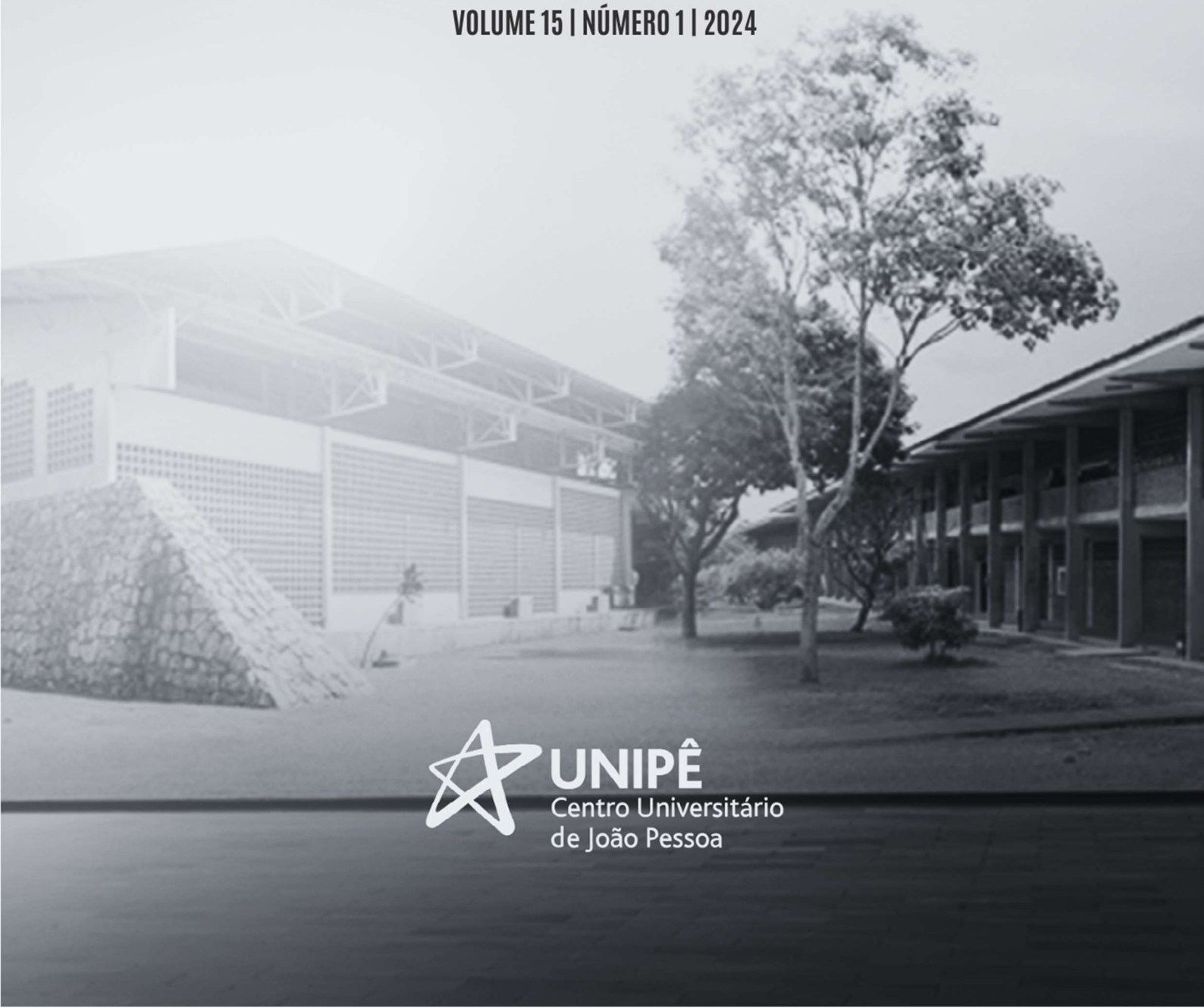
ISSN 2236-0859

DIREITO & DESENVOLVIMENTO

REVISTA DO PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO E DESENVOLVIMENTO SUSTENTÁVEL

VOLUME 15 | NÚMERO 1 | 2024



UNIPÊ
Centro Universitário
de João Pessoa

O EMERGIR DA PROTEÇÃO DE DADOS COMO UM DIREITO AUTÔNOMO NO CONTEXTO DA SOCIEDADE DIGITAL E DA INFOESFERA

THE EMERGENCE OF DATA PROTECTION AS AN AUTONOMOUS RIGHT IN THE CONTEXT OF DIGITAL SOCIETY AND THE INFOSPHERE

Mateus de Oliveira Fornasier [86]
Fernanda Viero da Silva [87]
Benhur Aurélio Formentini Nunes [88]

RESUMO

O presente artigo investiga a proteção de dados pessoais no contexto da era digital e de que forma as violações à privacidade e a má utilização de dados pessoais ferem a esfera íntima da pessoa e de qual forma são tuteladas juridicamente no Brasil emergindo assim como direito autônomo. Parte do seguinte problema: de que forma a proteção de dados pessoais migrou de um mero aspecto da privacidade a direito verdadeiramente autônomo? A hipótese preliminar aponta que as fronteiras entre o ambiente físico e digital esvanecem e não estão somente alterando a percepção do homem quanto a estes espaços, mas também alteram dinâmicas sociais, produzindo riscos à esfera intima dos agentes com o armazenamento, o acesso, o tratamento e o

[86] Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS, Brasil) (2013), com Pós-Doutorado pela University of Westminster (Reino Unido) (2018-2019). Atualmente é professor/pesquisador da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI), no programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direito. Email: mateus.fornasier@gmail.com
87 Doutoranda em Direito pelo programa de pós-graduação Stricto Sensu (mestrado e doutorado) em Direitos Humanos da Universidade Regional do Noroeste do Estado do Rio Grande do Sul - UNIJUÍ com bolsa integral CAPES/PROSUC. Mestre em Direito pelo referido programa com bolsa integral CAPES/PROSUC (2023). Pós-graduada (Especialização) em Advocacia no Direito Digital e Proteção de Dados pela Escola Brasileira de Direito - EBRADI (2021). Bacharel em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul - UNIJUÍ (2020). Email: fefeviero@gmail.com
88 Mestre em Direitos Humanos no Programa de Pós-Graduação Stricto Sensu da UNIJUÍ-RS. Pós-graduado em Direito Público: Constitucional, Administrativo e Tributário pela PUCRS. Possui graduação em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul (2019). . Email: benhur.nunes@gmail.com

compartilhamento de dados pessoais, suscitando assim a necessidade de regulação frente ao paradoxo da privacidade, emergindo assim um direito autônomo. Objetivos específicos: a) compreender a transformação da sociedade na era digital a partir das redefinições da esfera física e virtual e das fronteiras entre o analógico e o digital; b) estudar o paradoxo da privacidade no que tange a proteção de dados e a privacidade na era digital; c) identificar quais são os marcos regulatórios da estrutura jurídica brasileira para tanto e a influência do contexto normativo europeu. Como resultados, tem-se que a hipótese é confirmada. Metodologia: hipotético-dedutiva, com método de abordagem qualitativo e abordagem bibliográfica.

Palavras-Chave: Privacidade. Proteção de Dados. Regulação.

ABSTRACT

This article investigates the protection of personal data in the context of the digital age and how breaches of privacy and misuse of personal data violate an individual's intimate sphere and are legally protected in Brazil, thus emerging as a distinct legal right. It addresses the following problem: how has the protection of personal data transitioned from a mere aspect of privacy to a truly autonomous right? The preliminary hypothesis suggests that the boundaries between the physical and digital realms are fading, not only altering human perception of these spaces but also changing social dynamics, posing risks to individuals' intimate sphere through the storage, access, processing, and sharing of personal data, thereby prompting the need for regulation in terms of the privacy paradox, leading to the emergence of an independent right. Specific objectives include: a) understanding the transformation of society in the digital age through the redefinitions of physical and virtual spheres and the boundaries between analog and digital; b) studying the privacy paradox concerning data protection and privacy in the digital age; c) identifying the regulatory frameworks within the Brazilian legal structure and the influence of the European normative context. As results, the hypothesis is confirmed. Methodology: hypothetical-deductive, with a qualitative approach method and bibliographic approach.

Key-words: Data Protection. Privacy. Regulation.

1 INTRODUÇÃO

Conforme a dinâmica das transformações sociais adquire velocidade cada vez maior, a forma através da qual se observa a necessidade de proteger determinados direitos precisa ser revista ou repensada. A revolução tecnológica sem precedentes, na verdade, tem remodelado a realidade humana. Não se trata mais de prever formas de proteger direitos "online" ou "na rede": está-se diante de um mundo em que a fronteira entre o digital e o físico está, aos poucos, se desfazendo.

O direito humano à proteção de dados pessoais é tema de recente abordagem e tratamento por diversos sistemas jurídicos. Ao se considerar que a proteção de dados é elevada a direito fundamental, se reconhece a importância desse direito considerando sua evolução em paralelo às mudanças tecnológicas e sociais experimentadas.

No direito interno brasileiro, o tema consta de forma explícita no texto constitucional somente a partir da Emenda Constitucional nº 155, de 2022, através da inserção do inciso LXXIX no artigo 5º da Constituição Federal. Anteriormente, esse princípio era considerado implícito pela doutrina e pela jurisprudência, através da interpretação dos incisos XII e LXXII do mesmo artigo da Carta de 1988, que tratam, respectivamente, da inviolabilidade do sigilo de correspondências e do *habeas data*. Do ponto de vista internacional, a proteção dos dados pessoais passou por uma evolução, principalmente na Europa, a partir das primeiras leis na década de 1970, originadas de uma disposição inicialmente trazida pela Declaração Universal dos Direitos Humanos, que protegeu a privacidade, donde o direito à proteção de dados.

A presente pesquisa se propõe a debater as questões acima elencadas e irá se estruturar da seguinte maneira: em um primeiro

momento partirá da análise do conceito de infosfera (FLORIDI), traçando um panorama da sociedade atual e sua relação com a proteção de dados e a privacidade, estabelecendo que a forma pela qual o ser humano percebe a realidade mudou irreversivelmente com a revolução tecnológica que dissolve a fronteira entre o físico e o virtual, em uma hibridez na qual dados possuem a mesma importância e valor que outros bens jurídicos já há muito tempo tutelados juridicamente.

Na sequência, isso permitirá entender que a privacidade e a proteção de dados merecem ser tuteladas pelo direito, demonstrando haver a proteção de dados para além da privacidade, ou seja, compreender como o instituto próprio "proteção de dados" se descolou do direito à privacidade em termos gerais. Leva-se em conta que a forma como o ser humano percebeu a privacidade e o seu valor se modificou ao longo dos anos, na mesma medida em que a sociedade se tornou mais atrelada ao ambiente digital.

Por fim, será feita uma exploração da tutela jurídica do direito à proteção de dados pessoais, passando pelas primeiras regulações surgidas na Europa, abordando como o continente europeu chegou ao Regulamento Geral sobre Proteção de Dados (RGPD), diploma legal de referência sobre o tema. Após, será conduzida uma investigação dos caminhos percorridos pelo direito à proteção de dados no Brasil até o reconhecimento como direito fundamental, explícito na Constituição Federal, abordando, ao fim, a Lei Geral de Proteção de Dados (LGPD), lei que sistematizou recentemente a regulação dos dados pessoais no direito local.

Com isso, partimos do seguinte problema de pesquisa: como a proteção de dados pessoais deixou de ser apenas um aspecto da privacidade para se tornar um direito independente? Temos como hipótese inicial que as fronteiras entre o mundo físico e o digital estão se

dissipando, não apenas afetando a forma como as pessoas percebem esses espaços, mas também alterando as interações sociais. Isso gera riscos para a esfera íntima das pessoas devido ao armazenamento, acesso, processamento e compartilhamento de dados pessoais. Essa situação levanta a necessidade de regulamentação diante do paradoxo da privacidade, resultando na emergência de um direito autônomo.

O presente estudo justifica sua importância por visar estabelecer o direito à proteção de dados pessoais como um direito humano e fundamental, levando em conta as principais legislações sobre o tema, notadamente a brasileira, investigando quais seriam os aspectos mais importantes para a compreensão deste fenômeno, tanto do ponto de vista da tutela dos direitos fundamentais quanto do ponto de vista das transformações da sociedade em si.

Para realização desta pesquisa, observou-se o método de abordagem fenomenológico, que visa compreender e interpretar o mundo social a partir dos acontecimentos humanos. No que diz respeito ao método, o estudo mescla procedimentos monográficos, históricos e comparativos, a fim de fornecer uma pesquisa satisfatoriamente completa em torno do tema, ao mesmo tempo que delimitada e específica. Para tanto, o trabalho utilizou a técnica de pesquisa bibliográfica, pesquisando fontes mediatas e imediatas,

2 "INFOSFERA", PRIVACIDADE E PROCESSAMENTO DE DADOS

Luciano Floridi (1999) estabeleceu o conceito de infosfera, segundo o qual a sociedade está se transformando num ambiente no qual as fronteiras entre o virtual e o físico estão deixando de existir. É necessário, portanto, compreender como o autor vê essa

transformação e que, inevitavelmente, mudará a forma segundo a qual a própria realidade é percebida. Assim, é possível compreender como a privacidade adquiriu tanto valor e porque os dados pessoais são tão inestimáveis atualmente.

Autores notáveis concordam que, de fato, o ser humano está diante de uma verdadeira revolução digital e que a sociedade tende a se tornar informatizada em diversos níveis, cada vez mais profundos. Klaus Schwab estabelece, em *A Quarta Revolução Industrial*, que se enfrentamos uma grande diversidade de desafios fascinantes — entre eles, o mais intenso e importante é o entendimento e a modelagem da nova revolução tecnológica, a qual implica nada menos que a transformação de toda a humanidade. Estamos no início de uma revolução que alterará profundamente a maneira como vivemos, trabalhamos e nos relacionamos (SCHWAB, 2016, p. 14).

O autor considera, portanto, que esse conjunto de transformações sociais está ocasionando uma nova revolução industrial, e estabelece que a tecnologia não é nenhuma força externa ou estranha ao desenvolvimento humano, e que tampouco é incontrolável. Quanto mais o ser humano pensar e estudar sobre o fenômeno, maior serão suas condições de moldar a revolução da forma com que o mundo se torne um lugar melhor.

Shoshana Zuboff, por sua vez, apresenta uma visão ligeiramente mais pessimista, considerando que há perigos não percebidos e que a revolução está tomando a humanidade de forma menos perceptível. A autora entende que o mundo digital está ultrapassando e redefinindo tudo o que é familiar, mesmo antes de se ter a oportunidade de ponderar e decidir. Com isso, "celebramos o mundo em rede pelas muitas formas como enriquece as nossas capacidades e perspectivas, mas ele deu origem a novos territórios de ansiedade,

perigo e violência à medida que a sensação de um futuro previsível se esvai" (ZUBOFF, 2019, p. 10).

Assim, um questionamento importante é apresentado: o futuro digital pode ser nosso lar? Zuboff (2019) parece nos responder que sim, uma vez que admite que o acesso ao digital já está mais difundido do que a eletricidade. Embora pareça um dado estranho em uma primeira análise, ao fim evidencia que não há como se furtar da realidade digital. Não há como encarar um "exílio digital" e fugir da nova realidade.

No ponto que trata do quanto é perceptível ou não a tomada do digital sobre o real, o próprio Schwab (2016, p. 18) parece compreender que há sim certa falta de consciência sobre as transformações vivenciadas pela sociedade. Nesse sentido, a própria palavra "revolução" denota mudança abrupta ou radical, e que na história as revoluções têm ocorrido quando novas formas de tecnologia e percepção do contexto surgem, desencadeando alterações profundas nos mais variados sistemas sociais.

De fato, está-se diante de uma revolução sem volta, que é, ao mesmo tempo, alarmante por sua profundidade e imperceptível, por vezes, pela forma de perceber o tempo à qual a humanidade está acostumada. Zuboff (2019), então, se preocupa com a previsibilidade de um "futuro digital", e nessa mesma seara Schwab (2016) considera que a quarta revolução industrial está em andamento através da revolução digital que, embora não apresente necessariamente novas tecnologias (como a terceira revolução, que apresentou computadores, *softwares,* redes), está causando uma ruptura nas bases da terceira.

Então, o conceito sedimentado da quarta revolução digital apresentada pelo autor se forma ciente das várias definições e

argumentos utilizados para descrever as três primeiras revoluções industriais, e ela é caracterizada por ter uma internet "mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina)" (SCHWAB, 2016, p. 19).

Por mais que autores como os supracitados possam apresentar uma compreensão embasada da importância das mudanças que a era digital causou, está causando e vai causar na humanidade, os mesmos não chegam ao patamar que Floridi se propõe e explorar. Para que a presente investigação não encontre limites de compreensão em apenas estudar neologismos, deve-se investigar a forma como se constrói determinado termo como "hiperistória" e, mais adiante, a própria "infosfera", atribuídos ao autor, para que estes formem um contexto suficiente para compreensão dos fenômenos.

Floridi (2014) afirma que não se está mais diante de um tempo puramente histórico. A humanidade atravessou a pré-história, a história, e agora deve inevitavelmente adentrar na hiperistória. A pré-história é um tempo no qual a humanidade não conhecia quaisquer tecnologias da informação e comunicação (TIC). Já na história o ser humano tem seu bem-estar relacionado ao uso ou não das TIC. Por fim, na hiperistória o bem-estar da sociedade será dependente das TIC. Ou seja, "as TIC registam, transmitem e, sobretudo, processam dados, cada vez mais de forma autónoma, e as sociedades humanas tornam-se vitalmente dependentes delas e da informação como recurso fundamental" (FLORIDI, 2014, p. 52).

O conceito de Tecnologia da Informação e Comunicação por si já não é tão novo. Em termos amplos, são tecnologias digitais conectadas à uma rede (KENSKI, 2009). Então, o tempo hiperistórico de Floridi é atrelado ao quanto o ser humano e a sociedade são

dependentes das tecnologias de informação e comunicação. A partir desta ideia, o autor passa a desenvolver outro termo: a infosfera.

Conforme se extrai de Martens (2017), que analisou detidamente a origem do termo infosfera, apesar da palavra ser associada comumente a Floridi, trata-se de uma ressignificação feita pelo italiano a partir dos escritos de Boulding, datados da década de 1970. Logo, o termo "infosfera" se refere ao ambiente composto por todas as informações disponíveis e em circulação na sociedade. Esse conceito abrange ampla gama de fontes de informação, incluindo conversas, livros, televisão, rádio, discursos, cultos religiosos, aulas e palestras, bem como observações pessoais do mundo físico. De acordo com Boulding (1970, p. 15), a infosfera é um segmento essencial da sociosfera, ou seja, do ambiente social humano, e pode até reivindicar um domínio considerável sobre outros segmentos.

É importante perceber que a noção de redes informatizadas, baseadas em conceitos como internet e fluxo de dados, ainda eram, de certa forma, distantes da realidade da década de 1970. Para se ter ideia, conforme mapeado por Vianna (2014), em 1972, existiam 750 computadores no Brasil, e a busca por autonomia tecnológica no país estava se iniciando paulatinamente, com alguns indivíduos que se propunham a compreender as mudanças no porvir.

Basta lembrar que Alan Turing, em meados da década de 1930, contribuía definitivamente para o início da ciência computacional, inaugurando esse ramo científico e marcando seu lugar na história, ao resolver as primeiras grandes questões e pensar um conceito de computador universal, capaz de processar dados (SOMMARUGA; STRAHM; 2015).

Mesmo que se recorra a autores de ficção científica, é perceptível que a humanidade, até recentemente, não estava

preparada para a forma com que a revolução digital iria atingir a sociedade. Veja-se o exemplo de Isaac Asimov, que, convidado a "prever o futuro" (NEW YORK TIMES, 1964), e com todo seu brilhantismo e inventividade, imaginou maravilhas como aparelhos elétricos sem cabos, com baterias de grande duração — mas parecia se limitar a uma separação entre homem e máquina, físico e digital.

Dizer que as fronteiras entre o analógico e o digital estão se tornando imperceptíveis é, portanto, concluir que há, ao mesmo tempo, uma tendência de modificação do entendimento de posses, bens e objetos. Estamos modificando a nossa perspectiva quotidiana sobre a natureza última da realidade, ou seja, essa mudança de uma perspectiva materialista para uma perspectiva informativa, conforme descrita por Floridi (2013, p. 10), implica numa alteração fundamental na maneira como se concebe a realidade. Em vez de enfatizar a materialidade dos objetos e processos, dá-se ênfase à informação que contêm e representam.

Logo, eles são tipificados, no sentido de que uma instância de um objeto ("minha cópia de um arquivo de música") é tão boa quanto seu tipo ("seu arquivo de música do qual minha cópia é uma instância"). E eles são considerados, por padrão, perfeitamente clonáveis, no sentido de que minha cópia e o seu original se tornam indistinguíveis e, portanto, intercambiáveis (FLORIDI, 2013, p. 10). Esta é, portanto, a infosfera de Floridi — o ambiente híbrido e sem fronteiras, no qual a sociedade está mergulhando, que denota todo ambiente informacional constituído por todas as entidades informacionais e suas propriedades, interações, processos e relações mútuas.

O processamento dos dados e o apagamento paulatino das fronteiras entre o físico e o digital, conforme se percebeu, é um tema central para os autores relacionados ao tema. Nessa esteira, Schwab

entende tão logo que o grande desafio para a maioria das sociedades será saber como absorver e acomodar a nova modernidade e, ao mesmo tempo, abraçar os aspectos gratificantes de nossos sistemas tradicionais de valores (SCHWAB, 2016, p. 93).

Com isso, Zuboff (2019) novamente questiona: todos trabalharão para uma máquina inteligente, ou haverá pessoas inteligentes em torno da máquina? No mesmo raciocínio, desafios acerca da relação entre o humano e a máquina no que tange a tomada de decisões ganham destaque. Magrani (2019, p. 19) enfatiza uma mudança significativa na relação entre humanos e tecnologia, onde cada vez mais os algoritmos estão assumindo papéis anteriormente desempenhados por seres humanos. Essa transição está resultando em uma cultura emergente onde máquinas e dispositivos interconectados desempenham um papel central na tomada de decisões e na orientação de ações.

Tal fenômeno traz consigo uma série de considerações éticas importantes. À medida que os algoritmos se tornam mais prevalentes na sociedade e influenciam cada vez mais aspectos da vida humana, surgem questões sobre responsabilidade, transparência, justiça e autonomia. Por exemplo: quem é responsável quando um algoritmo toma uma decisão prejudicial? Como garantir que os algoritmos não reproduzam preconceitos e discriminações presentes na sociedade? Como podemos garantir que as decisões algorítmicas sejam transparentes e compreensíveis para os seres humanos afetados por elas?

Essas questões são especialmente importantes considerando os impactos cada vez maiores da comunicação e da decisão algorítmica na sociedade. Na medida em que se confia mais nas tecnologias computacionais para orientar ações e decisões, é essencial garantir

que sejam desenvolvidas e usadas de maneira ética e responsável. Essa ainda é uma cultura relativamente recente e implica considerações éticas importantes tendo em vista os impactos progressivamente maiores da comunicação e da decisão algorítmica/computacional na sociedade (MAGRANI, 2019, p. 19).

O embate real/virtual deu espaço para o desenvolvimento de inteligências artificiais, comandadas pelas fórmulas matemáticas dos algoritmos. Apesar de ser um conceito debatido e de diversas definições, um algoritmo também pode ser compreendido como uma sequência de etapas bem definidas para a solução abstrata de um problema. Trata-se de um conjunto de instruções finitas e encadeadas numa linguagem formal, executáveis num determinado tempo (SILVEIRA, 2019, p. 18).

Desde que se compreende a verdadeira magnitude das aplicabilidades das inteligências artificiais, é possível inferir que estas podem estar presentes em diversos setores da vida humana dado o crescimento exponencial do poder de computação, a disponibilidade de vastos conjuntos de dados devido às mídias sociais e o uso massivo de bilhões de smartphones e redes móveis de alta velocidade, a IA e, especialmente, o aprendizado de máquina, fizeram progressos significativos (COECKELBERGH, 2021).

Esse fato permitiu que os algoritmos assumissem muitas de nossas atividades, incluindo planejamento, fala, reconhecimento facial e tomada de decisões e tais aplicações de IA estão nos mais variados campos de aplicação, e dentre eles estão inclosos os atinentes as nossas relações afetivas. De acordo com Jordi Nieva Fenoll (2018), a inteligência artificial (IA) basicamente busca grandes quantidades de dados para estabelecer padrões estatísticos. E daí se sobressai que esta aplicação pode ser feita, além de tantas outras, para oferecer

produtos em redes sociais e sites, mas também para rastrear preferências dos usuários para influenciar sua opinião (inclusive, política).

Em todos esses casos, o que é estabelecido é um perfil, não somente de indivíduos, mas, sobretudo de grupos. O que se forma, neste caso, é um padrão de tendências que acaba, estatisticamente, muitas vezes, coincidindo com a realidade. Assim, as ferramentas de inteligência artificial passam a conhecer indivíduos e grupos. O que se percebe, de fato, é que o avanço da tecnologia tende a cada vez mais invadir a esfera subjetiva dos usuários da rede. Significa dizer que os dispositivos serão capazes de obter e interpretar as informações fornecidas pelos usuários e agregando essas informações pessoais, as plataformas poderão individualizar os resultados (MAGRANI, 2019, p. 53).

No contexto de recolhimento e utilização de dados pessoais, Giuliano da Empoli (2019), destaca, em *Engenheiros do Caos*, que as redes sociais podem ser manipuladas, tanto no sentido individual dos usuários como no sentido de massa. Em um excerto especifico, o autor destaca que Davide Casaleggio faz uma analogia entre as redes sociais e os formigueiros, sugerindo que ambos são sistemas auto-organizados onde os indivíduos seguem regras locais que resultam em uma estrutura globalmente organizada, mas não centralizada. Essa comparação destaca como as interações individuais entre os membros de uma rede social podem levar a padrões emergentes e comportamentos coletivos complexos. Como as formigas reagem ao contexto, ao espaço e às outras formigas ao seu redor, os usuários das redes respondem a estímulos em suas plataformas (Empoli, 2019, p. 31).

No entanto, Casaleggio também sugere que, apesar da auto-organização, ainda pode haver um papel para um observador externo

ou demiurgo. Esse demiurgo, assim como um observador do alto, poderia entender e, potencialmente, influenciar a evolução do sistema ao compreender as interações locais e os padrões emergentes (EMPOLI, 2019, p. 31). Essa visão implica que, embora as redes sociais sejam sistemas complexos e auto-organizados, ainda há espaço para intervenção externa com base na compreensão desses sistemas. Isso sugere a importância de uma abordagem informada e responsável ao gerenciar e interagir com redes sociais, reconhecendo tanto as dinâmicas emergentes quanto a possibilidade de influenciá-las de maneira ética e construtiva.

Assim, o que se percebe é que o uso da tecnologia algorítmica tem suscitado questionamentos e perpetrado violações a direitos fundamentais e Floridi (2013) explica esta cadeia de eventos que chega, em última instância, ao vilipêndio dos dados de uma pessoa para fins escusos, por terceiros. Ele observa que os dados utilizados para autenticação, como nomes, endereços, números de identificação (como números de Segurança Social), informações bancárias e números de cartões de crédito, são frequentemente tratados como meros rótulos associados ao indivíduo, sem terem uma conexão ontológica intrínseca com sua identidade.

Esses dados, embora úteis para autenticação e identificação, são destacáveis do indivíduo. Isso significa que, se forem comprometidos, roubados ou utilizados de forma ilegal, o indivíduo não é afetado em sua essência ou identidade intrínseca. No entanto, na infosfera, quanto menos fricção ontológica houver, ou seja, quanto mais fácil for o fluxo desses dados, mais vulneráveis eles se tornam a abusos. A facilidade de transferência e manipulação desses "rótulos" na infosfera aumenta o risco de roubo e uso ilegal dessas informações para diversos fins, como fraudes financeiras, roubo de identidade e

outros crimes cibernéticos (FLORIDI, 2013, p. 247).

Essa reflexão destaca a importância de abordagens robustas para proteger a identidade pessoal e os dados sensíveis na era digital, bem como a necessidade de considerar não apenas os aspectos técnicos da segurança cibernética, mas também as implicações éticas e sociais de como lidamos com esses dados na infosfera. Ainda, o "atrito ontológico" a que o autor se refere é, na realidade, o conjunto de barreiras colocadas ou a dificuldade encontrada para acesso aos dados. Na medida em que a infosfera vai turvando suas fronteiras entre físico e digital, cria-se um dilema entre proteger as informações e a manter o fluxo, que é cada vez mais difícil de ser controlado.

Na medida em que bens, produtos e informações são digitalizados e o seu fluxo se torna cada vez menos fisicamente tangível, passam a se enfrentar os desafios de proteção aos direitos que emergem destes institutos, uma vez que são traduzidos em dados, que são processados de forma cada vez mais rápida. Este tráfego de dados é o centro do nosso mundo digital (MONTY; WACKS, 2019).

3 O PARADOXO DA PRIVACIDADE NA INTERNET

A privacidade é um dos temas explorados por Luciano Floridi (2014), que por sua vez discute como a tecnologia, especialmente a internet e as redes sociais, impacta a privacidade e redefine as relações entre indivíduos, empresas e governos. Ainda, argumenta que a privacidade é crucial para a autonomia e a dignidade dos seres humanos e que a coleta constante de dados pessoais online, muitas vezes sem o consentimento explícito dos usuários, representa uma ameaça significativa a essa privacidade. Ele examina como nossas informações pessoais são coletadas, armazenadas, analisadas e

usadas por empresas e governos para diversos fins, incluindo publicidade direcionada, monitoramento de comportamento e até mesmo manipulação.

Autores como Cohen (2012) e Solove (2004) também contribuíram significativamente para o debate sobre privacidade na era digital. Eles argumentam que a coleta indiscriminada de dados pessoais pode levar a violações de privacidade e potenciais abusos de poder por parte das entidades que detêm esses dados. Quando a atenção é rentabilizada através da recolha constante de atividades e dados pessoais online, perdemos privacidade (COHEN, 2012; SOLOVE, 2004). Quando os Estados optam por monitorar os cidadãos na esfera online, perdemos privacidade. Quando a tecnologia não cumpre a sua promessa de anonimato, perdemos privacidade (OHM, 2009). Os escritos de Floridi (2014) podem fornecer reflexões importantes sobre o tema, ao desenvolver o questionamento: por que a privacidade importa? O que, afinal, é a privacidade após a quarta revolução?

Para Floridi, há dois tipos de interpretação sobre o valor da privacidade. A primeira, seria a interpretação reducionista que argumenta que o valor da privacidade assenta numa variedade de consequências indesejáveis que podem ser causadas pela sua violação e que também é uma utilidade no sentido de fornecer uma condição essencial de possibilidade de boas interações humanas, preservando a dignidade humana ou garantindo freios e contrapesos políticos, por exemplo (FLORIDI, 2014, tradução nossa).

A segunda interpretação baseia-se na propriedade e argumenta que a privacidade informacional precisa ser respeitada devido aos direitos de cada pessoa à segurança corporal e à propriedade, onde a "propriedade de x" é classicamente entendida como o direito ao uso exclusivo de x (FLORIDI, 2014, tradução nossa). De forma geral, ambas

interpretações propostas não são incompatíveis, mas demonstram diferentes aspectos do valor da privacidade. A primeira é mais orientada para as consequências em termos de custo-benefício para o indivíduo. Já a segunda é mais orientada para os direitos naturais, valorizando a privacidade em si, enquanto propriedade privada ou intelectual.

Conforme leciona Doneda (2020), a própria noção ou percepção de privacidade, em si, não é recente – com os diversos sentidos que apresenta, podendo ser identificada nas mais variadas épocas e sociedades. As definições clássicas tratam a privacidade tal como a "reivindicação de indivíduos, grupos ou instituições de determinar por si próprios quando, como e em que medida a informação sobre eles é comunicada a outros" (WESTIN, 1967, p. 07). Gavison (1980) por sua vez, procura separar características da privacidade, estabelecendo limites de acessibilidade: sigilo – informações conhecidas sobre um indivíduo; anonimato – atenção dada a um indivíduo; e solidão – acesso físico a um indivíduo.

Entretanto, Monty e Wacks (2019) argumentam que uma noção neutra de privacidade, como as apresentadas, rejeita os atributos das informações envolvidas. Significa que, nos termos apresentados, sempre haverá uma perda de privacidade quando qualquer informação sobre qualquer indivíduo se tornar conhecido, o que é uma extrapolação. Certamente algum fator limitante ou controlador está faltando na equação.

Ocorre que, claramente, os meios mais tradicionais de entender a privacidade já não se aplicam aos tempos contemporâneos, porque não levam em conta determinados problemas-chave introduzidos pela era digital (SOLOVE, 2004). Para exemplificar, Solove (2004) cita que o clássico "1984" jamais pensou no conceito de um dossiê digital sobre determinada pessoa, e nem poderia. Conforme já visto, as mentes

criativas da ficção, por mais inventivas que fossem, dificilmente poderiam prever este futuro com precisão.

Quando foram escritas obras fictícias como *1984*, de George Orwell (escrito em 1948) e *The Years* (escrito em 1936, onde a protagonista questiona se algum dia seria possível "ver coisas no fim do telefone"), de Virginia Woolf, as fundações da sociedade de informação que conhecemos estavam sendo construídas, de modo que seria difícil ter um completo senso da profundidade das transformações que viriam a partir daquele estágio de desenvolvimento (FLORIDI, 2014).

Estas ideias preliminares tiveram, então, que passar por uma evolução e que a moderna doutrina do direito à privacidade, cujo início podemos considerar como sendo o famoso artigo de Brandeis e Warren, *The right to privacy*, apresenta uma clara linha evolutiva. Em seus primórdios foi marcada por um individualismo exacerbado e portava a feição do direito a ser deixado só. A esse período remonta o paradigma da privacidade como uma zero-relationship, pelo qual representaria, no limite, a ausência de comunicação entre uma pessoa e as demais (DONEDA, 2020). Essa concepção foi de fato o marco inicial posteriormente lapidado por uma crescente consciência de que a privacidade seria um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade. Doneda (2020) ainda faz a ressalva de que a privacidade, mesmo hoje, apresenta alguns traços individualistas, próprios do contexto em que as primeiras ideias começaram a se formar, notadamente na segunda metade do século XIX, em claro apego ao liberalismo jurídico clássico.

No entanto, este substrato individualista que era marcado pela forma com que a privacidade era vista sob a ótica de que as pessoas conhecidas ou famosas deveriam ser deixadas em paz aos poucos se

modificou juntamente com a migração do Estado Liberal para o *welfare state*. A mudança do relacionamento entre cidadão e Estado, uma demanda mais generalizada de direitos como consequência dos movimentos sociais e das reivindicações da classe trabalhadora. Na medida em que a tecnologia avança, a capacidade técnica de coletar, processar e utilizar informações cresce exponencialmente. Isso tem implicações significativas para a privacidade e os direitos individuais dos cidadãos.

Enquanto originalmente a preocupação residia na simples revelação pública de fatos privados, as características contemporâneas levam a concluir que há preocupações com o mal-uso e o armazenamento de dados digitalizados (MONTY; WACKS, 2019). O que se deve levar em consideração é que, com tanta informação disponível no ambiente digital, nem tudo é considerado dado pessoal. Porém, é necessário estabelecer que um arquivo médico anônimo, um extrato bancário ou revelações chocantes de um caso sexual são inócuos até serem vinculados a um indivíduo identificado. Uma vez exposta a identidade do titular da informação, ela se torna pessoal (MONTY; WACKS, 2019).

Dados são considerados identificáveis quando estão associados a uma pessoa, mesmo que não haja uma conexão direta no momento. Essa associação pode ser indireta, como no caso de um endereço IP, que não identifica diretamente uma pessoa, mas pode ser vinculado a ela através dos registros do provedor de serviços de Internet. Essa definição é relevante para compreender como a privacidade pode ser afetada pela coleta e uso de dados (SOLOVE 2023, p. 06). Então, percebe-se que, embora a forma através da qual o ser humano percebe a privacidade e seu valor possa ter se modificado ao longo dos últimos anos, é inegável que este valor ainda existe, uma vez que

sua tutela é tão estudada por autores contemporâneos.

Considerados estes fatores, os usuários de qualquer site ou rede social acabam fornecendo dados aos operadores destas ferramentas. Assim, tem-se uma via de mão dupla na relação entre o recolhimento e a entrega de informações. Insere-se o consentimento do usuário para o tratamento de seus dados pessoais que é um dos pontos mais sensíveis de toda a disciplina de proteção de dados pessoais; por meio dele, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão (DONEDA, 2020).

O consentimento, no tocante a direitos da personalidade, assume hoje um caráter bastante específico visto que várias configurações possíveis, referentes tanto à privacidade como à imagem, identidade pessoal, disposições sobre o próprio corpo e outras, dependem em alguma medida de uma manifestação da autonomia privada (DONEDA, 2020). Em outras palavras, o consentimento representa a expressão da liberdade pessoal em relação ao uso de dados pessoais, servindo como meio para expressar a decisão individual, enquanto se respeitam os valores essenciais em jogo.

Conforme Luger, Moran e Rodden (2013), a capacidade de gerir as informações fornecidas aos sites e redes sociais no momento do consentimento é o principal meio pelo qual o usuário é capaz de proteger tanto a sua privacidade quanto sua identidade. Este perceptível ponto-chave (consentimento), entretanto, apresenta uma incoerência: apesar de as pessoas darem valor aos seus dados pessoais, suas condutas são dissonantes em relação a tal valoração: "suas condutas contradizem o que elas estimam, surgindo-se uma

relação de incoerência entre o que elas praticam e o que elas enxergam como ideal (KERR *ET AL*. IN BIONI, 2019)."

Daí surge o denominado paradoxo da privacidade, referenciado por Rossoglou (2015), que nada mais é do que uma face de hipossuficiência do cidadão: "ele está em uma situação de vulnerabilidade específica em meio a uma relação assimétrica que salta aos olhos, havendo uma série de evidências empíricas a esse respeito (BIONI, 2019)." Existe um dilema: uma vez sendo as informações compartilhadas voluntariamente, é perdido o controle sobre seu uso por outrem. E, para Sharma (2020, p. 04) duas questões permanecem sem resposta: será que é realmente perceptível o ponto até o qual os dados pessoais são monitorados? Que nível de controle e direitos se tem sobre informações pessoais geradas por meio de atividades e divulgadas involuntariamente?

Esta falta de percepção que parece ser inversamente proporcional à quantidade de dados que disponibilizamos nos ambientes online é o que cria este grande enigma. Bauman (2001), que apresenta a noção de modernidade líquida, compreende que no mundo líquido-moderno a solidez dos vínculos humanos é vista como uma ameaça, ou seja, qualquer qualquer compromisso a longo prazo prenuncia um futuro de obrigações que limitam a liberdade de movimento e a capacidade de perceber novas oportunidade (ainda desconhecidas) assim que (inevitavelmente) elas se apresentarem (BAUMAN, 2010, p. 40-41).

Há uma crise atual na privacidade que se liga ao enfraquecimento, desintegração e decadência das relações humanas em si (BAUMAN, 2011). A facilidade do acesso e do uso de redes sociais e outras formas de interação virtuais faz com que a maioria dos usuários não leia os próprios termos de uso das ferramentas (Barbosa, 2014). Este

desleixo é ligado a fatores tais como a falta de interesse em ler termos muito longos e repetitivos, elaborados de forma unilateral pela plataforma (LIMA, 2014). Ainda, ao se deparar com os termos, o usuário não possui pleno conhecimento do que está contratando, simplesmente concordando (BAGGIO, 2012). Bioni (2019) exemplifica um estudo capaz de colocar em xeque a noção de consumidores como sujeitos sequer capazes de controlar suas informações pessoais.

Ainda, argumenta-se que há uma banalidade gerada pelas facilidades das ferramentas virtuais e que numa vida de contínuas emergências, as relações virtuais derrotam facilmente a "vida real" e as relações virtuais contam com teclas de "excluir" e "remover spams" que protegem contra as consequências inconvenientes (e principalmente consumidoras de tempo) da interação mais profunda (BAUMAN, 2011).

Embora apresente um contraste entre virtual e real, ideia já superada por Floridi (1999), que definiu o ambiente em que vive o ser humano contemporâneo como a infosfera, Bauman (2011) é lúcido ao trabalhar questões que envolvem a efemeridade das relações humanas num novo ambiente híbrido. O ambiente virtual multiplica infinitamente as possibilidades, enfraquecendo laços e tornando as relações mais efêmeras ou superficiais.

Mas as múltiplas opções de acesso e possibilidades não se limitam a relações puramente interpessoais. Exponencialmente dissipadas as fronteiras entre o virtual e o real na infosfera, governos também utilizam das ferramentas tecnológicas para fornecer serviços: no Brasil já há uma miríade de facilidades, tais como solicitação de benefícios previdenciários, serviços de saúde, tributários, trabalhistas, de trânsito, acesso a dados educacionais (ENEM, SISU, PROUNI, etc.). Ao total, o Portal do Governo oferece 4220 serviços, a grande maioria

realizados de forma totalmente digital (BRASIL, 2023). Tais números evidenciam que, na realidade, sequer há opção ao cidadão a não ser entrar em um conflito entre privacidade e acesso aos serviços: ou fornece-se os dados ao Poder Público, ou não se acessa os serviços prestados pelo Estado. Por isso, há um paradoxo entre a importância do consentimento no fornecimento de dados a terceiros nos ambientes digitais e a facilidade com que as pessoas entregam tais dados para estabelecer suas relações.

A já explorada efemeridade das relações humanas tratadas na modernidade líquida em contraponto com a importância do direito à privacidade guarda relação direta com o que Floridi (2014, p. 103) chama de "atrito informacional", que por sua vez refere-se às forças que se opõem ao fluxo de informações dentro de uma região da infosfera e está diretamente relacionado com a quantidade de esforço necessário para algum agente obter, filtrar ou bloquear informações sobre outros agentes. Qualquer aumento ou diminuição no chamado atrito informacional afetará, necessariamente, a privacidade, e isso pode ser percebido através das novas TICs, nas quais a facilidade para obtenção das informações está tanto do lado do usuário (a um clique de distância) quanto do fornecedor (a um "aceito os termos" de distância). Percebe-se, então, pelos pontos de vista abordados, que o paradoxo da privacidade é multifacetado e pode ser analisado de determinados pressupostos: ou não há consciência, ou não se dá importância, ou não há sequer opção de negar acesso.

A conclusão, de qualquer modo, deve ser no sentido de que as pessoas não conseguem autogerir seus dados, e que a privacidade na infosfera merece salvaguarda legal no tocante aos dados pessoais, seu uso, tratamento, armazenamento e acesso. Sharma (2020) chega a esta conclusão em sua análise do enigma da informação voluntária:

são necessários um rigoroso sistema de regulação e mecanismos de gestão da informação pessoal, independentemente da voluntariedade com a qual os dados são fornecidos.

Neste mesmo caminho apresenta-se uma visão crítica da regulação legal, dizendo que, para ser efetiva, a lei sobre privacidade deve se focar no uso, nos danos e nos riscos, e não meramente na natureza do que sejam "dados pessoais". Todas as leis de privacidade definem o tipo de dados pessoais que abrangem, mas em contrapartida não podem abranger todos os dados, caso contrário seriam ilimitadas, pelo que limitam o âmbito dos dados que abrangem aos dados relativos às pessoas (SOLOVE, 2023, p. 06). Assim, quase todas as leis de privacidade são acionadas com base numa definição de dados pessoais. Com isso, na sequência será estudada a tutela jurídica dos dados pessoais e compreendidos os principais marcos regulatórios de proteção aos dados pessoais como direito humano e fundamental no Brasil.

4 TUTELA JURÍDICA DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Há pelo menos cinco décadas, ainda que timidamente, iniciou-se a construção da disciplina da proteção de dados pessoais. Para continuidade da análise proposta neste estudo, a tutela jurídica do direito à proteção de dados será investigada visando formar uma compreensão dos principais conceitos que são abrangidos por duas notáveis legislações relacionadas à proteção de dados, que são o Regulamento Geral sobre Proteção de Dados (RGPD) europeu e a Lei Geral de Proteção de Dados (LGPD) brasileira. Partindo-se das raízes na tradição ligada ao direito à privacidade, a proteção de dados pessoais passou a se estruturar de forma mais autônoma conforme o o

processamento de dados passou a representar, por si só, um fator de risco para o indivíduo (BIONI *ET AL.*, 2021).

Antes desse marco temporal, há exemplos de regulação do direito à privacidade no Artigo 12 da Declaração Universal de Direitos Humanos da Organização Nacional das Nações Unidas (ONU, 1948), que estabelece que "ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

A Alemanha figura como pioneira na regulação específica da matéria de proteção de dados, após debates no contexto já mencionado, onde se dava início ao descolamento da proteção de dados, passando de aspecto da privacidade a direito autônomo. A Lei de Proteção de Dados do *Land* alemão de Hesse, de 1970, é identificada como o primeiro diploma normativo que trata especificamente dessa matéria, e debates que tiveram lugar na segunda metade da década de 1960 foram extremamente ricos e fundamentais para definir o perfil dessa disciplina que hoje está presente em mais de 140 países (BIONI ET AL., 2021). Este ato pode ser considerado o embrião para que em diversas outras legislações europeias passassem a debater e positivar tal direito: também na década de 1970, Portugal e Espanha, recém-saídos de ditaduras e contando com novas Constituições (1976 e 1978, respectivamente), fizeram com que nelas fossem inseridas normas relacionando privacidade e informática (DONEDA, 2020). Essas Constituições consideradas como "jovens" inauguram, no jusfundamental, a preocupação com a informática na Europa (LIMBERGER, 2016).

A primeira previsão constitucional, em Portugal, datada da Constituição de 1976, garantia a proibição da criação de cadastros

únicos dos cidadãos, evitando assim com que tais compilações de dados se transformassem em um instrumento de vigilantismo e controle estatal sobre as pessoas (DONEDA, 2020). Em seu artigo 35, no que tange à utilização da informática: I - todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir sua retificação e atualização; II- a informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos; e, III - é proibida a atribuição de um número nacional único aos cidadãos (PORTUGAL, 1976).

A preocupação com a centralização de informações e tratamento de dados pelo governo, entretanto, não era característica exclusiva dos portugueses. O Brasil possui um caso ilustrativo que pode colaborar para a compreensão do contexto, que é o projeto RENAPE - Registro Nacional de Pessoas Naturais –, uma tentativa frustrada dos governos militares durante os anos 1970 de criar uma grande base de dados cadastrais informatizada e unificada dos cidadãos brasileiros (VIANNA, 2014). Mas houve intensa mobilização e fortes críticas contra este projeto governamental, de acordo com os relatos da época. Além do caráter confidencial do projeto, o ambiente de repressão do governo Costa e Silva e Médici contribuíram para que ele não recebesse debate público (VIANNA, 2014, p. 1462). A iniciativa também naufragou por limitações técnicas dos computadores da época, mas é possível perceber, que a intensa preocupação com a manipulação dos dados também era tendência na sociedade brasileira.

De volta à Alemanha, em 1978, o *Bundesdatenschutzgesetz* estabeleceu os princípios da proteção de dados e estabeleceu os direitos e responsabilidades dos controladores e processadores de

dados. Também criou o Comissário Federal para a Proteção de Dados, responsável pela aplicação da lei (ALEMANHA, 2023).

Em 1983, a Corte Federal Constitucional Alemã chegou a uma decisão fundamental sobre o Censo, que apresentou um veredito considerado como um marco na proteção de dados (INTERNATIONAL NETWORK OF PRIVACY LAW PROFESSIONALS, 2018). A primeira e segunda conclusões compreende que esse direito fundamental confere ao indivíduo a autoridade para, em princípio, decidir ele próprio sobre a divulgação e utilização dos seus dados pessoais.

Entretanto, o tema recebeu efetivo tratamento do ponto de vista comunitário europeu em meados da década de 1990. Em 1995 surge o documento que veio efetivamente a padronizar a proteção de dados pessoais no espaço da União Europeia: a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (DONEDA, 2020). Tal diretiva foi mais abrangente que a Convenção de Strasbourg, pois exigia que os legisladores dos estados-membros adotassem leis de acordo com seu conteúdo normativo, que era bastante definido e detalhado em grande parte e foi adotada após quatro anos de rodadas de negociações entre os países membros (HUSTNIX, 2013, p. 09)

Na época de sua publicação, as leis nacionais de proteção de dados na Europa ofereciam níveis consideravelmente diferentes de proteção, deixando de prover segurança jurídica aos indivíduos e, também, aos que controlavam informações e as processavam (VOIGT; VON DEM BUSSCHE, 2017). Assim, a diretiva ajudou a unificar as leis europeias sobre privacidade de dados em toda a União, mantendo as regras básicas de processamento em vigor até surgir a necessidade do RGPD (SHARMA, 2020, p. 33). Entretanto Voigt e von dem Bussche (2017,

p. 02) observam que as diretivas europeias não são diretamente aplicáveis em todos os Estados-Membros da UE e têm de ser transpostas para a legislação nacional. Assim, exigem medidas de implementação em cada Estado-Membro da UE.

Com isso, a Diretiva Proteção de Dados não cumpriu os seus objetivos e não conseguiu alinhar o nível de proteção de dados na UE uma vez que as diferenças jurídicas surgiram em consequência dos atos de execução adotados pelos vários Estados-Membros da UE (VOIGT; VON DEM BUSSCHE, 2017, p. 02). Ainda, as atividades de tratamento de dados permitidas num Estado-Membro da UE podem ser ilegais noutro no que diz respeito à execução específica do tratamento de dados.

Logo, percebe-se que seria previsível que a legislação não acompanharia o passo da evolução tecnológica, o que acabaria culminando em uma defasagem rápida das ideias firmadas nos anos 1990. Surge, assim, a necessidade, na Europa, de um novo ordenamento unificador, de onde nasceu a *GDPR – General Data Protection Regulation*, ou o RGPD – Regulamento Geral sobre Proteção de Dados. O Regulamento Geral sobre Proteção de Dados europeu, que vigora desde 2016 (UNIÃO EUROPEIA, 2016) em contraste com a Diretiva de Proteção de Dados de 1995, é aplicado diretamente aos destinatários, eliminando a necessidade de outras medidas e de implementação pelos Estados-membros. Ou seja, tratou-se de equalizar as regras para proteção de dados na Europa, o que deve conduzir a uma maior segurança jurídica e tende a eliminar potenciais obstáculos ao fluxo de dados pessoais (VOIGT; VON DEM BUSSCHE, 2017).

Logo no seu artigo 2º (UNIÃO EUROPEIA, 2016), o RGPD estabelece seu âmbito de aplicação material: "o presente

regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados" (UNIÃO EUROPEIA, 2016). Neste sentido, qualquer negócio que colete informação pessoal de qualquer tipo, mesmo que limitado aos empregados, está sujeito ao RGPD. Especificamente, para ser alvo na regulação um negócio precisa processar dados pessoais, total ou parcialmente, por meios automatizados ou não, e armazená-los ou pretender armazenar em algum tipo de sistema (SHARMA, 2020).

Estas regulações levam a concluir que as entidades ou organizações precisam realizar esforços consideráveis em termos de adequação ao RGPD, incluindo processos internos, criação de posições de emprego e mudança de condutas. O controlador dos dados precisa implementar políticas de proteção de dados proporcionais às atividades de processamento, no que pode ser chamado de uma proteção baseada no risco (VOIGT; VON DEM BUSSCHE, 2017).

Já seu artigo 4º, o RGPD trabalha definições de "dados pessoais", "processamento", "consentimento", entre vários outros. Sobre o tema, inclusive, Solove (2023) enuncia que as leis precisam definir aquilo que pretendem regular. O RGPD, assim, define dados pessoais como informações relativas a uma pessoa singular identificada ou identificável ('titular dos dados'). É considerada identificável

> uma pessoa singular que possa ser identificada, direta ou indiretamente com um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular" (União Europeia, 2016).

Da mesma forma, a ideia de Solove (2023, p. 07) parece

encontrar eco na definição trazida pelo RGPD, uma vez que o autor entende que a análise de dados moderna, é relativamente fácil direcionar e identificar pessoas com base em dados que não estão diretamente vinculados a uma pessoa. Através desta ideia, compreende-se que bastaria a possibilidade de identificação de uma pessoa, mesmo que através de uma informação aparentemente não relacionada, para que se aplique o RGPD. Esta preocupação, então, se mostra válida, uma vez que os dados podem ser usados de forma combinada, ou seja, não se trata necessariamente de um "crachá" com o nome da pessoa, mas pode ser até mesmo um quebra-cabeça de informações, montado com peças aparentemente não relacionadas (Sharma, 2020).

Nesse sentido, para que seja aplicado o RGPD, os dados precisam ser pessoais, ou seja, relacionados, nas formas investigadas, a qualquer indivíduo identificado ou identificável (VOIGT; VON DEM BUSSCHE, 2017). Dados anônimos ou puramente estatísticos podem ser trabalhados sem as vinculações do RGPD. Outro aspecto que merece ser tratado diz respeito ao consentimento. Isto porque "As atividades de tratamento de dados só podem ser lícitas se estiverem abrangidas pelo consentimento do titular dos dados ou por autorização legal" (VOIGT; VON DEM BUSSCHE, 2017, p. 92).

O RGPD também trabalha o conceito de "consentimento" do usuário, que por sua vez significa qualquer indicação dada livremente, específica, informada e inequívoca dos desejos do titular dos dados, pela qual ele ou ela, por uma declaração ou por uma ação afirmativa clara, expressa acordo com o tratamento de dados pessoais que lhe digam respeito (UNIÃO EUROPEIA, 2016). Esta conceituação legal, que guarda relação com a definição já trabalhada através de Doneda (2020) em momento anterior, implica que o consentimento implícito ou uma

autorização generalizada não é suficiente (VOIGT; VON DEM BUSSCHE, 2017).

As condições aplicáveis ao consentimento previsto no RGPD são encontradas no artigo 7ª do Regulamento com ênfase ao inciso terceiro que enuncia que o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento e que essa retirada do consentimento não compromete a licitude do tratamento efetuado e que o consentimento deve ser tão fácil de retirar quanto de dar (UNIÃO EUROPEIA, 2016).

Esse aspecto da lei trabalhado dialoga com a ideia anteriormente apresentada sobre o grande volume e difícil controle do fluxo de dados nos ambientes virtuais. Uma vez que dados pessoais foram lançados em um sistema que processa e realiza tratamento, interpretação e até mesmo capitalização, esta ação não pode e nem deve, de acordo com a legislação, ser desfeita. É digno, ainda, de nota, na seção do RGPD que trata sobre a retirada do consentimento, que o operador ou controlador dos dados deve informar ao sujeito que fornece os dados sobre seu direito de retirada. Violar esse dever é punível com multa e esta retirada deve ser tão facilitada quanto o fornecimento (UNIÃO EUROPEIA, 2016).

Bioni (2019) valoriza de forma especial a minúcia com que é tratada a descrição das condições do consentimento, destacando o consentimento nas legislações europeias tem tido destaque desde o início da trajetória das leis de proteção de dados (BIONI, 2019). Embora haja um conjunto de proteção legal que salvaguarda o consentimento como fundamental de proteção à privacidade, o paradoxo da privacidade, exposto anteriormente, continua a ser tema de relevância, pois se manifesta também filosoficamente, traduzido nas óticas da modernidade líquida (BAUMAN) e da infosfera (FLORIDI).

Fica claro, pela análise até aqui procedida que, no que se refere aos pontos principais elencados para estudo, o RGPD é uma tentativa de atualizar e corrigir lacunas de legislações anteriores sobre o tema de proteção de dados. Nasceu da percepção de que as transformações sociais ultrapassaram a inovação legislativa da forma com que a sociedade europeia convivia desde os anos 1970. Algo parecido se verá no caso brasileiro, cuja legislação atual sobre o tema é baseada no diploma europeu.

Na esfera legislativa brasileira esse direito está positivado constitucionalmente após a aprovação da Emenda Constitucional 115, de 2022 (BRASIL, 1988), tendo inserido o inciso LXXIX no seu artigo 5º, assegurando, nos temos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Ocorre que, do ponto de vista do direito interno, o direito à proteção de dados foi considerado, por muitos anos, para a doutrina e jurisprudência, como implicitamente positivado na Constituição Federal. Neste ponto, cita-se o art. 5º da CF/88, incisos XII e LXXII, os quais tratam, respectivamente da inviolabilidade do sigilo de correspondências e do *habeas data* (BRASIL, 1988).

A elevação do direito à proteção de dados pessoais ao nível de positivação constitucional, explicitamente, no Brasil, é tão recente que diversos escritos sobre o tema ainda o trazem como apenas implicitamente positivado, derivado de outros princípios fundamentais. Estas definições, entretanto, são úteis e válidas para ilustrar como a doutrina jurídica foi percebendo a necessidade de positivação.

Sarlet (2020, p. 183) entende que no caso brasileiro, embora se faça referência, no art. 5º, XII, CF ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas), não se contempla expressamente um direito fundamental à proteção e livre disposição dos dados pelo seu

respectivo titular, sendo o reconhecimento de tal direito algo ainda relativamente recente na ordem jurídica brasileira.

Possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade (SARLET, 2020, p. 185). Este, por sua vez, assume a condição de cláusula geral de proteção de todas as dimensões da personalidade humana, conceito considerado disposição geral que protege todas as facetas da individualidade humana. Ele se baseia em uma tradição jurídica estabelecida no direito constitucional estrangeiro de direitos humanos e abrange, entre outros direitos, o direito à livre gestão dos dados pessoais, também conhecido como direito à autodeterminação informativa.

O que se observa é que, mesmo tendo sido elevado à condição jusfundamental, esse direito não pode, jamais, ser analisado de forma isolada, pois logicamente decorre de uma série de outros corolários a ele relacionados, e que conferem ao tema ainda maior complexidade e importância. No tocante ao tema, nunca é demais destacar o que sejam, ainda que de forma breve, os direitos fundamentais.

Ainda que breves e incipientes, tais definições doutrinárias bastam para contextualizar o que se deseja transmitir quando o presente trabalho cita a fundamentalidade dos direitos e sobretudo do direito à proteção de dados, seja ele tratado de forma autônoma ou decorrente de outros direitos fundamentais. Sobre tais princípios Bioni (2021, p. 194) elenca um rol dos direitos fundamentais correlatos ao direito à proteção de dados, quais sejam: I- a finalidade; II - a adequação; III- a necessidade; IV- o livre acesso; V- a qualidade dos dados; VI - a transparência; VII- a segurança; e, VIII - a prevenção e a não discriminação, permeadas pelo princípio da boa-fé. Com isso,

pode-se entender a constelação principiológica da LGPD, fundada nos princípios constitucionais, e amparada em instrumentos jurídicos previstos em outras searas, para além do direito digital, como a civil, a penal e a consumerista.

As relações entre o princípio da dignidade da pessoa humana e o direito fundamental à proteção dos dados pessoais são estreitas, embora interpretáveis diversamente nas mais diferentes ordens jurídicas. As principais conexões são o princípio da autonomia (autodeterminação) e os direitos de personalidade. Estes incluem o direito geral ao livre desenvolvimento da personalidade e os direitos específicos à privacidade e à autodeterminação informativa, os quais estão interligados, embora não sejam os únicos. Apesar de nem todos os direitos fundamentais terem sua base na dignidade humana, no caso do direito à proteção dos dados pessoais a dignidade humana deve ser invocada para justificar a importância desse direito e determinar seu conteúdo, destacando sua relação com outros princípios e direitos fundamentais (BIONI *ET AL.*, 2021, p. 49).

No tocante ao direito à personalidade, é necessário fazer a ressalva de que embora a proteção de dados tenha sido associada, em diversos casos, à privacidade, o fato é que o objeto (âmbito de proteção) do direito à proteção de dados pessoais é mais amplo, porquanto, com base num conceito ampliado de informação, abarca todos os dados respectivos a uma determinada pessoa natural, sendo irrelevante a esfera da vida pessoal à qual se referem, descabida qualquer tentativa de delimitação temática. Isso significa dizer que a doutrina considera que o direito à proteção de dados avança para além da simples tutela da privacidade, não se tratando de mera evolução da privacidade. Daí se conclui que o ordenamento jurídico brasileiro amadureceu a ideia de necessidade de proteção de dados

pessoais, até há pouco considerada direito implícito, se torna autônomo e expresso.

Então, uma vez que resta fundamentalmente compreendida a importância da proteção de dados para o ordenamento jurídico brasileiro, se faz necessária a exploração do principal diploma legal sobre o tema, que é a Lei Geral de Proteção de Dados (BRASIL, 2018). Além da Constituição Federal (BRASIL, 1988), antes do advento da LGPD, ainda que de forma esparsa, o Código Civil, o Código de Processo Penal e o Marco Civil da Internet já traziam previsões sobre proteção de dados (KOHLS; DUTRA; WELTER, 2021).

Quanto ao Marco Civil da Internet (MCI), embora sua redação inicial tenha enfatizado que seus principais princípios eram privacidade, proteção dos dados pessoais, liberdade de expressão e neutralidade de rede, ele foi promulgado em resposta às violações de privacidade e dados pessoais. O artigo 7º, que originalmente tinha cinco incisos, passou a ter oito, e a noção de "autodeterminação informacional" foi introduzida, agora expressamente incluída no artigo 2º, II, da Lei Geral de Proteção de Dados (LGPD).

As análises da formulação do Marco Civil da Internet constataram que houve, de certa forma, uma participação colaborativa da sociedade no processo legislativo (Goulart; Silva, 2015). Ferramentas de consulta popular sobre o tema deram publicidade ao assunto de forma que fosse compreensível para o maior número de cidadãos possível (NICOLÁS *ET AL.*, 2017). Isso reforça a necessidade de a lei acompanhar a dinâmica da sociedade.

Ao tratar do tema, diante da ausência de uma lei específica na época, o Marco Civil da Internet observou princípios consagrados pela doutrina de proteção de dados pessoais, enfatizando os critérios de finalidade, pertinência e não abusividade da utilização das

informações coletadas (TEFFÉ; MORAES, 2017). Entretanto, a iniciativa não é livre de críticas, e a expectativa criada com a discussão dessa lei deu-se pela crença errônea de que as normas contidas na Constituição Federal, no Código Civil, no Código Penal, nos Códigos de Processo Civil e Penal, no Código de Defesa do Consumidor, no Estatuto da Criança e do Adolescente e na lei sobre interceptação de comunicações (Lei n. 9.296/96) não teriam aplicação nas relações jurídicas estabelecidas na internet (TOMASEVICIUS FILHO, 2016). Em relação a essa percepção, a crítica toca na ideia ultrapassada de separação entre virtual e físico. Entretanto, o autor chega a propor que a tal inutilidade do Marco Civil poderia ser mitigada com a adoção de normas internacionais, solução que desde o século XIX tem sido útil para a proteção de marcas e obras artísticas e literárias na Europa.

Aparentemente anacrônica, a solução do autor guarda relação com a noção de ausência de fronteiras no mundo digital, mas esbarra em uma contradição: considera que as relações jurídicas na internet têm o mesmo valor do que as do "mundo físico". Assim, não basta simplesmente celebrar acordos internacionais para dar força a regramentos no âmbito do direito interno. Adiante, firmando-se na importância de uma legislação local abrangente e bem definida, a edição da LGPD se tornou improtelável com a eficácia do RGPD, que serviria de base para muitos artigos da lei brasileira (KOHLS; DUTRA; WELTER, 2021).

A lei brasileira mostra forte influência do regulamento europeu ao adotar abordagem ampla sobre o tema, garantindo direitos fundamentais aos titulares dos dados e estabelecendo uma autoridade reguladora independente. Além disso, tanto na estratégia quanto nos mecanismos regulatórios de ambas as normas, observa-se uma abordagem similar, responsiva e baseada em uma governança

nodal — que visa garantir a implementação, aplicação e fiscalização mais eficazes das leis por parte das autoridades reguladoras. Deve-se salientar que não basta, entretanto, a "importação descontextualizada e acrítica das normas europeias de proteção de dados (DANTAS BISNETO, 2020, p. 24)". A LGPD, para ser efetiva, não pode se limitar à tradução da normativa europeia, visto que a construção das legislações, conforme já analisado, se deu por caminhos diferentes.

O artigo 1° da LGPD (BRASIL, 2018) merece especial destaque por dispor sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, de direito público ou privado. É interessante, portanto, a compreensão do ambiente híbrido da infosfera, ou seja, as legislações modernas estão percebendo que o ambiente *online* e *offline* se fundem em um novo espaço altamente conectado. Além de trazer proteção à liberdade e privacidade no primeiro artigo do texto (BRASIL, 2018), a LGPD redunda no assunto em seu artigo 2º, que elenca fundamentos da proteção de dados pessoais (Brasil, 2018), destacando: respeito à privacidade, autodeterminação informativa, liberdade de expressão, informação, comunicação e opinião; inviolabilidade da intimidade, honra e imagem, entre outros. Essa preocupação do legislador em balizar direitos fundamentais abrangidos pela disciplina da matéria é traduz o caminho que a proteção de dados pessoais percorreu no ordenamento jurídico brasileiro.

Em artigos seguintes, a LGPD traz definições dos conceitos utilizados ao longo do texto. Em seu artigo 5° a LGPD traz definições importantes de dados pessoais e consentimento. Dado pessoal, conforme a lei, é a informação relacionada a pessoa natural identificada ou identificável, e o consentimento diz respeito à

manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados (BRASIL, 2018). Destacam-se essas previsões de conceitos de dados pessoais e consentimento, muito conectadas e semelhantes aos conceitos europeus. Em verdade, isso é previsível, uma vez que já resta evidente a inspiração brasileira no RGPD. Há uma lógica na construção das legislações, que acompanha um caminho de tomada de consciência, pela sociedade, das mudanças que a era digital provocou na forma com que devem ser tutelados os institutos das liberdades individuais, sobretudo a privacidade, como era tratada inicialmente.

A evolução das legislações, que datam desde os primórdios dos anos de 1970, com incipiente desenvolvimento dos conceitos e das infraestruturas de redes e dados digitais, foi um caminho necessário de resposta do direito ao contexto tecnológico que se modificou de maneira rápida e irreversível. A proteção de dados é, em verdade, matéria multidisciplinar e guarda relação direta com outros direitos fundamentais.

5 CONSIDERAÇÕES FINAIS

O presente artigo objetivou em linhas gerais investigar o instituto da proteção de dados pessoais no contexto da era digital e de que forma as violações à privacidade e a má utilização de dados pessoais ferem a esfera íntima da pessoa e de qual forma são tuteladas juridicamente no Brasil emergindo assim como um direito autônomo. Em relação ao primeiro objetivo específicos, destacou-se durante a condução do estudo, a assertividade do olhar de Luciano Floridi e do seu conceito de infosfera. O ser humano não pode mais dissociar nenhuma atividade cotidiana do uso da tecnologia e a diferença entre os ambientes digital

e físico aos poucos restará dissipada. Esta conclusão é, inclusive, corroborada pela forma pela qual se conduziu o estudo do fenômeno no que diz respeito ao aspecto de digressão histórica dos princípios estudados.

Em relação ao segundo objetivo especifico, temos que para entendermos como a proteção de dados pessoais passou de um aspecto integrante do direito fundamental à privacidade para um direito autônomo precisamos compreender que a humanidade atravessa um período de avanço tecnológico capaz de formar por uma nova realidade em que não há separação entre real e virtual, ou seja, a forma como a humanidade percebe a sua realidade mudou de forma irreversível e o ser humano, que agora vive na infosfera, não pode deixar de considerar seus dados como um bem fundamental. Esta conclusão perpassa pela compreensão do valor do instituto da privacidade, de como o ataque aos direitos fundamentais a ela correlatos fere a esfera íntima do indivíduo, ressaltando a necessidade pujante de tutela ao direito fundamental à proteção de dados, que deve ser considerado como um direito autônomo.

Quanto ao terceiro objetivo específico temos que além de uma digressão histórica, um apanhado dos aparatos legislativos sobre o tema foi analisado e discutido, reforçando a conclusão quanto sua relevância como direito autônomo consolidado no rol de direitos fundamentais e que sua regulação no Brasil sofreu forte influência da legislação da União Europeia sendo hoje representada principalmente pelo advento da LGPD em que pese ainda careça de esforços legislativos. A hipótese formulada para guiar os estudos mostra-se confirmada ao fim dos esforços até aqui empreendidos, pois a compreensão dos principais aspectos que envolvem os direitos à proteção de dados foi satisfeita na mesma medida em que resta claro, por todo o exposto, que os dados

pessoais são amplamente instrumentalizados pelos seus detentores e manipuladores, sejam eles órgãos governamentais ou companhias privadas.

Possível concluirmos também que nas origens do direito à proteção de dados, o mesmo é apresentado como derivação do princípio da proteção à privacidade, ou seja, a noção de que indivíduos determinados ou determinados possuem informações que, se não protegidas, podem revelar de forma indesejada algum aspecto objetivo ou subjetivo que invadem a seara pessoal. Logicamente, o advento da era da informação, com a crescente informatização e avanço significativo da tecnologia, tornou o debate sobre a proteção de dados ainda mais relevante na sociedade moderna.

O fato de os cidadãos viverem conectados à internet e aos sistemas potencializou a oferta dos dados para governos e empresas privadas, tornando os dados pessoais poderosas ferramentas sociais ou comerciais e de valor econômico inestimável para diversas atividades mercadológicas. Daí se conclui a grande importância e relevância da regulação das atividades que envolvam armazenamento, tratamento e divulgação de dados pessoais, tendo em vista a ampla gama de violações a direitos que podem ocorrer quando, sem consentimento do titular, dados caem na posse de terceiros.

Por fim, o presente artigo não visa um total esgotamento da temática, alguns aspectos podem ser abordados de forma mais ampla para compreender de forma ainda mais completa e neste ponto foi possível observarmos que há grande margem para pesquisa sobre o paradoxo da privacidade como um campo ainda não explorado de forma larga ou extensa na literatura científica, mas pode ser aprofundado através dos confrontos provocados pela pesquisa conduzida neste trabalho, principalmente considerando os referenciais

teóricos de Luciano Floridi (infosfera), Zygmunt Bauman (modernidade líquida) e Shoshanna Zuboff (capitalismo de vigilância). A impossibilidade do cidadão em gerir por si próprio a tutela dos seus dados, pelos motivos explorados e encontrados durante o desenvolvimento, é ponto de interesse e análise mais profunda, que merece ser conduzida em estudos futuros.

REFERÊNCIAS

ALEMANHA. Bundersministerium der Justiz. **Bundesdatenschutzgesetz**. Berlim, 2023. Disponível em: https://www.gesetze-im-internet.de/bdsg_2018/. Acesso em: 03 jan. 2024.

BAGGIO, Andreza Cristina. **O direito do consumidor brasileiro e a teoria da confiança.** São Paulo: Editora Revista dos Tribunais, 2012.

BARBOSA, Murilo Oliveira. A Importância do Direito à Privacidade Digital, Redes Sociais e Extensão Universitária. **Revista Fragmentos de Cultura - Revista Interdisciplinar de Ciências Humanas**, Goiânia, Brasil, v. 24, n. 8, p. 89–97, 2014. DOI: 10.18224/frag.v24i0.3757. Disponível em: https://seer.pucgoias.edu.br/index.php/fragmentos/article/view/3757. Acesso em: 3 jan. 2024.

BAUMAN, Zigmund. **Modernidade líquida**. Rio de Janeiro: Jorge Zahar, 2001.

BAUMAN, Zigmund. **44 cartas do mundo líquido**. Rio de Janeiro: Jorge Zahar, 2011.

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

BIONI, Bruno Ricardo *et al*. **Tratado de Proteção de Dados Pessoais**.

Forense: Edição do Kindle, 2021.

BRASIL. [Constituição (1988)]. **Constituição Federal do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 01 nov. 2023.

BRASIL. Ministério da Inovação e da Gestão de Serviços. **Governo Digital**. Brasília, DF, 2023. Disponível em: https://www.gov.br/governodigital/pt-br. Acesso em: 03 jan. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 04 jan. 2024.

BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Proteção de Dados Pessoais. **Argumenta Journal Law**, Jacarezinho – PR, Brasil, n. 32, 2020, p. 191-207. Disponível em: https://seer.uenp.edu.br/index.php/argumenta/article/view/312. Acesso em 05 de dez. 2023.

BOULDING, Keneth Ewart. **Economics as a science**. New York: McGraw-Hill, 1970.

COECKELBERGH, Mark. **Etica de la inteligência artificial**. Ediciones Cátedra, 2021.

COHEN, Juie E. **Configuring the networked self:** Law, code, and the play of everyday practice. Connecticut: Yale Universith Press, 2012.

DANTAS BISNETO, Cícero. Reparação por danos morais pela violação à LGPD e ao RGPD: uma abordagem de direito comparado. **Civilistica. com**, v. 9, n. 3, p. 1-29, 2020. Disponível em:

https://civilistica.emnuvens.com.br/redc/article/view/493. Acesso em: 04 jan. 2024.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais [livro eletrônico]:** elementos da formação da Lei Geral de Proteção de Dados. 2. Ed. São Paulo: Thomsom Reuters Brasil. 2020.

EMPOLI, Giuliano Da. **Os engenheiros do caos.** Tradução Arnaldo Bloch. 1 ed. São Paulo: Vestígio, 2019.

FENOLL, Jordi Nieva. **Inteligencia artificial y proceso judicial.** Madrid: Marcial Pons Ediciones Jurídicas y Sociales, S. A., 2018.

FLORIDI, Luciano. **The Cambridge Handbook of Information and Computer Ethics.** Cambridge: Cambridge University Press, 2010.

FLORIDI, Luciano. **The Fourth Revolution: How the Infosphere Is Reshaping Human Reality.** Oxford University Press, 2014.

FLORIDI, Luciano. **Philosophy and computing: An introduction**. New York: Routledge, 1999.

GAVISON, Ruth. Privacy and the Limits of Law. **Yale Law Journal,** v. 89, n. 8, p. 421-471, jan. 1980. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957.

HUSTINX, Peter. **EU data protection law: The review of directive 95/46/EC and the proposed general data protection regulation**. University of Tartu. Data Protection Inspectorate, Tallinn, 2013. Disponível em: https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-dataprotection-article.pdf. Acesso em: 05 de dez. 2023.

KENSKI, Vani Moreira. **Educação e tecnologias: o novo ritmo da informação**. Campinas, SP: Papirus, 2009.

KOHLS, Cleize; DUTRA, Luiz Henrique; WELTER, Sandro. **LGPD: da teoria a implementação nas empresas.** 1. ed. São Paulo: Rideel, 2021.

LIMA, Cíntia Rosa Pereira de. O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos**. Congresso Nacional do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI)**, 23, 2014, João Pessoa. Anais [...]. Florianópolis: CONPEDI, 2014. p. 443-465. Disponível em: http://publicadireito.com.br/artigos/?cod=981322808aba8a03. Acesso em: 19 de dez. 2023.

LIMBERGUER, Têmis. Informação e internet: apontamentos para um estudo comparado entre o Regulamento Geral de Proteção de Dados Europeu e a Lei de Proteção de Dados Brasileira. **Novos Estudos Jurídicos.** Itajaí, v. 25, n. 2, p. 478-500, 2020. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/16916. Acesso em: 23 nov. 2023.

LUGER, Ewa; MORAN, Stuart; RODDEN, Tom. Consent for all: revealing the hidden complexity of terms and conditions. **CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems**, p. 2687-2696. Disponível em: https://dl.acm.org/doi/10.1145/2470654.2481371. Acesso em: 03/01/2024.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade.** 2. ed. Porto Alegre: Arquipélogo Editorial, 2019.

MARTENS, Betsy Van der Veer. An Illustrated Introduction to the Infosphere. **Library Trends**, v. 63, n. 3, p. 317-361, 2015. Disponível em: https://muse.jhu.edu/article/579339. Acesso em: 03 de jan. 2024.

MONTY, Andrea; WACKS, Raymond. **Protecting Personal Information: The Right to Privacy Reconsidered**. Hart Publishing, 2019. Edição do Kindle.

NICOLÁS, Maria Alejandra *et al*. A primeira fase da consulta pública da regulamentação do Marco Civil da internet: estrutura comunicativa, limites e contribuições. **Contemporânea Revista de Comunicação e Cultura**, v. 15, n. 2, p. 485-510, 2017. Disponível em: https://periodicos.ufba.br/index.php/contemporaneaposcom/article/view/22161. Acesso em: 04 jan. 2024.

OHM, Paul. 2009. Broken promises of privacy: Responding to the surprising failure of anonymization**. UCLA Law Review,** v. 57, p. 1701, 2010. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em: 04/01/2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Universal Declaration of Human Rights**. Nova Iorque: ONU, 1948. Disponível em: https://www.ohchr.org/en/human-rights/universal-declaration/translations/english. Acesso em: 22 dez. 2023.

PORTUGAL. **Constituição da República Portuguesa.** Disponível em: https://www.parlamento.pt/Parlamento/Documents/CRP1976.pdf. Acesso em: 10 dez. 2023.

ROSSOGLOU, Kostas. Computers, Privacy & Data Protection International Conference. **Do-it yourself privacy protection**. Bruxelas, 2015. 1 vídeo (1h 8min 24seg). Disponível em: https://www.youtube.com/watch?v=M_o_uaZwB2Y. Acesso em: 23 nov. 2023.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988**: contributo para a construção de uma dogmática constitucionalmente adequada. Direitos Fundamentais & Justiça, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em 22 nov. 2023.

SCHWAB, Klaus. **A quarta revolução industrial.** Tradução Daniel Moreira

Miranda. São Paulo: Edipro, 2016.

SHARMA, Sanjay**. Data Privacy and GDPR Handbook**. Wiley, 2020.

SILVEIRA, Sérgio Amadeu da. **Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas.** São Paulo: Edições Sesc SP, 2019.

SOLOVE, Daniel J. **The digital person**: Technology and privacy in the information age. New York: New York University Press, 2004.

SOLOVE, Daniel J. **The future of reputation**: gossip, rumor, and privacy on the internet. Yale: Yale University Press, 2007.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar-Revista de Ciências Jurídicas**, v. 22, n. 1, p. 108-146, 2017. Disponível em: https://ojs.unifor.br/rpen/article/view/6272. Acesso em: 04 jan. 2024.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, p. 269-285, 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?lang=pt. Acesso em: 04 jan. 2024.

UNIÃO EUROPEIA. **Regulação (EU) 2016/79 do Parlamento Europeu e do Conselho Europeu de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 04 jan. 2024.

VIANNA, Marcelo. Um novo "1984"? O Projeto RENAPE e as discussões

tecnopolíticas no campo da informática brasileira durante os governos militares na década de 1970. Oficina do Historiador. Porto Alegre, **EDIPUCRS**. Suplemento especial – eISSN 21783748 – I EPHIS/PUCRS - 27 a 29.05.2014, p.1448-1471. https://revistaseletronicas.pucrs.br/ojs/index.php/oficinadohistoriador/article/view/18998. Acesso em: 20 de dez. 2023.

VOIGT, Paul; VON DEM BUSSCHE, Axel. **The EU general data protection regulation (GPDR). A Practical Guide.** 1. ed., v. 10, n. 3152676, Springer International Publishing, 2017

WESTIN, Alan F. **Privacy and Freedom**. Nova Iorque: Atheneum, 1967.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. Nova Iorque: Public Affairs, 2019. Edição do Kindle.