordo com a estrutura estabelecida pelo decreto nº 10.474/2020, a ANPD tem quatro funções principais: Normativa: tem como objetivo proteger os dados pessoais através do regulamentaçãolegal; Educativa: tem como objetivo conscientizar a população dos perigos na falta decuidados e divulgação das novas políticas públicas; Fiscalizatória e Punitiva: como o próprio nome sugere, tem o poder de polícia, monitorando o fluxo de tratamento de dados e aplicando punições em caso de descumprimento ao que está visto em lei.

3.3 PRINCIPIOS QUE REGEM A LGPD

A lei geral de proteção de dados estabelece uma série de princípios aos quais todapessoa deve se basear para proceder ao tratamento de dados pessoais. São eles:

- Princípio da finalidade: tanto a coleta quanto o gerenciamento dos dados devem ser claros e explanados ao proprietário, que deve consentir com isso.

Tratamentos diferentes do acordado não podem ser realizados.

- Princípio da adequação: trata do contexto em que o interessado consentiu no tratamento, ou seja, a compatibilidade do tratamento com afinalidade comunicada ao interessado.

- Princípio da necessidade, dispõe sobre a limitação do tratamento e recolha de dados ao mínimo necessário para o efeito. Sendo assim não é permitida a coleta excessiva de dados que não correspondam à finalidade.

- Princípio do livre acesso: garante aos titulares uma consulta simplesclara e objetiva de forma gratuita como estão sendo tratados os seus dados, por quanto tempo e com que finalidade.

- Princípio da qualidade dos dados: este princípio refere-se à exatidão dos dadosà clareza da atualização e à pertinência, de acordo com a necessidade e finalidade da coleta de dados.

- Princípio de transparência: tem como objetivo garantir que os dados sejam claros, precisos e facilmente acessíveis aos titulares dos dados.

- Princípios de segurança: os dados devem ser armazenados de forma segura usando uma variedade de métodos. para impedir o acesso não autorizado as informações pessoais dos titulares em questão.

- Princípio da prevenção: Aborda a adoção de medidas para prevenir danos resultantes do tratamento de dados pessoais.

- Princípio da não-discriminação: limitar o tratamento de dados pessoais. Impedindoassim o processamento para fins preconceito ou divisão social.

- Princípio de responsabilidade: as empresas devem demonstrar que executam medidas eficazes para garantir o cumprimento de todos os regulamentos de proteção de dados pessoais e a eficácia das medidas tomadas.

4 O PODER DOS DADOS EM MEIO A FINS CORPORATIVOS E SUA RELAÇÃO COM O MERCADO

4.1 A COMERCIALIZAÇÃO DE UM DIREITO FUNDAMENTAL

Neste capítulo, de maneira introdutória, ressaltaremos que a Lei Geral de Proteçãode Dados (LGPD) é regulamentada pela lei de nº 13.709/18 e entrou em vigor em 2020, “que estipula o tratamento de dados pessoais, incluindo suportes digitais a proteção dos direitos fundamentais à liberdade e privacidade além do livre desenvolvimento da personalidade do particular”. Seus fundamentos estão alicerçados na expansão informacional promovida pela digitalização dos dados em Big Data, na qual a lei deve garantir direitos privados como a privacidade e a autodeterminação informacional no que se refere ao comportamento de empresas que utilizam ou negociam dados na área de segurança de TI.

A criação do quadro jurídico nacional vindo com a LGPD tem por objetivo fazer valer os direitos básicos relacionados com a privacidade através da proteção dos dados pessoais, indispensáveis ao exercício da cidadania à autodeterminação dos dados e à garantiada dignidade da pessoa humana.

Ao mesmo tempo, também busca fortalecer os princípios da livre concorrência e propõe um caráter regulatório para os dados que visa criar uma cultura das organizações que protegem os dados pessoais, promovendo conceitos importantes para as empresas como reputação e confiança.

A LGPD requer regulamentação uniforme, haja vista o surgimento de uma economia baseada em dados que pode dar segurança jurídica a esses processos financeiros, e sustentar a economia. Traz, portanto, sólida perspectiva jurídica para todos os setores da economia onde permeia o tratamento de dados pessoais. Assim, qualifica e dá condições para a criação de uma cadeia produtiva baseadaem dados e processos decisórios automatizados no Brasil. O sujeito da lei que ele protege como produtor de dados é o portador dos dados.

O principal vetor da LGPD é a autonomia privada no ato do consentimento “expressão livre, informada e inequívoca pela qual o titular consente no tratamento de seus dados pessoais para fim determinado”, (art. 5º, XII), da mesma forma que oMarco Civil da Internet (Lei nº 12.965/2014) garante o consentimento como elemento essencial para o exercício dos direitos relacionados à internet e ao exercício da

cidadania, o consentimento é a parte crucial da gestão de dados pessoais de acordo com a lei.

Analisando a trajetória normativa do conceito de consentimento, apontando a existência de visões conflitantes de cidadãos que defendem o consentimento, esta é uma visão puramente prescritiva, considerando a intensidade e as consequências comportamentais da disseminação da informação garantindo que existem (ultra)vulnerabilidades que precisam ser protegidas, ao mesmo tempo em que garante que os cidadãos tenham controle sobre seus dados.

Portanto, esta é a dualidade da proteção de dados: por um lado, revela a importância da autonomia privada e, por outro, entende que os consumidores estão em uma posição extremamente frágil em suas relações com as grandes tecnologias. A introdução da economia de vigilância política limita essa autonomia privada ao ato de expor seus dados pessoais estando sobre o controle direto de máquinas anônimas e de maioria inacessíveis.

O consentimento como asserção de direitos relacionados aos dados digitais é polémico justamente por buscar consagrar a liberdade e a autonomia privada em um cenário de profunda desigualdade na gestão de dados, dada a assimetria de infraestrutura e conhecimento sobre data Science.

Na era da *big data*, especialmente quando se trata dos últimos progressos em aprendizado de máquina e inteligência artificial, diante desse papel central da liberdade individual a LGPD sugere como materialmente possível no campo do consentimento, o consentimento é interposto sobre formas de análise e uso de dados que o ser humano não pode sequer conceber.

A chamada cidadania digital, também sugere uma pessoa jurídica digitalizada, ouseja, com direitos relacionados a dados digitais. A condição de sujeito de direito é um paradigma que decorre e regula a acumulação capitalista, ou seja, é uma forma jurídica que medeia a troca de bens sob o pressuposto de relações completamente voluntárias, sob a livre manifestação de sua vontade. Desta forma, não há capitalismo, no entanto, esta é a natureza puramente formal das relações sociais.

Não é novidade que mudanças estão acontecendo constantemente na sociedadealterando significativamente o estilo de vida das pessoas. Nesse contexto fenomenal, e embora a organização social atual não se limite ao ambiente virtual, as inovações tecnológicas desempenham um papel importante na etapa de organização da sociedade e produção de riqueza, pois permitem grande quantidade de informações

de qualquer parte do mundo a ser processado e transmitido quase em tempo real.

Nesse cenário, a informação tornou-se o centro gravitacional da nova forma de organização social e econômica, denominada sociedade da informação, pois não só altera as relações sociais, redefinindo noções de tempo e espaço, como também tem valor comercial.

A principal característica econômica da sociedade em rede, dinamiza a produção de riqueza em um sistema econômico que progressivamente valoriza o banco de dados como mercadoria e fator gerador de valor econômico de modo especulativo. Corporações privadas como Google e Meta acumulam todos os tipos de dados pessoais sobre os usuários na Internet, tais como seus padrões de navegação, preferências culturais, compras realizadas online, religião, corporal, ideológica, websites de interesse, expressões entre diversos outros tipos de dados pessoais, “impressões digitais eletrônicas” que servem para estabelecer uma categorização minuciosa de cada usuário na rede.

Segundo Bioni (2020, p. 11), não basta avaliar a informação em si para torná-la produtiva para a estratégia empresarial, é preciso transformá-la em conhecimento aplicado sobre o comportamento humano, mais precisamente sobre os hábitos de consumo das pessoas. Assim, a nova ordem econômica utiliza essas informações, que são dados das experiências humanos, como matéria-prima para fins comerciais, segmentando campanhas para perfis específicos de consumo e criando produtos cada vez mais personalizados, que acabam orientando as escolhas dos usuários e criando uma personalidade comercial para cada pessoa, dando um valor diferente para cada usuário.

Nesse sentido, a informação expressa uma nova lógica de acumulação de capital, conhecida como capitalismo de vigilância, que se nutre de uma proposta chamada Big Data, cujo principal objetivo é extrair dados pessoais para combiná-los para prever o comportamento do consumidor.

Nas palavras de Bueno (2020), "Esta nova forma de mercado assume que satisfazer as necessidades reais dos indivíduos é menos lucrativo do que vender previsões eletronicamente coletadas de seu comportamento". Para Zuboff (2019), a lógica da *big data* vai além da mera previsão decomportamento. Explica o autor que, para que os lucros aumentem, as previsões devem ser cada vez mais precisas e diretas. Para isso, será necessário explorar cada vez mais dados não apenas para prever, mas também para modificar o comportamento humano como meio de gerar

renda e controlar o mercado (ZUBOFF, 2019, p. 18). Por meio disso, quem tiver a capacidade de compreender e manipular o consumidor, terá um enorme poder de mercado.

Bioni (2020, p. 36) ressalta que o que leva empresas e governos a usar *big data* é a capacidade de achar com precisão correlações entre agrupações de dados derivados de situações do mundo real. Mas não entendendo a causa a capacidadede predizer o futuro. *Big Data* é um sistema complexo, pois é praticamente impossível de ser interpretado pela mente humana, por isso o processamento de dados massivos, como os gerados sobre a população de grandes países, por exemplo, tem exigido investimentos em novas tecnologias.

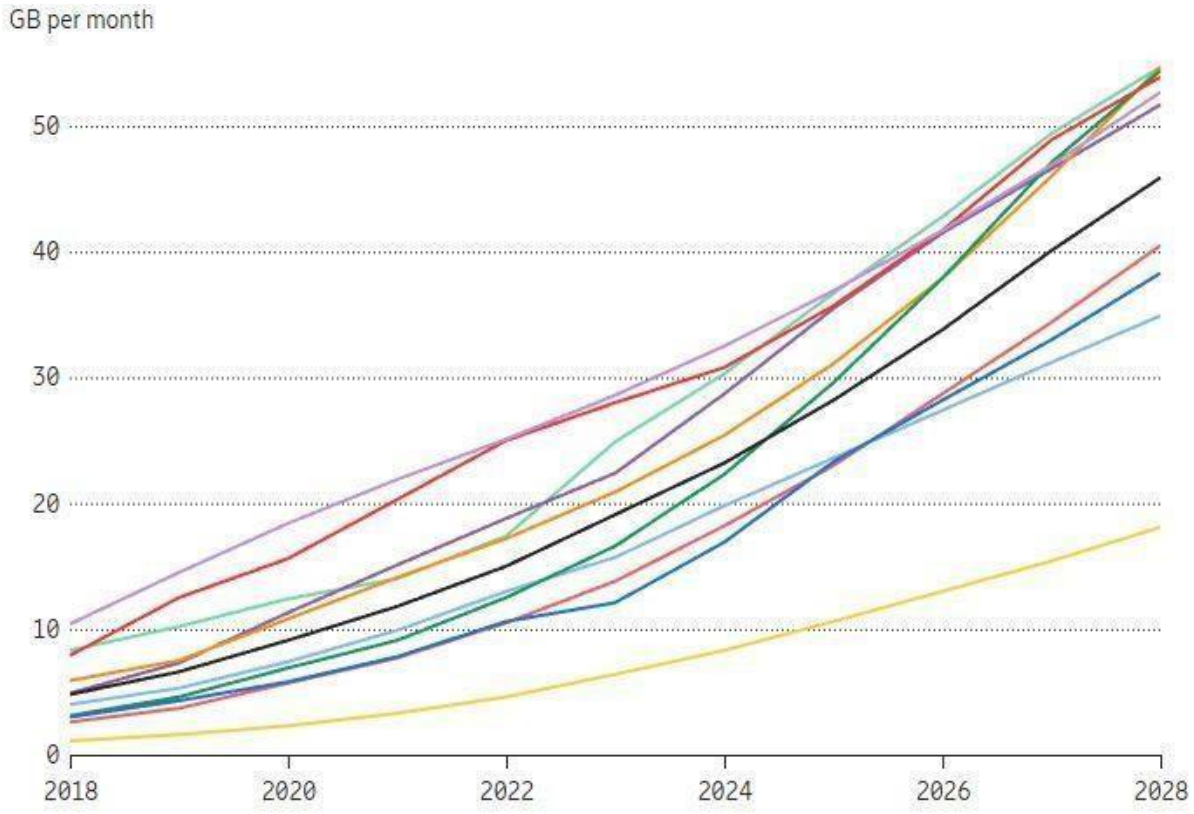
A análise de dados algorítmicos e uso de inteligência artificial que permitem o uso para melhorar serviços públicos, como erradicação de epidemias, como nas circunstancias da COVID19, do qual os sistemas de inteligência artificial auxiliaram a uma agilidade e melhor analise situacional da expansão viral ou o mapeamento de ações criminosas e organização do trânsito entre outros benefícios, Em meio a isso Crawford e Boyd (2012) descrevem *big data* como um:

> um fenômeno cultural, tecnológico e acadêmico baseado na interação de três fatores: (1) Tecnologia: maximização da precisão dos algoritmos e do poder de computação para reunir, analisar, relacionar e comparar grandes conjuntos de dados; (2) Análise: processamento de grandes conjuntos de dados para identificar padrões para atender às necessidades de ordem econômica, social, técnica e legal; e (3) Mitologia: a ampla crença de que grandes conjuntos de dados possibilitam uma forma mais avançada de inteligência e conhecimento que podem gerar insights até então impossíveis de se alcançar, de forma objetiva e confiável (BOYD; CRAWFORD, 2012, p. 2 **tradução nossa**).

Com o processo de informatização dos sistemas de gestão e o surgimento da internet a população depende cada vez mais das tecnologias digitais para acessar serviços e viabilizar suas atividades de trabalho e lazer.

Foi debatido no evento da *Ericsson Mobility Report 21*, um estudo chamado *Visual Networking Index*, onde afirmava-se que em 5 anos existiram o equivalente a 8 bilhões de smartphones no mundo, ao menos 1 smartphone por pessoa. Isso representa um crescimento de 28% em comparação a 2018, no entanto, impulsionadas pelo fator da COVID-19. Sendo assim, as realidades atuais exigem uma sociedade conectada e integrada e o uso de dispositivos que fornecem conectividade ilimitada como indicada na Figura 2 abaixo.

Figura 2 – Evolução do uso de smartphones e internet



Fonte: Ericsson Mobility Report data and forecasts Mobile data traffic outlook.

Na Internet, os usuários tornam-se consumidores que interagem e compartilham opiniões sobre suas experiências com determinados produtos ou serviços, passam aparticipar ativamente do ciclo de consumo, condição para a criação do próprio produto ou serviço: cocriadores (prossumidor).

A Internet facilita, assim, a organização dos dados pessoais de forma mais evolutiva, tornando-se um elemento estratégico e transformador do marketing em geral, uma vez que permite experiências cada vez mais personalizadas, garantindo o encontro entre os interesses do consumidor e o bem de consumo de forma cirúrgica. Nesse sentido, os dados pessoais do consumidor são ativos na economia da informação, pois facilitam o sucesso do estímulo ao consumo por meio da publicidade direcionada, por que as informações pessoais são uma visão geral de nossas atividades sociais e personalidade.

Nesse cenário, a capacitância de coleta de dados foi estendida a casos surpreendentes, atingindo conjuntos de informações de consumidores coletados por meio de cadastros ou bancos de dados de consumidores.

A esse respeito, vale ressaltar que a legislação não diferencia banco de dados deregistro de consumo: os conceitos são tratados indistintamente na Lei nº 8.078/90 do Código de Defesa do Consumidor, em seu art. 43, como um consumo de coleta e armazenamento de informações do consumidor.

4.2 FUNCIONAMENTO DE DADOS COM MACHINE LEARNING

Devemos entender mais a funcionalidade dos dados na sua aplicação real cotidiana. Sendo assim as diferenças entre bancos de dados e cadastros de consumidores são registradas em origem e destino dos dados no seguinte sentido: bases de dados são aleatórios, e os registros de consumo pressupõem uma relação jurídica entre fornecedores e consumidores: como a compra em lojas tipo “Amazon”.

Os bancos de dados organizam as informações para uso futuro, enquanto os cadastros de consumidores utilizam as informações imediatas. Nas bases de dados, o armazenamento de dados não requer consentimento do consumidor e os registros do consumidor dependem do consentimento prévio do consumidor. O objetivo dos bancos de dados é transmitir informações a terceiros e os cadastros de consumidores utilizam os dados em tempo hábil.

Em outras palavras, tanto o banco de dados quanto o registro são coleções de informações sobre um consumidor. No entanto, eles diferem porque o banco de dados coleta informações do mercado enquanto o cadastro consiste em informações fornecidas diretamente pelo consumidor, sendo assim, milhares de bases de dados foram criadas para identificar (perfilar) padrões de comportamento na internet através do uso de *Machine learning* e há vários exemplos de como esse mercado pode ser manipulador e lucrativo.

Segundo o portal Economatica3, o valor de mercado do Google Inc. é de US$ 2 trilhões de dólares dólar enquanto o da megacorporação Meta é de US$ 677 bilhões de dólares dólar após uma queda de 20% devido ao fracasso do meta-verso. A ligação entre dados e finanças é irrefutável.

Os instrumentos digitais converteram-se em uma rede crucial de informações, tornando-se um bem valioso (CRESPO,2011, p 38).

É importante ressaltar que para o propósito deste estudo não discutiremos questões éticas relacionadas a este tema. No entanto, por uma questão de informação existe a ideia de que a lógica da big data coloca os consumidores em uma bolha social,

isso ocorre porque a construção de perfis internos tornar a experiência de cada usuário na internet tão privada que eles podem permitir isso ourestringir o acesso apenas às informações conteúdos considerados relevantes, paraum determinado fim, como expressado por Freitas e Pamplona (2017);

> Assim, a informação fragmentada é resultado da aplicação desistemas de informação dispersos e heterogêneos, que estãosendo projetados de forma independente por diferentes empresas, a fim de aperfeiçoar individualmente a informação desejada por cada um dos usuários a partir de implementação de processos específicos com base no conjunto de dados de cada usuário (FREITAS; PAMPLONA. 2017, p. 121).

No entanto, os consumidores certamente não sabem o custo real desse das Informações ou de qual informações podem ser extraídas atualmente, O consentimento é mais propriamente assumido como uma pretensão de um ato unilateral, cujo efeito é supostamente autorizando um determinado processamentode dados pessoais. Nesse sentimento, Tepedino, Frazão e Oliva (2019) afirmam que:

> [...] o mercado de dados em geral cresce a partir da difusão de visões como a de que o modelo de negócios é justo, já que os usuários receberiam contrapartidas adequadas pelos seus dados, ou mesmo necessário, dado que haveria um verdadeiro trade-off entre inovação e privacidade, de maneira que a violação desta última seria o preço a pagar ou o mal necessário para o progresso tecnológico e os novos serviços que daí decorrem. Até a forma como a questão é apresentadajá reflete a perspectiva utilitarista que permeia a análise, pois se parte da premissa de que, em nome da inovação, é justificável o sacrifício de direitos fundamentais elementares (TEPEDINO; FRAZÃO; OLIVA, 2019, p. 31).

Assim, políticas de privacidade funcionam como um contrato de adesão, partindoda premissa de que o usuário está predisposto a aceitar qualquer conteúdo que lhe seja descrito, a partir do momento em que decide utilizar os serviços oferecidos.

Por meio deste contrato, o objetivo é garantir o consentimento do usuário para a legitimidade de toda e qualquer ação para o processamento de seus dados. O que se vivencia, na prática, é que o usuário clica em um botão "Concordo/Aceito", mas tem dificuldade de ler os longos e complexos termos e políticas de privacidade, além de muitas vezes não possuir informações tecnológicas suficientes para compreensão do mesmo, conhecimento para desvendar as peculiaridades da linguagem comumente utilizada nesses textos. Sendo assim e por diversas razões, este

mecanismo tem-se demonstrado falho, seja porque reforça a assimetria do mercado de informação, seja porque é uma ferramenta que não permite ao consumidor exercer controle sobre a sua informação pessoal.

Essa relação assimétrica de poder é ainda mais ampliada, como explica, sobre o assunto Zuboff. (2019) O autor defende a ideia de que os usuários da nova ordem econômica são apenas cadáveres abandonados, como elefantes após a extração do marfim (ZUBOFF, 2019). Nesse contexto, o titular dos dados não tem controle sobre o que pode acontecercom suas informações e está imerso em diversas incertezas na medida em que pode sofrer prejuízos decorrentes do uso indevido de seus dados pessoais. Danos imprevistos nos tornam vulneráveis não apenas tecnicamente, mas também de forma digital e econômico.

Além disso, deve-se levar em conta que além de coletar informações para fins comerciais, há também uma elaboração de perfil digital que estende o físico para o digital de uma pessoa através de suas informações, Uma Persona digital, como um segundo você, entendendo seus gostos e desprezos.

Este é o resultado do fenômeno de geração de dados. Isso porque, com base nasinformações coletadas, os perfis ou padrões são segmentados e classificados: são criados estereótipos e esse é um fator importante no processo de tomada de decisão. Com o desenvolvimento da tecnologia e dos algoritmos, uma inteligência artificial começa a tomar mais decisões.

Isso já é uma realidade e os exemplos não faltam. Não são mais os gerentes do banco que aprovam o crédito, é um algoritmo que vai coletar informações de um indivíduo e gerar uma valoração no mesmo, precificar se ele vale o credito solicitado ou não, ou seja, se aquele indivíduo é bom ou mau pagador, e com base nesse resultado, serão calculados os valores dos empréstimos e as taxas de juros.

Portanto, ter o controle dos dados não é apenas uma questão de segurança ou saber para que fins serão aplicados, mas também um meio de garantir que esses dados sejam coletados com qualidade para que as decisões tomadas sobre os usuários atinja o máximo de qualidade evitando fraudes e transtornos. Isso ocorre porque nossa capacitância de autodeterminação é cada vez mais calibrada por nosso uso de dados, Uma sociedade em que os cidadãos não têm controle sobre suas próprias informações põe em risco seu próprio sistema democrático.

A Constituição protege uma série de aspectos específicos relativos à privacidadedos titulares de dados. O ordenamento jurídico brasileiro também possui

poucos outros estatutos civis ou processuais e regulamentares com foco na proteção da privacidade (MENDES; DONEDA, 2019).

No entanto, para promover a responsabilização do interessado, surgiu a necessidade de regulamentação específica da matéria não só porque o tratamento indevido de dados pessoais pode violar os direitos de privacidade, tanto como outros direitos fundamentais do indivíduo, mas também porque o detentor tem um certo poder de pechinchar que pode equilibrar as assimetrias. Nesse contexto está a lei Geral de Proteção de Dados Pessoais (Lei nº 13709/2018).

5 RESPONSABILIDADE NO TRATAMENTO DE DADOS

A LGPD assegura ao titular, em seu art. 21 e entre outros direitos, que os dados pessoais relativos ao exercício regular dos direitos pelo titular não podem ser aplicados em prejuízo dos mesmos. A lei suscita ainda uma importante questão processual na defesa das garantias aí previstas, qual seja, a defesa dos interesses e direitos. Os direitos dos interessados poderão ser exercidos judicialmente,individual ou coletivamente, conforme os dispostos na legislação pertinente, quanto aos instrumentos de proteção individual e coletiva. Portanto, não há dúvida de que além da proteção dos dados pessoais, a LGPD prevê expressamente a proteção dosdireitos e garantias gerais nela contidos.

Com foco nesse tema, Roque (2019, p. 8) relembra a classificação do CDC, que divide os direitos coletivos nas seguintes categorias: existindo diferentes regimes jurídicos para cada categoria:(a)direitos distribuídos;(b) direitos coletivos em sentido estrito, e(c)direitos individuais homogêneos. As premissas (d) e (e) incumbem-se de proteção de direitos coletivos. Enquanto a última cláusula é um direito pessoal homogênea. Trata-se da proteção coletiva dos direitos coletivos da contingência homogênea dos indivíduos (ROQUE, 2019). Os autores não atribuem a categoria de direitos coletivos.

Questões abstratas como a proteção de dados pessoais, pois algumas nuances de um caso concreto podem afetar tais direitos coletivos, o que defendendo fundamentalmente errado. Neste sentido, a proteção coletiva de dados pessoais pode incluir:

> [...] direitos difusos (por exemplo, no caso em que se pretendecorrigir algum tratamento inadequado de dados pessoais realizado por autoridades públicas, relativamente a todos os que vivem em certa localidade – tutela indivisível e sem que exista uma relação jurídica base prévia que delimite o grupo), coletivos em sentido estrito (ilustrativamente, na hipótese em que se pede a adequação do tratamento de dados pessoais realizado por uma empresa, relativamente a seus consumidores – tutela também indivisível, mas referente a umarelação jurídica de consumo base) e individuais homogêneos (por exemplo, pleito de danos morais e materiais veiculado contra certa empresa decorrente do vazamento de dados de um grupo de pessoas – tutela que poderia ser postulada em ações individuais, existindo uma origem comum para os danosalegados) (ROQUE, 2019, p.10).

Nesse sentido, Roque (2019, p. 10) conclui que “é a categorização de direito coletivo, portanto, dependerá invariavelmente da análise da causa da ação e da demanda de tutela jurisdicional especificamente formulada", e propõe que, para

identificar qual categoriade direito se aplica a cada caso, duas questões devem ser respondidas; (a) a tutela édivisível, ou seja, "está sujeita a cisão em ações individuais, sem necessariamente terrepercussão no campo jurídico dos demais titulares". Se a resposta for positiva, estamos diante de direitos individuais homogêneos; em caso negativo, impõe-se uma segunda questão; (b) “sendo a tutela indivisível, existe uma conexão jurídica fundamental, responsável pela constituição do grupo?” Se, por sua vez, a resposta for positiva, configura-se a presença de direito coletivo em sentido estrito, se a resposta for negativa e, portanto, a formação do grupo se basear em simples circunstâncias fáticas, estamos diante de um direito difuso.

Ao resumir a análise da governança geral da proteção de dados pessoais, a questão então foi levantada sobre quem teria o direito de iniciar a ação apropriada. A LGPD não fez qualquer referência a esta questão, devendo, portanto, ser utilizadas as principais fontes do processo coletivo, a saber, a Lei de Processo Civil Público (nº 7.347/1985), especialmente em seu art. 5º, e art. 82 do código do consumidor.

Assim, como se depreende da leitura dos referidos artigos, são legítimos para intentar ação indenizatória em caso de vazamento de dados: o Ministério Público e a Defensoria, quando houver necessidade a administração pública, entre eles a Agencia Nacional de Proteção de Dados (ANPD), e as associações civis, nos termos da legislação em vigor. Quanto ao particular, segundo Roque (2019), só será legitimado para a atividade Popular, embora, pelas particularidades que esta ação possui, seja difícil para o autor imaginar uma hipótese na qual concorra.

Em todo caso, Roque (2019) não exclui a possibilidade de que a legitimação do indivíduo, desencadeia ações coletivas, quando, por exemplo, no município onde reside, não exista outras legitimadas e que a infração seja perpetrada pela administração pública(ROQUE 2019, p. 12-13). Assim, a partir da leitura conjunta do art. 22 e 42 da Lei geral de proteção de dados (LGPD), bem como as disposições das Leis de ações civis públicas e da Lei de defesa do consumidor conclui-se que a legislação brasileira permitirá medidas repressivas na esfera administrativa para proteção de dados pessoais utilize o microssistema proteger direitos considerados difusos, e promover a atuação dos órgãos civis especializados, bem como do Ministério Público e da ANPD junto ao poder judiciário.

Vale citar aqui o Acórdão do recurso Extraordinário (RE) nº 1101937, que trata daconstitucionalidade do art. 16, da lei da Ações Civis Públicas, que limita a eficácia dessas sentenças à competência territorial do órgão que as profere, que por fim

votaram pela inconstitucionalidade da norma.

O fator preocupante em relação a essa questão é que os dados dos brasileiros estão sendo divulgados pela internet e são necessários mecanismos para protegê-los, ameaçando sérios danos à sociedade como um todo.

O problema é alarmante, principalmente considerando os 57 escândalos de vazamento de dados ocorridos nos últimos dois anos: o vazamento de dados da Enel, concessionária de energia de São Paulo; o Tesouro Nacional, que foi invadidopor um *ransomware* em 2021 do qual o governo vigente noticiou que não havia gerado danos ao sistema do tesouro; já em outubro foi a vez de Hari-Express, Correios, Magazine Luiza Mercado Livre e *Shopee*, sofrendo o vazamento de 1,7 bilhões de dados sensíveis vazados totalizando 610Gb; e, finalmente, e por duas vezes o Ministério da Saúde foi invadido em 2020 e 2021 relatando vazamentos, dos quais os dados foram vazados de cerca de 223 milhões de brasileiros.

Se consideramos a hipótese de que 10% dos brasileiros entram com ações individuais por danos decorrentes de tais vazamentos, teremos cerca de 20 milhões de novos processos na Justiça, representando pelo menos dezembro de 2019 dos 77,1 milhões que serão avassaladores.

Portanto, a delimitação coletiva ao órgão que prolatou, conforme sugere o artigo oart. 16 da LACP, não só traz séria insegurança jurídica, como também contribui para a superlotação do Judiciário, que também dispõe de recursos limitados e não pode ficar à mercê de pedidos individuais propostos por cada estado brasileiro. No entanto, dado que a proteção de dados é um repto para a administração da justiça, o STF tem a oportunidade de garantir o efeito nacional das decisões proferidas em processos civis públicos e, consequentemente, evitar um possível colapso do sistema, previsto no art. 10 e pelo art. 16 que é considerado inconstitucional. Exemplo contrário, o risco de superlotação pode ser ainda maior se aceitarmos a responsabilidade civil objetiva e a conjectura dos danos pois o lesado nem precisa provar que sofreu algum dano efetivo para que a violação ocorra e tenha direito, a indenização por dano moral e material.

A forma de evitar a justiça em massa é a transparência e o plena conscientização dos envolvidos, a fim de demonstrar com firmeza que a porta para resolver a confusãoestá inicialmente com o controlador de dados em questão e não com o sistema de justiça.

6 CONSIDERAÇÕES FINAIS

A nova era tecnológica necessita de adaptação, e adaptação requer tempo assim como a adaptação de normas expostas por uma nova lei, não acontece da noite para o dia, A LGPD se aplica a governos e empresas, devendo garantir maior segurança aos dados pessoais. Ainda haverá um tempo em que as empresas principalmente as pequenas não saberão das boas práticas de tratamento de dados.

Embora a lei geral de proteção de dados pessoais seja focada em fins de proteção econômica, demonstra que a natureza jurídica da responsabilidade é subjetiva e a sua estrutura jurídica reforça um sistema integrado para fim de proteger os interesses coletivos

Os fundamentos constitucionais deixam determinado que o respeito à privacidade, liberdade de expressão, inviolabilidade intimidade, são alguns dos fundamentos básicos que o indivíduo detém para si como direito pétreo, Por conta disso o ainda assombra o perigo de que as informações que sejam monopolizadas por entidades privadas, acarretem uma maior chance de ocorrer abusos, já que apesar das evoluções a lei ainda depende muito da questão de confiar que as empresas irão agir da forma correta.

Vindo de um medo ou receio de se sentirem invadidas, cada vez mais pessoas pedem maior transparência no uso de seus dados pessoais. Em um futuro não muito distante, a transparência e o cuidado com o consumidor serão requisitos para a contratação de um serviço ou aquisição de um produto.

Sendo assim é crucial que as medidas transcendam a confiança de que as empresas irão agir de forma correta, sendo assim, lidando com o problema preventivamente antes de chegar ao sistema judiciário, evitando assim uma super lotação por excesso de processos.

REFERÊNCIAS

BRANDEIS, Louis; WARREN, Samuel. The Right to Privacy. **Harvard Law Review,** v. 4, n. 5, 1890, p. 193-220.

BRASIL. **Lei nº 7.347, de 24 de julho de 1985**. Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico (VETADO) e dá outras providências. Brasília, DF, 1985. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm>. Acesso 12 nov. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm. Acesso em14 nov. 2022.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF, 1996. Disponível em:<https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso 14 de novembrode 2022.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Brasília, DF, 1997. Disponível em:<https://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acessoem: 13 nov. 2022.

BRASIL. **Lei nº 10406, de 10 de janeiro de 2002.** Institui o Código Civil. Disponível em:< https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 11 nov. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF, 2011. Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso: 15 nov. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF, 2012. Disponível em:< https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 12 nov. 2022.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018**. Dispões sobre a Lei geral de proteção de dados. Brasília, DF, 2018. Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso: 15 nov. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais.** A função e os limites do consentimento. Rio de Janeiro: Ed. Forense Ltda., 2020.

BOYD, Danah; CRAWFORD, Kate. Critical questions for Big Data. **Information, Communication & Society**, v. 15, n. 5, 2012, p. 662-679.

BUENO, Claudio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, a. 21, n. 53, Jan./Mar., 2020, p. 97-115.

FREITAS, Cinthia; PAMPLONA, Danielle. Cooperação entre estados totalitários e corporações: o uso da segmentação de dados *profiling* para violação de direitos humanos. Disponível em:<https://www.passeidireto.com/arquivo/53270691/pamplona-cooperacao-entre-estados-totalitarios-e-corporacoes>

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro**. Sequência Estudos Jurídicos e Políticos**, [S. l.], v. 38, n. 76, 2017**,** p. 213–240.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

UE. **Jornal Oficial C 303 da União Europeia.** UE, 1948. Disponível em:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C:2007:303:FULL&from=en>.

FERNANDES, Camila. **Análise das Leis no 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimescibernéticos.** 2013. Monografia (Bacharelado em Direito) - Faculdade Baiana de Direito, Salvador, 2013.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteçãode Dados (Lei 13.709/2018). **Revista de Direito do Consumidor**, São Paulo, n. 120, nov./dez., 2018 p. 469-587.

OCDE. **Diretrizes da OCDE sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais.** 2002. Disponível em: <https://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso: 14 nov. 2022

OLIVEIRA JUNIOR, Eudes Quintino. A nova lei Carolina Dickman**. JusBrasil,** 2012. Disponível em:<https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>. Acesso: 14 nov. 2022.

ROQUE, André. A Tutela Coletiva dos Dados Pessoais na Lei Geral de Proteçãode Dados (LGPD). **Revista Eletrônica de Direito Processual,** Rio de Janeiro, v. 20, n. 2, maio/ago., 2019, p. 1-19.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 23-52.

UNIÃO EUROPEIA. Diretiva 95/46 do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. **Eur-Lex**, 1995. Disponível em:<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046>. Acesso em: 25 set. 2022.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR)**, UE, 2016. Disponível em:<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 25 set. 2022.

ZUBOFF, Shoshana. Big Other: **A era do capitalismo de vigilância**. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.