**CENTRO UNIVERSITÁRIO INTERNACIONAL – UNINTER**
**PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO**
**MESTRADO**

**FERNANDA GONÇALES**

# PRIVACIDADE E PROTEÇÃO DE DADOS NA ERA DOS ALGORITMOS

**CURITIBA**
**2021**

**FERNANDA GONÇALES**

# PRIVACIDADE E PROTEÇÃO DE DADOS NA ERA DOS ALGORITMOS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito do Centro Universitário Internacional – UNINTER como requisito parcial para obtenção do título de Mestre em Direito.

Orientadora: Profª. Dra. Estefânia Maria de Queiroz Barboza.

**CURITIBA**
**2021**

## DEDICATÓRIA

*Aos meus pais, pelo incentivo incondicional.*
*Ao meu sobrinho Fabrício, que me ensina a olhar a vida de um modo sempre renovado.*

## AGRADECIMENTOS

Minha jornada acadêmica não seria possível sem uma rede de apoio, obrigada pelo incentivo a cada um que fez parte dela.

Agradeço a meus pais, por serem exemplo de inteligência e sabedoria, por me ensinarem desde pequena que os livros são universos inteiros e que a curiosidade e o interesse podem nos levar longe.

Ao meu sobrinho Fabrício, espero que entenda a razão de eu não estar presente em seu aniversário e nos feriados.

Ao meu amigo Davi, que mesmo longe tem papel fundamental em minha vida e com quem compartilho minhas conquistas, obrigada por mais de uma década de amizade.

À querida amiga Marta, que me influenciou a entrar no mestrado.

Ao professor Mario Ramidoff, pela parceria na produção acadêmica e pelas aulas que foram verdadeiras pílulas de ânimo no decorrer dessa jornada.

À minha orientadora Estefânia, obrigada por me adotar nesse desafio, tu és inspiração como mulher, jurista e mestre. O empoderamento feminino é essencial para que a sociedade encontre o equilíbrio fundamental para as relações humanas e para a democracia. Mulheres como você são incentivo e exemplo diário.

Obrigada ao Prof.º Daniel, que em momento desafiador não me deixou desistir. Agradeço pelas aulas incríveis, a academia precisa de mais mestres que tratem o Direito com a profundidade e crítica tão aprimoradas quanto as suas.

Às queridas Anna e Elenice, por serem sempre atenciosas e prestativas.

Aos demais professores por compartilhar seu tempo e conhecimento.

À Uninter, por proporcionar o curso em forma de bolsa de estudos integral.

À Juno, por ser uma empresa tão incrivelmente humana que possibilitou minha ida às aulas em horários de trabalho. Espero que mais Instituições sigam o exemplo da Uninter e da Juno, a inciativa privada é absolutamente necessária para que cada vez mais se produza conhecimento. Este país precisa mais do que nunca de conhecimento produzido por brasileiros para brasileiros. Conhecimento empodera, é um dos mecanismos mais eficazes no desenvolvimento social.

## RESUMO

Este estudo debate a ideia de proteção à privacidade a partir do tratamento de dados por algoritmos, considerando para tanto, que dados pessoais se tornaram uma importante mercadoria na economia da sociedade digital. A abordagem metodológica partiu de uma revisão bibliográfica sobre o tema, utilizando-se de uma visão integrada entre direito e tecnologia. A primeira parte do trabalho faz um levantamento doutrinário sobre privacidade e direito à privacidade, dentro dos diferentes contextos histórico-sociais, para formular o conceito a ser utilizado nesta pesquisa. Este capítulo também traz um apanhado normativo sobre o direito da privacidade e apresenta casos importantes relacionados ao uso de dados tanto pelo Estado quanto pela iniciativa privada, justificando a importância de se falar em privacidade na atualidade. A segunda parte trata sobre a proteção de dados, qual sua relação com o reconhecimento da autodeterminação informativa como direito, além da apresentar duas importantes leis; o Marco Civil da Internet e Lei Geral de Proteção de Dados, elencando algumas das demandas regulamentadas pelas referidas normas. Finalizando a pesquisa, a terceira parte apresenta o que são os algoritmos e debate como o seu uso no tratamento de dados afeta ou não o direito à privacidade. Ao final, apresenta quais são os principais desafios para a defesa do direito à privacidade no contexto do uso de algoritmos, apontando alguns caminhos que podem ser seguidos pelo ordenamento jurídico.

**Palavras-chave:** *Direitos Fundamentais*; *Privacidade; Algoritmos; Dados.*

## ABSTRACT

This study debates the idea of privacy protection based on data processing by algorithms, considering that personal data has become an important commodity in the economy of the digital society. The methodological approach was based on a literature review on the subject, using an integrated view between law and technology. The first part of the work makes a doctrinal survey on privacy and the right to privacy, in different historical-social contexts, to formulate the concept to be used in this research. This chapter also provides a normative overview of the right to privacy and presents important cases related to the use of data by both the State and the private sector, justifying the importance of talking about privacy today. The second part deals with data protection, what is its relationship with the recognition of informational self-determination as a right, besides presenting two important legislations; the Marco Civil da Internet and the General Data Protection Law, listing some of the demands regulated by these norms. Finalizing the research, the third part presents what algorithms are and discusses how their use in data processing affects or not the right to privacy. In the end, it presents the main challenges for the defense of the right to privacy in the context of the use of algorithms, pointing out some paths that can be followed by the legal system.


**Keywords:** *Fundamental Rights*, *Privacy; Algorithms; Data.*

**SUMÁRIO**

## INTRODUÇÃO

A ideia deste estudo nasceu com o desafio de implementação da Lei Geral de Proteção de Dados no ambiente de uma empresa de tecnologia no ramo de serviços financeiros e os diversos questionamentos advindos nesse processo tais como, o quanto a tecnologia pode interferir em nosso conceito de "vida privada"? Qual é o limite da privacidade? Juridicamente, há meios eficazes para garantir a privacidade de alguém? No contexto digital, há recursos tecnológicos adequados para garantir esse direito? O cidadão comum é capaz de compreender como os algoritmos funcionam e como eles podem influenciar suas escolhas?

Tecnologia é um termo empregado em diversos ramos, desde a medicina até a informática, como sinônimo de aperfeiçoamento e inovação[1] tanto no mundo físico quanto no virtual. Sistemas virtuais ou digitais são criados por meio de técnicas de programação não visíveis. Este estudo considera a tecnologia em meio digital e o seu desdobramento a partir do uso de algoritmos.

A evolução do acesso à internet e à tecnologia vem modelando novos modos de comunicação, comportamentos, costumes e grafias, dentro de um universo digital próprio. A sociedade é naturalmente cambiável e condutas até então inaceitáveis, como a exposição da intimidade, hoje fazem parte do cotidiano, definindo uma nova realidade social. Nesse contexto o Direito não pode se mostrar inerte, sua adaptação é necessária para acompanhar essas constantes evoluções.

Dentro dessa nova realidade digital circulam ideias, manifestações de pensamentos, dados e informações de cunho pessoal. O controle e uso desses dados pode se tornar um mecanismo de graves violações aos direitos individuais. Por essa razão, o direito precisa estar preparado para coibir abusos decorrentes do mau uso de dados.

---

[1] No dicionário Houaiss tecnologia significa: 1. Tratado das artes em geral. 2. Conjunto dos processos especiais relativos a uma determinada arte ou indústria. 3. Linguagem peculiar a um ramo determinado do conhecimento, teórico ou prático. 4. Aplicação dos conhecimentos científicos à produção em geral: Nossa era é a da grande tecnologia. T. de montagem de superfície, Inform.: método de fabricação de placas de circuito, no qual os componentes eletrônicos são soldados diretamente sobre a superfície da placa, e não inseridos em orifícios e soldados no local. T. social, Sociol: conjunto de artes e técnicas sociais aplicadas para fundamentar o trabalho social, a planificação e a engenharia, como formas de controle. De alta tecnologia, Eletrôn. e Inform.: tecnologicamente avançado: Vendemos computadores e vídeos de alta tecnologia. Sin: high-tech. Fonte: https://houaiss.uol.com.br/corporativo/apps/uol_www/v5-4/html/index.php#0.

Nessa intersecção entre o Direito e a tecnologia é onde se encaixa o tema desta pesquisa, enfocando, principalmente, no relacionamento entre os algoritmos e a privacidade no contexto digital.

A privacidade não existe sem a sociedade, é uma necessidade criada pela vida em comum (SOLOVE, 2008, p. 5). A história da privacidade está entrelaçada com a história da tecnologia, há muito que uma definição para o termo é debatida. É possível dizer que a ideia sobre o que é privacidade é mutante, assim como é mutante o comportamentoo da própria sociedade.

No início do século XXI, por exemplo, a publicação de fotografia sem o consentimento do fotografado poderia se tornar objeto de litígio entre o sujeito e o autor da fotografia[2], mas atualmente é comum acessar redes sociais e se deparar com a publicação de momentos íntimos de conhecidos e desconhecidos.

A preocupação com a privacidade varia ao longo do tempo, dos subgrupos étnicos, realidades sociais e assim por diante. Um aparentemente simples nome e endereço em uma página na internet pode não trazer qualquer implicação para grande parte da população, mas situações de vulnerabilidade alteram profundamente o contexto de privacidade, por exemplo, casos de vítimas de agressão doméstica e testemunhas de crime certamente não pretendem que seus dados estejam disponíveis ao acesso público.

Sem um núcleo de significado jurídico para o termo privacidade no contexto atual, ainda que exista uma previsão legal, qualquer lei será inadequada para efetivar esse direito. Samuel Warren e Louis Brandeis, em artigo publicado no ano de 1890, apontaram que a tolerância social e legal à exposição pública pode corromper uma sociedade, desviando a atenção de questões econômicas e políticas importantes.

É preciso entender que a sociedade está totalmente inserida em uma revolução digital, mas está apenas começando a entender suas implicações, inclusive no campo do direito. Tal fato revela a necessidade do estudo e do preparo, não só do profissional do Direito, mas também da legislação para atender a "nova sociedade digital" e suas demandas.

---

[2] *Marian Manola v. Stevens & Myers*, Suprema Corte de Nova York, New York Times de 15 de junho de 1890. A queixosa alegou que enquanto estava tocando no Broadway Theater, em um papel que exigia sua aparição sob a luz de flash, ela foi fotografada clandestinamente e sem o seu consentimento, pelos réus Stevens,e Myers, rogando para que os réus fossem impedidos de fazer uso da fotografia tirada.

Nas últimas décadas, o modo como as compras acontecem, transações bancárias são realizadas, ou mesmo, o formato das interações sociais, sofreu mudanças absurdas resultando em um acúmulo de informações sobre onde o indivíduo está, o que faz, o que possui, seus gostos e até suas variações de humor. Com o uso da tecnologia, esses registros são preservados indefinidamente em bancos de dados, são classificados, reorganizados, combinados em centenas de formas diferentes e utilizados para os mais diversos fins, desde notificações de marketing, análise de crédito e até para avaliação de possíveis combinações amorosas. São os algoritmos a principal tecnologia que possibilita o uso de dados de uma forma tão ampla e rentável.

Algoritmos se tornaram um recurso importante no desenvolvimento e aprimoramento de produtos e serviços. Como exemplo é possível citar um Banco, que pode utilizar dados sobre o hábito de navegação e cliques dos usuários em seu site para aprimorar a visualização da tela do programa, melhorando a experiência do cliente, com a redução de tempo entre o usuário *logar*[3] no site e efetivar um pagamento.

Diante de tamanha influência tecnológica em nosso cotidiano, se faz imprescindível o desenvolvimento de pesquisas a partir do olhar jurídico. Ademais, é necessário debater o uso de algoritmos em mecanismos de violação à privacidade.

Para Danilo Doneda (2020), o Direito deve estar apto a apresentar respostas às questões trazidas pela tecnologia em atenção ao texto constitucional. O autor ressalta que “o verdadeiro problema não é saber sobre o que o Direito deve atuar, mas sim como interpretar a tecnologia e suas possibilidades em relação aos valores presentes no ordenamento jurídico [...]” (DONEDA, 2020, p. 181).

Ademais, a instrumentalização e efetividade do Direito passa pela construção de interpretações sólidas. A falta de clareza em termos jurídicos cria entraves para formular políticas,[4] ou mesmo, para resolver litígios. Os parâmetros trazidos pela

[3] Verbo adaptado do conceito de "fazer login". *Login* é o início de uma sessão de conexão em que geralmente é feita a identificação do usuário no sistema.

[4] Na Inglaterra, o descontentamento com a definição de privacidade levou o Comitê Younger de Privacidade a recomendar, em 1972, contra o reconhecimento do direito à privacidade, conforme proposto na legislação da época. A principal dificuldade em promulgar uma proteção estatutária da privacidade, declarou o relatório do comitê, é a "falta de qualquer definição clara e geralmente aceita do que é a privacidade em si". Os tribunais teriam dificuldade em lidar com "um conceito tão mal definido e instável". Como resultado, a legislação não foi aprovada.

interpretação e aplicação da lei refletem a segurança jurídica que a plena cidadania demanda.

Nesse sentido, muito além da hermenêutica na interpretação das normas, o Direito se depara com um novo desafio a partir das questões tecnológicas digitais. É essencial que o Direito compreenda a aplicação da tecnologia no contexto das relações sociais com a profundidade que o assunto demanda. Para Danilo Doneda (2020), um Direito que não seja capaz de entender a dinâmica entre sociedade e tecnologia e os novos problemas decorrentes dessa relação perde contato com a realidade tornando-se precocemente obsoleto.

Muito há que se pesquisar e produzir, o aparato teórico é fundamental para orientar a melhor interpretação e aplicação da lei aos casos concretos. Ao buscar a biografia das referências utilizadas nesse trabalho, o que se encontrou foram diversos filósofos, sociólogos e pesquisadores ligados à tecnologia da informação, mas poucos ligados ao Direito, o que reforça a necessidade e a importância de estudos da matéria sob a perspectiva jurídica.

A tecnologia faz parte da vida contemporânea e, por ser expressão da realidade da sociedade da informação, não pode ficar à margem do Direito. O judiciário certamente terá de julgar demandas envolvendo código-fonte, algoritmos, *Structured Query Language* (SQL),[5] *phishing*,[6] tecnologia das coisas (*Internet of Things* – IoT),[7] entre tantos outros assuntos, para uma melhor análise jurídica a base acadêmica é fundamental.

É nessa lacuna que esta pesquisa visa contribuir, aprimorando conhecimento para melhoria e evolução material da sociedade, possibilitando, por exemplo, um arcabouço teórico para a efetiva aplicação normativa ao caso concreto ou no desenho de novas políticas públicas voltadas ao bem-estar social e à proteção de direitos fundamentais.

---

[5] Injeção de SQL (do inglês *SQL Injection*) é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados através de comandos SQL, onde o atacante consegue inserir uma instrução SQL personalizada e indevida dentro de uma consulta (*SQL query*) através de entradas de dados de uma aplicação, como formulários ou URL de uma aplicação (CARDOSO, 2018).

[6] *Phishing* é o crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito.

[7] Internet das coisas é um conceito que se refere à interconexão digital de objetos cotidianos com a Internet, conexão dos objetos mais do que das pessoas. Em outras palavras, a Internet das coisas nada mais é que uma rede de objetos físicos capaz de reunir e de transmitir dados.

Partindo da hipótese de que o uso de algoritmos para captura e tratamento de dados pessoais, pode violar o direito à privacidade, através da metodologia baseada em revisão bibliográfica, este estudo incialmente descreve as configurações histórico-sociais para entender os diversos significados do termo privacidade no decorrer do tempo, delimitando um conceito do termo “privacidade” para esta pesquisa. A pesquisa ainda buscou relatar o histórico normativo interno e externo do direito à privacidade; investigar o cenário da proteção de dados, sob a perspectiva de controle de informações como exercício do direito à privacidade; entender a relação entre algoritmos, dados pessoais e violação de privacidade, identificando a necessidade de regulamentação prévia da estrutura tecnológica como premissa para o exercício do direito à privacidade e apontar possíveis caminhos para a preservação da privacidade no uso de dados.

Diversos autores e pesquisadores de direito, tecnologia e sociologia foram consultados como referencial teórico da presente dissertação, entre eles Danilo Doneda, Marcel Leonardi, o jurista italiano Stefano Rodotá, como também os sociólogos Zygmunt Bauman e Pierre Lévy.

Para melhor entendimento do assunto proposto, a presente dissertação foi estruturada em três capítulos, com base nos objetivos específicos e construído de forma que se pudesse alcançar o objetivo geral. No primeiro capítulo, o estudo traz um apanhado bibliográfico sobre os conceitos de privacidade e direito à privacidade, suas características dentro do contexto social de diferentes épocas até as mais recentes discussões, com reflexões sobre a impossibilidade de se tornar um conceito fechado. No tocante a privacidade como direito, o capítulo também relaciona algumas das principais normativas sobre o tema.

No segundo capítulo, a pesquisa traz a evolução normativa do direito à proteção de dados no cenário externo e interno e uma breve análise sobre duas importantes legislações voltadas à proteção de dados no Brasil: o Marco Civil da Internet e Lei Geral de Proteção de Dados, relacionando quais as dores da sociedade digital que as normativas pretendem regulamentar. O capítulo trata ainda sobre a autodeterminação informativa e proteção de dados como mecanismos de defesa do direito à privacidade.

Para finalizar a pesquisa e entender a magnitude da discussão, o terceiro capítulo apresenta a definição de algoritmos, como eles estão imersos e camuflados no cotidiano da sociedade para entender se o seu uso para captura, armazenamento

e tratamento de dados, afeta ou não o direito à privacidade. O capítulo debate ainda quais são os próximos desafios para a defesa do direito à privacidade no contexto do uso de algoritmos, apontando alguns caminhos que podem ser seguidos no ordenamento jurídico, entre eles, a aproximação do direito com a tecnologia para a elaboração de normativas que definam os parâmetros da estrutura dos algoritmos e criação de uma jurisdição internacional relacionada ao uso de dados em ambiente digital.

Na configuração atual da sociedade, em que a tecnologia está presente em quase todas as atividades, certamente há muitas razões para se falar em privacidade, mas considerando que este trabalho trata sobre a privacidade com foco em proteção de dados e o uso de algoritmos, é a partir desse viés que serão apontadas algumas razões sobre porque se tornou tão importante falar sobre o tema.

Necessário mencionar que partes desta pesquisa foram apresentadas e publicadas em eventos acadêmicos.

# CAPÍTULO 1 – PRIVACIDADE

## 1.1 De onde vem a ideia de privacidade

Considerando os diversos ângulos pelos quais o assunto “privacidade” pode ser abordado, é indispensável, como bem aponta Danilo Doneda (2020), identificar o cenário no qual surge a noção de privacidade, delineando o seu desenvolvimento no plano histórico para uma consequente contextualização no momento atual.

A ideia sobre o que é privacidade naturalmente sofreu alterações, acompanhando o progresso da própria humanidade, certamente, inobstante a ausência de registros, ou mesmo a noção do que seria a privacidade, a vida nas comunidades primitivas gozava de algum modo de se exercê-la, seja pelo convívio afastado ou pelo hábito de migração típico dos primeiros grupos sociais; aquele que pretendesse não compartilhar sua intimidade com os demais, organizava seus pertences e partia para um novo local. Na antiguidade, as comunidades eram pequenas e íntimas. As informações pessoais foram preservadas na memória de amigos, familiares e vizinhos e foram espalhadas por meio de fofocas e histórias (SOLOVE, 2004).

A partir do momento em que as cidades surgem, o convívio se torna mais duradouro, exigindo regras adequadas para os relacionamentos em sociedade, ao mesmo tempo, se inicia a distinção entre individual e social. O espaço da casa permite um ambiente de separação em relação ao comum (DONEDA, 2020), a vida neste ambiente ganha maior relevância, inclusive com a mudança de comportamentos relacionados ao ambiente familiar[8].

Conforme explica Hannah Arendt (2007, p. 39) na sociedade grega, as esferas pública e privada eram marcadas pela separação entre família e política, sendo a forma de organização de ambas oposta, mas necessariamente coexistentes. A separação entre esfera pública e privada residia essencialmente “na ausência de outros”, o homem privado, em tese, não existe, vez que ele não se dá a conhecer. Nesse sentido, seus atos permanecem sem importância ou consequência para os demais, é dentro do espaço familiar que o homem se sente resguardado do mundo,

[8] O ato sexual e as necessidades fisiológicas passam a ser encobertos (THIBES, 2014, p. 86).

seus atos não têm valor porque são desconhecidos do mundo exterior (ARENT, 2007, p. 39).

Ao adentrar na esfera pública, o cidadão existia de outra maneira, por meio de uma “segunda vida (*bio politikos*) e não mais se relacionando com aquilo que lhe é próprio (*idion*), mas com o que lhe é comum (*konion*)”. Ainda que o espaço privado fosse respeitado e autônomo “em relação à polis, esses limites se mantinham, sobretudo, pelo fato de que não seria possível que o cidadão participasse dos negócios do mundo sem ser dono de sua casa, sem ter um lugar que lhe pertencesse” (ARENDT, 2007, p. 39-41).

Nessa época a privacidade literalmente constituiu uma privação, a separação do círculo mais importante da vida humana: a pública. Em Atenas, a esfera pública era configurada por assembleias de todos os cidadãos masculinos livres. No entanto, para entrar na arena pública era necessário ser proprietário (casa), o que possibilitou a configuração da "vida privada" (NIGER, 2006).

Esse comportamento social trazia a ideia de aparência e de interpretação de papéis; enquanto cidadão perante a sociedade, o indivíduo detinha um comportamento esperado, adequando-se a censura da vida em comunidade. Já no ambiente do lar, lhe era permitido desfazer-se dos padrões, dando liberdade ao próprio “eu”. O privado está relacionado àquilo que não se mostra a todos, na medida em que relaciona necessidade de sobrevivência “às exigências vitais de cada indivíduo” (FERRAZ JUNIOR, 1993, p. 441).

Durante a Idade Média, ensina Jürgen Habermas (2014) que a esfera pública é traduzida, com influência do Direito romano, como *res publica*. Sobre o assunto e tendo como base a leitura de Jürgen Habermas, Cancelier (2016, p. 46-47) destaca que “durante o período na Europa, o nobre ganha a figura da autoridade, encarnando nele mesmo características dessa esfera, materializando aquilo que se chama comumente, hoje, de pessoa pública”.

A ideia de privacidade se desenvolve à medida que o homem se reproduz, densificando os espaços naturais e aprimorando seus relacionamentos interpessoais. A interação entre o indivíduo e esse mundo externo traz consigo a necessidade de limites para que em alguma medida o homem possa manter e controlar a propriedade de seu espaço, onde ele pode expressar hábitos, gostos e emoções, ou seja, há uma concepção de separação entre o homem e o externo, entre o privado e o público a partir da ótica da propriedade.

Aos poucos, as questões do lar passam a se tornar mais relevantes ao indivíduo, dando início a uma nova formatação para o espaço privado e público. Maria Zanata Thibes (2014, p. 87) aponta que o liberalismo trouxe consigo a ideia de privacidade como uma esfera de soberania individual onde, distante da coletividade e do Estado, o indivíduo pudesse "desenvolver com plenitude suas capacidades".

Stefano Rodotà (2008, p. 27) aponta que, com a Revolução Industrial e a emergência da classe burguesa, o enlevo pela individualidade é potencializado. Para o autor, a privacidade decorre de um contexto econômico, o burguês se apropria dos espaços, dispondo de maior poder material, levanta barreiras como modo de proteger seu próprio ambiente, revelando uma nova necessidade de intimidade, que seria "um direito à propriedade solitária" com "forte componente individualista" (RODOTÁ, 2008, p. 27). Diversos estímulos que reforçam a ideia de identidade e individualidade surgem, tais como: diários, álbuns de fotografia (THIBES, 2014, p. 87).

Sobre esse interesse da sociedade da época em se manter afastada das classes menos abastadas Hannah Arendt elucida que:

> [...], a sociedade assumiu o disfarce de uma organização de proprietários que, ao invés de se arrogarem acesso à esfera pública em virtude de sua riqueza, exigiram dela proteção para o acúmulo de mais riqueza. Nas palavras de Bodin, o governo pertencia aos reis e a propriedade aos súditos, de sorte que o dever do rei era governar no interesse da propriedade de seus súditos (ARENDT, 2007, p. 38).

A privacidade pode ser tida como uma consequência óbvia da estrutura geral dos sistemas jurídicos burgueses em que o reconhecimento formal dos direitos da personalidade se traduz principalmente na garantia acentuada da propriedade, entendida como a projeção máxima dos direitos individuais da liberdade. "A ideia que hoje fazemos de privacidade é, portanto, herdeira daquela engendrada pela sociedade burguesa florescente." (THIBES, 2014, p. 87). De acordo com Stefano Rodotá (2008, p. 27), "a privacidade passa a ser prerrogativa de uma classe que, com seu forte componente individualista, utiliza-se dela para marcar sua identidade na sociedade como também para proporcionar que o indivíduo se isole dentro de sua própria classe".

A privacidade, filha das necessidades de uma sociedade burguesa moralista, se manteve restrita ao meio em que nasceu até o final da primeira metade do séc. XX. Nesse momento da vida da sociedade se dá o início a uma nova mudança de percepção de público e privado e a vida privada se torna uma forma de expressão da

personalidade, permitindo ao indivíduo um espaço de liberdade para exercer sua própria soberania. “Ou seja, a privacidade, nos moldes como é compreendida atualmente, funda-se na percepção da relação do indivíduo com a sociedade” (DONEDA, 2020, p. 127).

Conforme Maria Cláudia Cachapuz (2006, p. 66-68), a “[...] alteração fundamental tem origem numa conceituada emancipação psicológica [...]” do sujeito perante a sociedade e, com isso, “[...] aquilo que é privado em contraposição ao que é público deixa de ser identificado por um enfoque político para ganhar força na oposição entre o social e o íntimo” (CACHAPUZ, 2006, p. 68).

Como bem aponta Byung-Chul Han (2015, p. 58), “Trata-se de uma época na qual se estabeleceu uma divisão nítida entre dentro e fora, amigo e inimigo ou entre próprio e estranho.”

Como já dito, o cenário de sociedade burguesa evolui para o cenário da sociedade do capitalismo industrial, onde essa separação de vida privada e social passa a despertar a curiosidade alheia, espalham-se notícias sobre comportamentos e acontecimentos, inclusive por meio da imprensa. Maria Zanata Thibes (2014, p. 91) aponta que um dos pontos fundamentais para a divisão de público e privado no capitalismo, foi a criação de unidades de produção, separadas do âmbito familiar. Em outras palavras, o indivíduo, diariamente em uma janela de tempo, deixa o local onde reside e convive com familiares e se dirige para a unidade de trabalho, onde interage com diversos outros indivíduos em uma relação, muitas vezes não tão próxima. Assim também interage com o Estado, quando se faz uso de serviços público em locais próprios para tal.

A própria arquitetura do ambiente de trabalho e de residência são alterados, delimitando claramente suas diferenças, tornando-os cada vez distantes (RODOTÀ, 2008, p. 26).

Assim, novos parâmetros da acepção de privacidade passam a ser desenhados, surgindo também a opinião pública[9]. A notícia, os escândalos e fofocas

[9] Na Inglaterra, desde meados do século XVII, começa a ser chamado de public aquilo que até então era designado pela palavra world ou mankind. Do mesmo modo, surge le public francês como definição para aquilo que na Alemanha do século XVIII, seguindo o dicionário dos irmãos Grimm, costumava-se chamar de Publikum, termo proveniente de Berlim. […]. No fim do século XVII, surge o termo inglês publicity, derivado do francês publicité. Na Alemanha, a palavra aparece no século XVIII. A própria crítica se apresenta na forma de [opinião pública], termo que se formou a partir de opinion publique na segunda metade do século XVIII. Quase simultaneamente surge na Inglaterra public opinion; contudo, muito tempo antes já se falava de general opinion. (HABERMAS, 2014, p. 134)

familiares passam a ter valor econômico, ou seja, se tornam mercadoria. A comercialização da imprensa incentiva a interação do público, extrapolando a delimitação entre as esferas pública e privada até então existentes.

Nessa nova configuração, a imprensa além de veículo de notícias, também passa servir à administração pública, que a utiliza para anunciar ordens e decretos, fazendo com que os destinatários do poder público comecem a se tornar propriamente "o público" (HABERMAS, 2014). Dessa forma, é possível dizer que a imprensa teve importante papel na definição de privacidade da época, a partir do momento que ela se torna um componente da divisão entre o que o social público e o social privado. Sobre o assunto, Tércio Sampaio Ferraz Júnior explica que:

> A afirmação generalizada da "sociabilidade" trouxe o problema da distinção entre o social público (área da política) e o social privado (área do econômico, do mercado), donde o aparecimento de duas novas e importantes dicotomias que estão na raiz dos direitos humanos modernos: Estado e sociedade, sociedade e indivíduo. É nesse contexto que surge a privacidade. O social privado, o mercado, passa a exigir a garantia de um interesse público (livre concorrência, propriedade privada dos bens de produção) que não se confunda com o governo (política), embora dele precise. Mas, contra a presença abrangente e avassaladora do mercado que nivela os homens à mercadoria, contrapõe-se a privacidade do indivíduo (FERRAZ JUNIOR, 1993, p. 141).

A questão toma novos caminhos principalmente a partir da década de 1960, diante do crescimento da circulação de informações, diretamente relacionada ao desenvolvimento tecnológico, onde a relação indivíduo-mundo exterior desenvolve novas formas (COSTA JÚNIOR, 1970, p. 17). A construção da personalidade humana perante o mundo não mais se limita a seara individual, mas decorre da relação entre o indivíduo e o externo. Essa interação perpassa os meios digitais de comunicação. Sendo assim, a tutela desse indivíduo deve se realizar "em relação aos outros (o sentido da alteridade) e ao mundo externo. [...] o ser humano existe apenas como integrante de uma espécie que precisa de outro(s) para existir (*rectius*, coexistir)" (MORAES, 2010, p. 14).

Com a chegada da imprensa, as questões até então tidas como privadas são amplamente reveladas e debatidas (BAUMAN, 2013, p. 107). A interação entre o privado e o público afeta essa dissociação entre esferas que prevalecia até então. Os costumes burgueses perdem força com a sociedade tecnológica, o indivíduo mergulhado nos mecanismos de manipulação da massa deixa de exigir a preservação do seu isolamento (COSTA JÚNIOR, 1970, p. 18). De modo que esse novo modelo

de interação modifica também o conceito de privacidade, que passa a ser vista como a ideia de limitação da interação do homem com o externo, calcada na ideia de proteção da personalidade.

Por sua vez, a chegada da tecnologia digital muda novamente esse formato, na medida em que a interação indivíduo-externo amplia-se em proporções absurdas. Essa interação produz dados e informações que passam a ter valor comercial e são usadas em sua grande parte sem o consentimento do titular, muitas desses dados se referem diretamente ao espaço pessoal do homem, seus hábitos, gostos e emoções. Assim, surge a necessidade de controle de dados como modo de preservar a privacidade.

Costa Júnior (1970, p.15-21) lembra que diversos estudiosos do tema, apontam o paradigma da privacidade na atualidade; ao mesmo que a tecnologia possibilita conforto e uma perfeita integração entre o indivíduo e seu lar ela conspira contra a intimidade e corrói a vida privada, refletindo profundamente em questões éticas e jurídicas.

Como visto, o conceito sobre o que a sociedade entende como privacidade evolui junto com ela, lá nos primórdios, o lar é tido como mecanismo de proteção à privacidade fundamentado na separação material. A chegada da imprensa quebra as barreiras físicas até então existentes, exigindo uma nova abordagem para o tema, a privacidade passa a abranger a personalidade e tudo que se relaciona a ela, nome, imagem etc.

Mais recentemente, a sociedade digital remodela novamente o conceito, porque as interações em ambiente digital geram dados com valor econômico, nesse sentido nossa identidade digital[10] também carece de proteção jurídica.

Embora não haja dúvidas sobre a importância e valor da privacidade, o entendimento sobre seu significado não é uníssono, a depender do ângulo de análise, seja filosófico, jurídico, econômico, individual ou coletivo, ela pode tomar formas e interpretações diversas, algumas mais restritivas outras mais abrangentes. É importante entender o histórico do conceito de privacidade na medida em que o direito se vale dessas ideias para construir normas e políticas públicas. Assim, a delimitação do termo “privacidade” para fins desta pesquisa é o assunto do próximo tópico.

[10] O terceiro capítulo trata de questões relacionadas à identidade digital.

## 1.2 Sobre qual privacidade estamos falando? Delimitando a esfera de interpretação

Como próximo passo do desenvolvimento do tema, importa tratar da privacidade como direito. Não pretende o presente estudo cunhar uma definição semântica, preocupa-se, muito mais, em destacar a necessidade de harmonização quanto aos limites interpretativos, sob a perspectiva do Direito e da realidade tecnológica-digital atual.

A privacidade é tida como uma das questões protagonistas da nossa época e verdadeiros aspecto-chave da dignidade humana. O contraste entre o panorama da privacidade em 2021 e aquele do início dos anos 1990 é perceptível. A chegada da era digital ao cotidiano da sociedade criou novas complexidades, intensidades e vulnerabilidades, ressaltando a necessidade de renovada análise jurídica que considere o envolvimento da tecnologia digital nos aspectos da privacidade.

Como já dito, são tantas as facetas da privacidade que as diferentes disciplinas a utilizam para se referir a conceitos bastante distintos: da autonomia à confidencialidade; da liberdade para segredo; da solidão ao anonimato.

As diferentes concepções podem ser resultado da metodologia utilizada, o que torna a discussão ainda mais complexa. Marcel Leonardi (2011, p. 47) aponta que a grande parte das tentativas de modular o significado de privacidade usa métodos tradicionais como a definição *per genus et differentiam*[11], nesse sentido, se faz uso de uma combinação de elementos comuns, o "núcleo", "essência", "âmago", "eixo", "mola-mestra", "cerne", "alma", "bojo", que permite diferenciar um direito à privacidade, no caso, dos demais direitos, criando uma noção unitária. Com essa técnica se pretende separar conceitos, permitindo subsumir determinada situação fática a essa ou aquela categoria a depender de sua definição.

Bruno Lewicki (2003, p. 9) afirma que palavras de uso corrente para exprimir a ideia de privacidade como 'segredo' e sigilo' estariam relacionadas à inviolabilidade das comunicações pessoais, 'recato' teria o sentido de pudor, 'intimidade' conotação sexual e 'reserva' além de pouco utilizada não teria muita precisão, mas poderia estar ligada à preservação de aspectos íntimos.

[11] Pelo gênero próximo e pela diferença específica.

A privacidade pode ser definida muito mais subjetivamente do que objetivamente. Descrita como um anglicismo derivado de *privacy* (COSTA JÚNIOR, 1979, p 26), o vocábulo "privacidade" é comumente utilizado como um termo mãe ou palavra-chave, que compreende uma infinidade de possíveis interpretações, a respeito do qual a doutrina[12] utiliza diversos outros sinônimos tais como: âmbito interno, vida íntima, secreto, segredo, sigiloso, estar só e autonomia. Danilo Doneda (2006, p. 101) acrescenta termos como "vida privada, intimidade, sigilo, recato, reserva, intimidade da vida privada, e até mesmo 'privatividade' e 'privaticidade'".

Marcel Leonardi (201, p. 48) menciona que a concepção de privacidade pode ser mais ou menos abrangente e algumas expressões correlatas podem ser incluídas, ou não, a depender da linha de entendimento adotada pelos diversos doutrinadores, apontando como relacionados à privacidade os seguintes termos "[...] liberdade de pensamento, controle sobre o próprio corpo, quietude do lar, recato, controle sobre informações pessoais, proteção da reputação, proteção contra buscas e investigações, desenvolvimento da personalidade, autodeterminação informativa." (LEONARDI, 2011, p. 48).

Dessa forma, é possível dizer que a privacidade está relacionada ao íntimo do indivíduo, ao seu espaço pessoal, sendo este inviolável. Todavia, Paulo Mota Pinto (1993, p. 504) afirma que o termo privacidade é elástico e tentar defini-lo é praticamente impossível, em suas palavras: "[...] Se é verdade que se empreenderam tentativas de definição filosófica, política, sociológica ou psicológica da '*privacy*', não parece que se tenha logrado extremar o conceito com o mínimo de precisão indispensável para ele poder servir de base a um regime jurídico coeso."

Nesse sentido, é possível afirmar que a palavra privacidade não é autoexplicativa, na medida em que compreende um universo inteiro em si mesma, seria possível dizer que o termo envolve tudo aquilo que se relaciona com o espaço pessoal de cada indivíduo, os aspectos de si mesmo, seu corpo, pensamentos, desejos, medos, seja no mundo físico ou não, e que a sua falta torna o indivíduo vulnerável ao externo. Assim, uma vez que se alterna a existência dentro de uma

[12] O mesmo ocorre na doutrina estrangeira, que se socorre de uma variedade de expressões para se referir à privacidade. Na Alemanha, tem-se die *Privatsphäre,* separando a autonomia individual e a vida social; na Espanha, prefere-se o termo *Derecho a la intimidad*; nos Estados Unidos, utiliza-se a expressão *privacy*; na França, fala-se em *droit au secret de la vie privée* e em *protection de la vie privée*; na Itália, refere-se ao *diritto alla riservatezza* e ao *diritto alla segretezza* e à *privacy*; em Portugal, se diz reserva da intimidade da vida privada e privacidade (LEONARDI, 2011, p. 46).

dinâmica de vida social, a privacidade pode ser representada também pelas atitudes e reservas individuais.

A problemática que envolve uma concepção para privacidade tem dois lados; a definição é ampla demais ou estreita demais, a depender dos termos utilizados, que podem englobar assuntos considerados privados ou não (LEONARDI, 2011, 51). A ausência de uma forma delimitada, pode acarretar a dificuldade da aplicação enquanto direito, inviabilizando sua tutela, notadamente diante de direitos e interesses colidentes (LEONARDI, 2011, p. 53).

A maioria da doutrina que trata de privacidade defende sua importância, mas não a define. De acordo com Ferdinand Schoeman (1994, p. 21), os autores comumente a relacionam com vários outros valores, incluindo o direito de ser deixado em paz (direito ao esquecimento) e o respeito devido à personalidade inviolável do indivíduo. Com base no autor, é possível dizer que uma pessoa tem privacidade na medida em que os outros têm acesso limitado às informações sobre ela, bem como às intimidades de sua vida e/ou a seus pensamentos ou corpo.

Acontece que sem uma noção do que é privado, as concepções de acesso limitado não demonstram quais são os substantivos que implicariam em privacidade plena. Daniel Solove (2008) aponta que nem todo acesso ao *self* infringe a privacidade, apenas aquele relacionado a dimensões específicas ou a assuntos e informações particulares. Para além, não há entendimento sobre o grau de acesso necessário para constituir uma violação de privacidade. De acordo com as definições de Hannah Arendt (2007, p. 41) seria possível definir privacidade como a separação entre a vida comum, em meio aos demais iguais, e o espaço do âmbito familiar. A autora explica que:

> A polis diferenciava-se da família pelo fato de somente conhecer ´iguais´, ao passo que a família era o centro da mais severa desigualdade. Ser livre significava ao mesmo tempo não estar sujeito às necessidades da vida nem ao comando de outro e também não comandar. Não significava domínio, como também não significava submissão (ARENDT, 2007, p. 41).

Contudo, a dicotomia pessoa-espaço-público e pessoa-espaço-familiar não pode ser considerada como a melhor definição para a construção da privacidade como direito na atualidade. A ideia de privacidade é um construto histórico e cultural, ou seja, desenvolve-se a partir de condições sociais, econômicas e políticas de determinada época e em determinado local. Com isso, a formação do sentido de

privacidade trazida por Hannah Arendt (2007. p. 39-41) tem ligação direta com a realidade vivenciada lá atrás pela sociedade grega, calcada no conceito de propriedade e de um “corpo político”. A atual conjuntura social tecnológica digital por si já afasta a ideia de privacidade como separação de esferas entre público e familiar.

Gonçalves e Rodrigues (2018) citam a Teoria dos Círculos Concêntricos da esfera da vida privada (ou Teoria das Esferas da Personalidade) elaborada pelos alemães Heinrich Hubmann e Heinrich Henkel para discutir sobre o tema. A teoria preconiza a existência de três níveis distintos da vida privada - são três círculos concêntricos que tratam da privacidade de forma ampla: o círculo da vida privada em sentido estrito, o círculo da intimidade e, no meio, o círculo do segredo.

A respeito da Teoria dos Círculos Concêntricos, Sônia Vieira (2002, p. 17) ensina, de forma resumida, que:

> A esfera individual, responsável pela proteção à honra, tem como manifestações mais importantes o direito ao nome e a reputação. A esfera privada tem por objetivo a proteção contra a indiscrição. Na esfera individual o cidadão do mundo acha-se relacionado com seus semelhantes; na esfera privada, ao contrário, o cidadão acha-se na intimidade ou no recato, em seu isolamento moral, convivendo com a própria individualidade (VIEIRA, 2002, p.17).

No centro do círculo, ou esfera do segredo, está o âmago da privacidade, onde a parcela mais íntima do indivíduo existe, cujas informações, quando compartilhadas, o são a um número restrito de pessoas (COSTA JÚNIOR, 1970, p. 33).

O círculo do meio, ou a segunda esfera, seria a da intimidade (*Vertrauensphäre/Vertrauensphäre*), dela participam aquelas pessoas nas quais o indivíduo deposita certa confiança e mantém amizade. De acordo com Paulo José da Costa Jr. (1970, p. 31): “Fazem parte desse campo conversações ou acontecimentos íntimos, dele estando excluídos não só o *quivis ex populo*, como muitos membros que chegam a integrar a esfera pessoal do titular do direito à intimidade”.

Sobre o terceiro círculo Paulo José da Costa Jr. (1970, p. 31) preleciona que a esfera mais externa seria a esfera privada stricto sensu (*Privatsphäre*) "nele estão compreendidos todos aqueles comportamentos e acontecimentos que o indivíduo não quer que se tornem do domínio público". Dessa forma, o círculo mais amplo diz respeito à vida privada em sentido estrito, em que repousam as relações interpessoais mais rasas, nas quais não há um amplo grau de conhecimento da vida alheia. Nessa

situação, ainda que o acesso ao público seja restrito, seu grau de limitações é o menor dentre as três esferas[13].

Dada a natureza multifacetada da privacidade, o direito pode oferecer um ângulo interessante de análise. Um dos objetivos da pesquisa acadêmica é entender a função e utilidade da norma, nesse caso, o quanto a privacidade como direito afeta positivamente ou negativamente as relações jurídicas. A tentativa de definição para o termo privacidade requer o enfrentamento de muitas contradições semânticas, mas é possível dizer que, de um modo geral, a privacidade tem um valor positivo por si só.

As tradicionais maneiras de conceituar privacidade não levam em conta as particularidades e os problemas que a era digital introduziu (SOLOVE, 2004). Urge então a necessidade de definição do termo privacidade sob o viés jurídico e incorporado ao contexto atual, ou seja, dentro da realidade vivenciada pela sociedade, principalmente, com inserção da tecnologia digital.

Historicamente, o direito à privacidade tem sido entendido como o direito de "ser deixado só", esse entendimento é fundamentado no artigo de Samuel Warren e Louis Brandeis (1890). Esse direito - o "direito de ser deixado em paz" - era um "direito geral à imunidade da pessoa, o direito à personalidade" (SOLOVE, 2008, p. 212). Danilo Doneda (2020) aponta que os autores em nenhum momento definem o direito à privacidade:

> A associação que geralmente é feita do artigo com o *right to be let alone* deve ser relativizada: essa é uma citação da obra do magistrado norte-americano Thomas Cooley, que os autores não chegam a afirmar que traduziria propriamente o conteúdo do direito à privacidade – ou seja, Warren e Brandeis não chegaram a trabalhar com uma perspectiva fechada de *privacy* (DONEDA, 2020, p. 105-106).

Como apontado por Doneda, a definição de direito à privacidade não é trazida por Samuel Warren e Louis Brandeis (1890), os autores destacam apenas que se trata de um direito protegido pela *Common Law*. Visando desenhar o conceito de privacidade, Marcel Leonardi (2011, p. 52) elenca as principais ideias para uma concepção do termo privacidade: "a) o direito a ser deixado só (*the right to be let alone*); b) o resguardo contra interferências alheias; c) segredo ou sigilo; d) controle sobre informações e dados pessoais".

[13] A teoria das três esferas é reconhecida pelo Supremo Tribunal Federal no ARE 867326 RG/SC; pelo Tribunal Superior do Trabalho no RecAdm-PADMag 06.2013.5.02.0000.

Como lembra Danilo Doneda (2020), a privacidade como direito surge em um período em que diversas questões da vida em sociedade passam a ser judicializadas, pela mudança de percepção da pessoa humana no ordenamento jurídico.

A chegada do século XX reinventou a privacidade: “De um direito com uma dimensão estritamente negativa e com uma conotação quase egoísta, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático” (MENDES, 2014, p. 29).

Para Rodotà, a privacidade é entendida como “o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular” (2008. p. 15). Alexandre de Moraes (1999, p. 80) entende que o direito à privacidade deve proteger o indivíduo face:

> (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional (Moraes, 1999, p. 80).

O direito à privacidade visa a proteger o indivíduo “dos esforços de atores comerciais e governamentais” em torná-los “predizíveis” (COHEN, 2013, p. 1905). Milton Fernandes (1977, p. 99), aponta que a melhor definição de privacidade é: “o direito de excluir razoavelmente da informação alheia ideias, fatos e dados pertinentes ao sujeito”, para o autor, esta é a “essência da intimidade”.

Para Caitlin Mulholland (2012, p. 2), privacidade alude à proteção da esfera privada ou íntima de uma pessoa, face as ingerências externas, alheias e não autorizadas. A autora entende que “a privacidade evoluiu para incluir em seu conteúdo situações de tutela de dados sensíveis, de seu controle pelo titular” e elenca três concepções do direito à privacidade, (i) o direito de ser deixado só, (ii) o direito de ter controle sobre a circulação dos dados pessoais, e (iii) o direito à liberdade das escolhas pessoais de caráter existencial (MULHOLLAND, 2012, p.3).

Bruno Lewicki (2003, p. 9) afirma que o conceito está ligado diretamente ao “respeito à liberdade das escolhas pessoais de caráter existencial”. Alan Westing (1968, p. 7), por sua vez, aduz que privacidade “é a pretensão de indivíduos, grupos ou instituições de determinarem para si quando, como, e em que extensão a

informação sobre eles será comunicada a outros". Solove entende privacidade como "[…] a fundamental right, essential for freedom, democracy, psychological well-being, individuality, and creativity[14]" (SOLOVE, 2008, p. 92-94).

Para Tércio Sampaio Ferraz Jr (1993, p. 439-459) a privacidade é subjetiva, orientada pelas escolhas individuais e não segue padrões. "No recôndito da privacidade se esconde, pois, a intimidade. A intimidade não exige publicidade porque não envolve direitos de terceiros. O âmbito da privacidade é o mais exclusivo dos seus direitos" (FERRAZ JÚNIOR, 1993, p. 442).

A Ministra Rosa Weber em seu voto da Ação Direta de Inconstitucionalidade nº 5.527[15] aponta que a esfera privativa deve ser um ambiente seguro de expressão do eu, de desenvolvimento da autonomia individual, onde conflitos pessoais e erros da juventude, não significam julgamentos. "Permite, dito de outro modo, o espaço de liberdade onde se processa a experimentação necessária ao progresso social". No entendimento da Ministra a proteção da privacidade está relacionada diretamente a "passar a vida sem ser contrariado, sem sentir desconforto social, sem ser ofendido" (BRASIL, STF, 2020).

Nessa mesma linha Cristiano Chaves de Farias e Nelson Rosenvald (2012, p. 247) entendem privacidade como sinônimo de refúgio individual, para os autores;

> A vida privada é o refúgio impenetrável pela coletividade, merecendo proteção. Ou seja, é o direito de viver a sua própria vida em isolamento, não sendo submetido à publicidade que não provocou, nem desejou. Consiste no direito de obstar que a atividade de terceiro venha a conhecer, descobrir ou divulgar as particularidades de uma pessoa (FARIAS; ROSENVALD, 2012, p. 47)**.**

Flávio Tartuce (2014, p. 166-167), baseado na teoria da ponderação, traz um contraponto interessante ao debate ao afirmar que o direito à privacidade não é absoluto e deve ser ponderado em relação a outros princípios constitucionais. O autor menciona ainda, que a efetividade desse direito representa verdadeiro desafio, diante das violações constantes.

---

[14] [...] um direito fundamental, essencial para a liberdade, democracia, bem-estar psicológico, individualidade e criatividade. Tradução livre.

[15] A ADI nº 5.527 questiona a constitucionalidade dos artigos 10, parágrafo 2º, e 12, incisos III e IV do Marco Civil da Internet, usados para fundamentar decisões judiciais que determinaram a suspensão dos serviços do aplicativo Whatsapp entre 2015 e 2016.

A privacidade como direito é decorrente também do direito à liberdade, que, por sua vez, é um dos pilares da democracia. Embora a democracia se preocupe com as liberdades públicas, como a liberdade de manifestação, de imprensa, liberdade artística e de religião por exemplo, ela também se preocupa com a liberdade privada, protegendo a intimidade e a vida privada.

Como se pode ver, o conceito de privacidade pode estar relacionado ao direito à privacidade para parte da doutrina. Privacidade e direito à privacidade são assuntos que não perdem a característica de atualidade, na medida em que são discutidos há muito tempo, sob a perspectiva de uma sociedade mutante.

É importante mencionar que, na atual época, com o termo privacidade sendo comumente utilizado quando o assunto envolve tecnologias digitais , é necessário que sua definição jurídica tenha contornos claros, para que não venha a se tornar um direito banalizado, mal interpretado e mal aplicado.

Ademais, a proteção da privacidade é essencial para o bem-estar psicológico individual, bem como, para a harmonia social, notadamente na era da digital, onde os limites entre o que é público e privado são extremamente tênues. Stefano Rodotà (1995, p.102) descreve que o fundamento do direito à privacidade passou da configuração “pessoa-informação-segredo”, para “pessoa-informação-circulação-controle”. Para o jurista, a privacidade configura a realização da “liberdade existencial” e deve possibilitar ao indivíduo uma “maneira de construir sua própria esfera particular” (RODOTÀ, 2008, p.15) e a realização plena de sua liberdade existencial (RODOTÀ, 2008, p. 92). Vinícius Borges Fortes (2016, p. 103) menciona que a necessidade de privacidade é inerente a todas as sociedades e se relaciona diretamente com outras áreas da vida:

> [...] a privacidade individual, a intimidade do grupo familiar, a comunidade como um todo. As normas de privacidade para a sociedade são estabelecidas em cada uma dessas três áreas. Na primeira área, o indivíduo busca privacidade assim como busca companhia em suas interações diárias com outros indivíduos. Os limites são definidos para manter algum grau de distância em momentos cruciais da vida. No ambiente familiar, também são instituídas normas para os membros da família e do ambiente externo, de modo a proteger as atividades dentro do lar. Na terceira área, cerimônias e rituais significativos na sociedade são protegidos por regras de privacidade de cada grupo (FORTES, 2016, p. 103).

Como visto, privacidade é uma palavra de muitos significados, a problemática abordada pelo debate filosófico, linguístico e jurídico é justamente a imprecisão do

conceito. Mas, essa dificuldade não é uma qualidade apenas da privacidade, diversos outros termos encontram o mesmo obstáculo, liberdade e a democracia são exemplos. Nesse sentido, vale lembrar, mas sem aprofundar no assunto, que a problemática se revela não apenas quanto ao conceito do termo, mas também na aplicação prática desse direito.

Embora existam diferenças trazidas pela literatura, duas abordagens são comumente encontradas para caracterizar o que seria a privacidade: a ideia de restrição ao acesso alheio e a noção de controle.

Assim, para este estudo, a percepção de privacidade será considerada a partir desses dois elementos: a) restrição de acesso àquilo que se relaciona ao indivíduo, como informações e dados pessoais e; b) controle, no sentido de que pertence ao titular permitir o uso de seus dados. Ressalta-se que os referidos elementos foram definidos a partir do ponto de vista da privacidade como direito da personalidade. Por fim, vale mencionar que o conceito definido para este trabalho não leva em consideração o debate sobre a natureza de direito de propriedade sobre dados que permitiria ao titular dispor livremente sobre eles.

Delimitados os parâmetros de interpretação para o termo “privacidade” é necessário apresentar o desenvolvimento histórico do direito à privacidade. Este é o próximo assunto a ser tratado.

## 1.3 Privacidade como direito

Como veremos adiante, os primeiros estudos e decisões judiciais que deram a privacidade o status de direito remontam ao séc. XIX, o que é relativamente recente. Como já debatido, tal fato tem sentido quando a privacidade é analisada sob o viés da construção da sociedade. Em ambientes restritos, como pequenas cidades ou áreas rurais e sem a presença da imprensa, não parece vital falar de privacidade, tampouco tratá-la como um direito.

A palavra privacidade não possui um conceito único e objetivo para a doutrina. Nessa mesma ideia, o direito à privacidade, assim como os demais direitos fundamentais, possui caráter eminentemente elástico e variável, conforme o tempo, o espaço e o titular da garantia.

No continente Europeu, no ano de 1846, David Augusto Röder, publicou um trabalho defendendo que adentrar recinto sem se fazer anunciar seria um ato violador do direito natural à vida privada[16].

No ano de 1858, o Tribunal de Séné, na França, reconheceu pela primeira vez o direito à privacidade, impedindo que imagens de uma atriz, em momentos antecessores à sua morte, fossem divulgadas sem a autorização da família[17] (SAMPAIO, 1998, p. 55-60). A decisão do Tribunal reflete o progresso do conceito sobre o que é privacidade no sentido de proteção à personalidade.

As principais discussões sobre os temas privacidade, intimidade e vida privada surgem com a chegada de recursos tecnológicos, como o uso de máquinas fotográficas e da imprensa, porque esses mecanismos possibilitaram a exposição de ambientes até então restritos em larga escala.

No ano de 1890, a Harvard Law Review, publicou o artigo *Right to privacy*, escrito por Samuel Dennis Warren e Louis Demitz Brandeis, o trabalho é considerado o marco doutrinário sobre o direito à privacidade. Tratando de questões relacionadas à privacidade e tecnologia da época, como fotografia e jornais, como esses meios haviam entrado na vida privada de muitas pessoas. Os autores foram os primeiros a reconhecer e expor as ameaças à privacidade que poderiam refletir no desenvolvimento da sociedade. Warren e Brandeis na formulação do direito à privacidade e seus limites, identificaram muitos aspectos importantes: o direito à privacidade não era absoluto, porque o poder público poderia sobrepor a ele. A violação de direitos sobre a privacidade pode ser esquecida mediante o consentimento do afetado. A veracidade da informação não afastava a violação de direitos.

No estudo, os Autores analisam precedentes da Suprema Corte dos EUA relacionados à propriedade, à difamação e aos direitos autorais. A redação do artigo aponta que as decisões proferidas pela Corte refletiam a caracterização de um direito geral à privacidade, para proteger o indivíduo tanto do governo como de outros indivíduos.

---

[16] Grundzüge des Naturrechts oder der Rechtsphilosophi.

[17] Caso Affaire Rachel: Para atender ao último pedido da atriz, a irmã contratou dois fotógrafos para fotografá-la em seu leito de morte, com a condição de que a fotografia não poderia ser reproduzida. Contudo, os profissionais de forma não autorizada, cederam a imagem para elaboração de um desenho que foi posteriormente. A família da atriz ajuizou ação em face do desenhista e o Tribunal proferiu sentença no sentido de que não seria dado a ninguém reproduzir e dar publicidade a traços de uma pessoa em seu leite de morte, sem autorização formal da família. (MACHADO, 2014, p. 35-36)

Os juristas apontam a necessidade do reconhecimento efetivo do direito à privacidade pelas Cortes, por meio de mecanismos disponíveis da *common law,* do *right to privacy*, como um desdobramento da tutela da personalidade humana, consubstanciado no direito de o indivíduo estar só com suas emoções, sentimentos e pensamentos mesmo que expressos nas mais diversas formas, físicas ou não, tais como diálogos, arte ou escrita. (WARREN; BRANDEIS, 1890).

Samuel Warren e Louis Brandeis (1890) destacam que a tecnologia ao invadir o âmbito residencial ameaça expor questões relacionadas ao sagrado do lar, servindo de veículo para a disseminação de fofoca com fins comerciais. O uso dos meios de comunicação para publicar futricas acaba por se tornar um sistema de oferta e demanda e um mal que poderia empobrecer os valores da sociedade. Para além, tal fato certamente causa danos em dimensões que vão além das vítimas das matérias.

O trabalho entende que o cerne da privacidade não é a propriedade, mas a inviolabilidade da personalidade, seu valor não se perfaz no direito a receber indenização em decorrência da violação, mas sim na segurança e capacidade de impedir a própria violação. Em conclusão, os autores consideram que o direito de estar só não seria absoluto e poderia sofrer relativização em alguns casos como; autorização legal; matéria de interesse geral do público e diante do consentimento do titular (WARREN; BRANDEIS, 1890).

Sobre o artigo de Samuel Warren e Louis Brandeis (1890), Dorothy J. Glancy (1979, p. 3) destaca que os autores, com base na investigação da jurisprudência da Corte Americana de áreas tradicionais do direito como contratos, propriedade e direitos, captaram subsídios para defender o direito de ser deixado só como uma categoria do direito fundamental à vida, previsto na quinta emenda à Constituição dos Estados Unidos: "Nenhuma pessoa deve [...] ser privada da vida, liberdade ou propriedade sem o devido processo legal [...]" (GLANCY, 1979, p. 3).

No campo normativo, os primeiros passos relacionados à privacidade acontecem principalmente em décadas do pós-guerra. A partir da Segunda Guerra os direitos da personalidade ganham reconhecimento e notável força normativa, sendo chamados pela doutrina de "emanações da própria dignidade humana", na medida em que são reconhecidamente inseparáveis de qualquer indivíduo (BARROSO; BARCELOS, 2004, p. 12).

A Declaração Universal dos Direitos do Homem, aprovada no ano de 1948, concedeu à privacidade relevância internacional, ao dispor em seu art. XII: "Ninguém

será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques".

A inserção do direito à privacidade como um direito fundamental na Declaração Universal dos Direitos Humanos é o resultado do avanço no reconhecimento desse direito como essencial ao desenvolvimento da personalidade humana e da própria sociedade.

Anos depois, em 1966, o Pacto Internacional de Direitos Civis e Políticos, também tratou do tema no art. 17, § 1: "Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação."

O tema se tornou objeto de diversos congressos na década de 60, entre eles; Trento – 18 a 20 de maio de 1962, que tratou do direito à intimidade; Jornadas Jurídicas Ítalo-Iugoslavas – 7 a 16 de maio de 1963, que discutiu questões relacionadas a personalidade e Simpósio *"diritto ala riservatezza e la sua tutela penale"* – 5 a 7 de setembro de 1967 (COSTA JÚNIOR, 1970, p. 13).

No ano de 1969, o Pacto de São José da Costa Rica, reproduziu o texto da Declaração Universal dos Direitos do Homem, no art. 11. Novo marco pode ser visto em 1974, quando foi acrescido ao Código Penal italiano, o art. 615, que dispôs sobre a tutela da intimidade, a partir do momento em que vetou a filmagem ou a gravação de imagens referentes à vida privada (COSTA JÚNIOR, 1970, p. 13).

As previsões em documentos internacionais, serviram para fomentar a inclusão do direito à privacidade ao conjunto legislativo interno de diversos países, cujos textos passaram a prever a proteção à privacidade, inclusive no Brasil, conforme será estudado no próximo item.

### 1.3.1 Direito fundamental à privacidade na Constituição de 1988

Inexistia, no Brasil, antes da promulgação da Constituição Federal de 1988 a proteção da privacidade como um direito em si, notadamente porque as relações eram essencialmente patrimonialistas.

Vale lembrar que nos anos que antecedem a Constituição Federal de 1988, o país atravessava um duro período da história nacional, configurado pelo abuso e

desrespeito aos direitos fundamentais, a Ditadura Militar. Só houve mudança com a proclamação da Constituição da República Federativa do Brasil de 1988, que consagrou no art. 1º, inciso III, a dignidade da pessoa humana como um dos fundamentos da República (AGUIAR, 2003).

Durante os anos que a Ditatura esteve instalada, nem de longe os termos privacidade e direito à privacidade faziam algum sentido prático. Além da severa repressão do Estado, muitas famílias jamais puderam ter acesso às informações de entes desaparecidos por conta do sigilo imposto pelo governo à diversos documentos, sob a alegação de se que tratavam de informações de caráter privado.

O cenário histórico e a chegada da internet, com toda a sua complexidade, exigiram que a matéria se tornasse objeto de debate pelo poder constituinte. “Seria necessário dispensar maior proteção à pessoa, que foi anteriormente negligenciada pela ênfase dada ao patrimônio” (BIONI, 2019, p. 57). Além disto, a criação de normas tratando sobre privacidade justificava-se pelos riscos iminentes causados por emergentes mecanismos de escuta e captação de imagens por satélite, além de armazenamento de informações em bancos de dados privados como o Serasa.

Embora a história recente nos mostre a importância da defesa da privacidade como direito, no Brasil ela não possui legislação específica, contudo, conta com o *status* de direito fundamental, garantido pela Constituição Federal de 1988, que em seu art. 5º, inciso X, prevê:

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

Pode-se dizer que tanto os princípios quanto as regras constituem fundamentos para juízos concretos de “dever ser” e se formulam com a ajuda de expressões deônticas fundamentais, como mandamento, permissão e proibição (ALEXY, 1993, p. 83).

Em termos gerais, a Constituição Federal Brasileira de 1988 protege o direito à privacidade, como um direito da personalidade, compreendendo o sigilo de correspondência, comunicações telegráficas, telefônicas e de dados. Originariamente,

tal garantia foi expressa na Constituição como forma de proteção do indivíduo ante as arbitrariedades do Estado na condução de investigações, calcadas em fundamentos ideológicos como forma de manter governos autoritários (PINHEIRO, 2010, p. 12).

Os direitos fundamentais da privacidade e da inviolabilidade de sigilo de dados, são fundamentos da própria cidadania, o sigilo está ligado diretamente a segurança do cidadão, princípio cujo conteúdo valorativo diz respeito à exclusão do arbítrio, não só de parte da sociedade como sobretudo do Estado que só pode agir com observância da ordem normativa que o constitui. (FERRAZ JÚNIOR, 1993, p. 457).

Vale mencionar o entendimento da Ministra Rosa Weber, relatora da Ação Direta de Inconstitucionalidade nº 5.527, que em seu voto menciona que "[...] compreendida a privacidade, a conclusão inarredável é a de que, tanto quanto a ampla liberdade de expressão, a proteção da privacidade também é uma característica estrutural indispensável das sociedades democráticas" (BRASIL, STF, 2020).

Além da previsão constitucional, o Brasil ratificou tratados internacionais, bem como, conta com normas infraconstitucionais de proteção à privacidade como veremos a seguir.

### 1.3.2 Demais normativas nacionais de proteção à privacidade

As previsões infraconstitucionais nacionais de proteção à privacidade estão dispersas em leis e códigos, as principais são: o art. 21, do Código Civil de 2002, que prevê "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma"; o art. 3º inciso II[18], art. 7º, inciso I[19], art. 8º, [20]e art.11, §3º[21]

[18] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
[...]
II - proteção da privacidade;
[19] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
[20] Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
[21] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a

da Lei 12.965/2014, conhecida como Marco Civil da Internet e diversos artigos da recente Lei 13.709/2018, Lei Geral de Proteção de Dados.

Ainda, o Brasil ratificou instrumentos internacionais relacionados ao direito de privacidade, incluindo o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), promulgado pelo Decreto nº 592/1992, que em seu art. 17 estabelece que "ninguém será sujeito a interferências arbitrárias ou ilegais em sua privacidade, família, lar ou correspondência, nem a ataques ilegais à sua honra e reputação".

O Brasil também contribuiu na construção da Resolução 68/167[22] da Organização das Nações Unidas sobre o direito à privacidade na era digital, adotado pela Assembleia Geral em 18 de dezembro de 2013.

Vale ressaltar que a Resolução 68/167, o Marco Civil e a Lei Geral de Proteção de Dados serão tratadas no próximo capítulo deste trabalho.

Entendemos até aqui que a privacidade sofreu diferentes interpretações de acordo com as diferentes épocas do progresso da sociedade, desde a suas primeiras concepções, fundadas no direito de propriedade, até as mais recentes no sentido de proteção da personalidade humana e seus atributos; imagem, voz e dados pessoais.

Mas porque falar de privacidade hoje? Por que a necessidade de tratar de privacidade do ponto de vista de dados pessoais? Será que entendemos o nível de preocupação necessária com a privacidade no contexto digital em que vivemos? Nos próximos tópico trago alguns casos de significativa repercussão para reflexão.

### 1.4 Por que falar de privacidade?

Nas últimas décadas muito se discute sobre as vantagens do uso da tecnologia de sistemas baseados em algoritmos para a melhoria da comunicação, eficiência do consumo de serviços e produtos em geral. Como nem tudo são flores na era digital, o uso de algoritmos de forma não transparente, levanta

---

legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
[...]
§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

[22] Disponível em: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

preocupações em relação aos preceitos fundamentais previstos na nossa Constituição, principalmente o direito à privacidade.

Atualmente é possível obter imagens do quintal vizinho com detalhes tão aprimorados que permite distinguir entre uma casinha de cachorro e uma banheira de hidromassagem. Também é possível comprar fotos de alta resolução de prédios governamentais em países estrangeiros, navios-tanque de refugiados, um polêmico local de extração de madeira ou o pátio de produção de seu principal concorrente comercial do outro lado da cidade (PETERSEN, 2007, p. 3-6).

As novas tecnologias, principalmente aquelas que fazem uso de algoritmos, permitem diariamente novos e sofisticados mecanismos de ataque cibernético. Véliz (2020, p. 92) menciona que em 2015, mais de 30 milhões de pessoas tiveram seus dados pessoais expostos. Hackers divulgaram todo o banco de dados de um site que ajuda pessoas casadas a terem encontros amorosos. Mesmo usuários que cancelaram suas contas tiveram seus nomes, endereços, preferências e números de cartão de crédito vazados.

Shoshana Zuboff (2015, p. 83) afirma que "as pessoas esperam resultados de pesquisa e anúncios personalizados". A autora menciona que o Google procura ir além do atual “resultado de pesquisa” para saber e responder antes mesmo do usuário dizer o que busca, o que é verdadeiramente preocupante, na medida em que não há qualquer regulamentação ou sanção sobre atividades como a do *Google* e os usuários têm pouco ou nenhum conhecimento das operações de negócios da empresa, ou como seus dados são instrumentalizados e monetizados por ela.

Devo tecer uma observação pessoal sobre os próximos tópicos, enquanto desenvolvi a pesquisa, ao conversar com pessoas de diversas áreas sobre meu tema, mas principalmente profissionais do direito, ao indagar: “você conhece o caso *Cambridge Analytica?”,* a maioria respondeu: “Já ouvi falar, mas não sei o que significa”. Após a explicação o que pude perceber é que mesmo pessoas com certo nível de instrução tiveram dificuldades em compreender a mecânica do caso e a relevância da questão nos debates sobre democracia, o que torna a discussão necessária.

Não cabe mais discutir se somos a favor ou contra as tecnologias de um modo geral, mas é necessário fomentar a discussão sobre os limites de seu uso. Não são os dados em si o grande desafio, porque eles existem independentemente

de sua exploração, mas sim, como eles são utilizados e em qual medida isso pode caracterizar malefícios ou benefícios para o indivíduo e a sociedade.

A seguir, este estudo traz um panorama sobre dois elementos essenciais da atualidade, a Internet e as redes sociais.

### 1.4.1 Eis que surge a Internet e as redes sociais

Criada durante a Guerra Fria e desenvolvida para comunicação acadêmica entre os anos de 1970 e 1980, foi principalmente na década de 90 que a Internet alcançou o grande público (FIORILLO, 2015, p. 148).

De acordo com a Agência Nacional de Telecomunicações (ANATEL, 1995), 'Internet' é um nome genérico para um grupo de redes, meios de transmissão e comutação, roteadores, equipamentos e protocolos todos com necessidade de uma conexão em um computador.

O Ministério da Ciência e Tecnologia (1996) define Internet como "um conjunto de redes interligadas, de abrangência mundial" (MCT, 1996, p. 1), que foi uma menção na época a funções como o "[...] correio eletrônico, transferência de arquivos, acesso remoto aos computadores, acesso à base de dados e diversas categorias de serviços de informação [...]" (MCT, 1996, p. 1).

Existem diversos conceitos para definir 'Internet', é tarefa impossível relacionar todos diante das diferentes abordagens. Merece destaque o conceito de Esther Morón Lerma (1999, p. 2), que a define como "uma amálgama de milhares de redes de computadores que conectam entre si milhões de pessoas". Na mesma linha de interpretação de Pedro Alberto de Miguel Asensio (2001, p. 27) constata que a 'Internet" é um meio para comunicação global constituído por "[...] um emaranhado mundial de redes conectadas entre si de modo a tornar possível a comunicação quase instantânea de qualquer usuário de uma dessas redes a outros situados em outras redes de conjunto [...]" (ASENSIO, 2001, p. 27).

De acordo com Paloma Llaneza González (2000, p. 36), "a 'Internet' não é uma entidade física ou tangível, mas sim uma rede que se conecta em inúmeros pequenos grupos de redes de usuários que de certa forma estão conectados entre si, se tornando assim uma rede de redes". Existem redes fechadas, que não se

interconectam com outros usuários, contudo, a grande maioria das redes está conectada a outras redes, que por sua vez estão conectadas a outras redes, permitindo ao usuário de qualquer uma delas a comunicação com usuários de quaisquer outras redes do sistema (GONZÁLEZ, 2000, p. 36).

A comunicação dentro dessa teia de redes é possível devido a uma linguagem chamada de TCP/IP uma sigla para *Transmission Control Protocol/Internet Protocol*, ou Protocolo de Console de Transmissão/Protocolo de Internet, que permite que diferentes computadores se comuniquem entre si e transmitam informações de linguagem, utilizando pacotes de dados (PASQUALE, 2016).

Sinteticamente, a Internet é o sistema global de redes de computadores interconectadas que usam o conjunto de protocolos para conectar dispositivos em qualquer parte do mundo. A Internet conecta redes privadas, públicas, acadêmicas, comerciais e governamentais, em âmbito local e global, através de uma ampla variedade de tecnologias de redes eletrônicas, sem fio e ópticas (PASQUALE, 2016).

Essa interconexão entre redes permitiu o surgimento das redes sociais virtuais, onde milhares de pessoas se conectam e compartilham informações sem qualquer interferência de barreiras geográficas. De acordo com Boyd e Herr (2007), em meados dos anos 1990 nos Estados Unidos surgiam os primeiros sites de relacionamento que posteriormente viriam a se tornar as chamadas redes sociais. A criação desses sites tinha como base vínculos diretos, estabelecidos entre colegas e conhecidos, como também relações indiretas, entre amigos de amigos e aqueles que eram apenas conhecidos. Os sites de relacionamento nesta época eram inspirados em duas pesquisas acadêmicas: o experimento sobre o “mundo pequeno” (S*mall Word*), realizado em 1967 pelo sociólogo e psicólogo estadunidense Stanley Milgram, que gerou a ideia dos “seis graus de separação”[23]; e o estudo de Mark Granovetter sobre a “força dos vínculos fracos”[24] (sobretudo nos contatos profissionais) (BOYD; HERR, 2007).

[23] A ideia dos “seis graus de separação” surgiu a partir de uma pesquisa realizada por Milgram com 160 pessoas, onde constatou que existem apenas seis graus de separação dividem dois grupos de pessoas, isso porque nas regras de sua pesquisa, cada pessoa recebia uma correspondência e deveria enviar para uma pessoa-alvo, porém, não poderia enviar para ela diretamente, devendo buscar amigos em comum, outros contatos, enfim, outros meios para que conseguisse chegar até ela. Durante essa pesquisa ele observou que cada pessoa precisava em média de seis atravessadores, antes de chegar ao seu destino final. A pesquisa de Milgram comprovou que as redes sociais de que as pessoas fazem parte podem ser relativamente maiores do que elas têm conhecimento. (LIMA, 2011).

[24] A teoria de Granovetter remete aos relacionamentos pessoais como apenas uma forma de competição entre os indivíduos, não havendo elementos emotivos nesses relacionamentos, havendo

No ano de 2002, as redes sociais se expandiram, Boyd e Herr (2007) mencionam que essa nova geração de comunicação e interação nasceu com o lançamento do site *Friendster*, onde os usuários construíam um perfil público e o associavam a outros perfis com quem possuíam algum tipo de proximidade na vida real, sendo conectados por uma rede de *hiperlinks*.

O *Friendster* alavancou, obtendo um número de usuários inesperado, segundo Boyd e Herr (2007) esse número atingiu 3,3 milhões de usuários em menos de 1 ano, com a maioria dos usuários com idade entre 20 e 30 anos. Contudo, com a demanda crescente de usuários os servidores não suportaram, limitando as possibilidades de conexões entre os integrantes, fator que abriu espaço no mercado para o surgimento de novas redes sociais. Assim, entre os anos de 2003 e 2005 diversos sites de relacionamento tomaram conta da Internet, surgindo nesse período o *Myspace, Orkut* e *Facebook*. Nas últimas décadas, outras redes sociais ficaram em destaque como o *Instagram, Twitter, LinkedIn* e mais recentemente o *ClubHouse*.

Em síntese as plataformas de redes sociais promovem a interação entre seus usuários, que se conhecem fisicamente ou não, distinguindo-se apenas pelos modelos de interação e propósitos.

As redes sociais consistem, de acordo com Marteleto (2001, p. 72), em "[...] um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados". Para Costa et. al. (2003, p. 73) rede social "é uma forma de organização caracterizada fundamentalmente pela sua horizontalidade, isto é, pelo modo de inter-relacionar os elementos sem hierarquia".

Para Castells (2003, p. 565) "redes constituem a nova morfologia social de nossas sociedades e a difusão da lógica de redes modifica [...] processos produtivos e de experiência, poder e cultura". Machado e Tijiboy (2005, p. 3) complementam afirmando que "essa forma de organização vem conquistando novos espaços e formas de agir baseadas na colaboração e cooperação entre os segmentos envolvidos".

Com o aprimoramento e popularização do acesso à internet, a interação entre indivíduos toma outros rumos. Diversos sites são alimentados a partir da participação de seus usuários, como a Wikipédia por exemplo, não é necessário conhecimento acadêmico ou comprovações científicas sobre o que é disponibilizado ali. Fundado na

---

apenas valor, medido em termos de possibilidade de alcance do interesse individual. O autor destaca que tudo é permitido quando se tem a frente a busca por interesses pessoais. (FURTADO, 2008).

ideia de melhorar o trânsito, o aplicativo de navegação *Waze* é alimentado pelos usuários que reportam acidentes, congestionamentos e locais perigosos. Na Grã-Bretanha site chamado *Internet Eyes*, permite aos usuários, por meio do computador pessoal, monitorar circuitos de segurança de vídeo e notificar diretamente os proprietários das câmeras nos casos de cenas suspeitas ou quando visualizarem crimes ocorrendo (BRUNO, 2013, p. 136).

Silveira (2019, p.74-76) menciona que as redes sociais, ainda que de natureza privada, se tornaram espaços de articulações de opiniões, onde “ocorrem importantes debates públicos”. Nesse contexto, sistemas baseados em algoritmos selecionam o público, influenciam a formação de opiniões e captam dados. Quanto maior o número de clientes de uma plataforma de uma rede social mais valiosa ela se torna, em razão dos inúmeros dados e informações que esses usuários geram.

Por outro lado, as redes sociais representam muito mais do que meros mecanismos de interação, na medida em que se tornaram verdadeiros mecanismos de vigilância. Fernanda Bruno (2013, p. 9) aponta que estruturas tecnológicas, como plataformas e redes sociais, potencializaram as formas individuais de comunicação e expressão, mas, por outro lado, mecanismos de monitoramento, captura, rastreamento e categorização de dados cresceram na mesma proporção, para “alimentar estratégias de publicidade, segurança, desenvolvimento de serviços e aplicativos [...]” (BRUNO, 2013, p. 9).

Atualmente somos altamente “vigiados” por diversas instituições que trabalham com captação de dados pessoais em meios eletrônicos para uso preponderantemente comercial e de vigilância. Essas empresas se utilizam de dispositivos que permitem o monitoramento permanente do comportamento e preferências dos usuários, de forma individual ou coletiva, como veremos nos casos descritos a seguir. Vale destacar que o tema “captação de dados e seus desdobramentos” será retomado e aprofundado no terceiro capítulo do trabalho.

### 1.4.2 O caso Snowden

Após os ataques de 11 de setembro de 2001, as questões de segurança se tornaram prioritárias para os EUA, nessa época, o presidente George W. Bush

sancionou o *USA Patriot Act*[25], que deu ao governo verdadeiros poderes de vigilância, fundamentados no combate às ações terroristas.

A Agência de Segurança, autorizada pelo presidente Bush, implementou um programa de coleta em massa de registros domésticos de telefone, internet e e-mail (GREENWALD, 2013). Não existiam informações públicas disponíveis sobre a coleta, tampouco, quem seria o alvo dessa captura até 2013, ano em que vazaram documentos da Agência de Segurança Nacional (NSA)[26]. Esses documentos revelaram espionagem de alto nível sobre cidadãos comuns do mundo todo.

O livro escrito por Glenn Greenwald[27], originalmente intitulado "*No Place to Hide*"[28], narra a história de uma das maiores denúncias sobre uso de dados pessoais em massa para fins de vigilância realizado pelo governo dos Estados Unidos. Para entender o tamanho da problemática, é apresentado um resumo do que aconteceu nesse caso.

O responsável pelo vazamento do caso é Edward Snowden, que trabalhava há alguns anos para a *Central Intelligence Agency* (CIA) e saiu da agência em 2009, quando passou a atuar para empresas privadas de tecnologia, que prestavam serviços para a NSA. No início de 2013, foi contratado como administrador de

---

[25] Sobre o *Patriot Act*: https://www.justice.gov/archive/ll/highlights.htm.

[26] De acordo com a página da NSA: The National Security Agency (NSA) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations in order to gain a decision advantage for the nation and our allies under all circumstances. The Central Security Service (CSS), part of NSA, provides timely and accurate cryptologic support, knowledge, and assistance to the military cryptologic community. CSS coordinates and develops policy and guidance on the SIGINT and IA missions of NSA/CSS to ensure military integration. A National Security Agency (NSA) lidera o governo dos EUA em criptologia que abrange produtos e serviços de Signals Intelligence (SIGINT) e Information Assurance (IA), e permite operações de rede de computadores a fim de obter uma vantagem de decisão para a nação e nossos aliados sob todas as circunstâncias. O Serviço de Segurança Central (CSS), parte da NSA, fornece suporte criptológico preciso e oportuno, conhecimento e assistência à comunidade criptológica militar. O CSS coordena e desenvolve políticas e orientações sobre as missões SIGINT e IA da NSA / CSS para garantir a integração militar. (Tradução livre) Fonte: https://www.intelligence.gov/index.php/how-the-ic-works/our-organizations/413-nsa.

[27] Glenn Greenwald, é jornalista, advogado constitucionalista, autor de quatro livros entre os mais vendidos do *New York Times* na seção de política e direito, e um dos três fundadores do The Intercept. Antes de fundar o Intercept, Glenn escrevia para o jornal britânico *The Guardian* e para o portal *Salon*. Por conta de suas reportagens sobre a NSA, recebeu o Prêmio George Polk de Reportagens sobre Segurança Nacional; o Prêmio de Jornalismo Investigativo e de Jornalismo Fiscalizador da Gannett Foundation; o Prêmio Esso de Excelência em Reportagens Investigativas no Brasil (foi o primeiro estrangeiro premiado) e o Prêmio de Pioneirismo da Electronic Frontier Foundation. Ao lado de Laura Poitras, a revista *Foreign Policy* o indicou como um dos 100 principais pensadores globais de 2013. As reportagens sobre a NSA para o jornal *The Guardian* receberam o Prêmio Pulitzer de 2014 na categoria Serviço Público. Texto adaptado. Fonte: https://theintercept.com/equipe/glenn-greenwald-brasil/

[28] Em português: Sem lugar para se esconder.

sistemas, na divisão localizada no Havaí, da *Bozz Allen Hamilton*, empresa que também presta serviços para a Agência de Segurança Nacional (SPANIOL, 2015).

Enquanto atuou na prestação de serviços para a NSA Snowden obteve acesso a documentos cujo conteúdo era relacionado às atividades de inteligência dos Estados Unidos. Com dados e documentos reunidos foi até Hong Kong, onde encontrou o jornalista Glenn Greenwald, com quem estava em contato há algum tempo, e a cineasta Laura Poitras, para conceder as entrevistas divulgadas posteriormente pelos jornais *The Guardian* e no *The Washington Post*[29] (HAAS, 2013).

Os arquivos de Snowden demonstram que a NSA controla telefones e dados de usuários, no mundo todo, com acesso aos servidores de empresas como *Google*, *Yahoo, Facebook*, *Skype* e *Apple;* o monitoramento seria parte do programa PRISM[30], que permitiu que a NSA, que atua principalmente no combate ao terrorismo, tivesse acesso direto a servidores de grandes empresas da Internet, o que possibilitou o monitoramento de comportamentos de usuários em escala mundial (GREENWALD, 2013).

Para Snowden, o governo dos Estado Unidos, por meio da NSA estaria construindo mecanismos que possibilitariam o acesso a todo tipo de informação, de qualquer pessoa no mundo, sem ciência prévia e sem possibilidade de controle (SPANIOL, 2015).

Como lembra Bruce Schneier (2015) muito do que se sabe a respeito da vigilância realizada pela NSA vem da denúncia de Edward Snowden, embora tenham ocorrido vazamentos da agência antes e depois dele, certamente esse foi o caso de maior repercussão e alvo de diversas discussões na medida em que se trata de denúncia grave e o alegado combate às ações terroristas nada mais é do que uma desculpa para a prática de um sistema de vigilância onipresente em clara violação à privacidade.

Como veremos a seguir não apenas o Estado promove a captação e uso de dados, a iniciativa privada também tem interesse na coleta de nossas informações, principalmente para criar um perfil digital dos usuários da Internet.

---

[29] Após a entrevista e matérias divulgadas, o governo dos EUA revogou o passaporte de Snowden acusando-o de ser espião. Atualmente ele mora na Rússia.

[30] Sigla para Métodos Sustentáveis de Integração de Projetos, o programa possibilita a coleta de histórico de navegação, download e transferência de arquivos, conteúdo de e-mails e conversas.

### 1.4.3 *Cambridge Analytica*

No ano de 2004, nos Estados Unidos, foi criado o *Facebook*, mais precisamente dentro da Universidade de *Harvard*, por Mark Zuckerberg e outros três amigos, dentre os quais um brasileiro, Eduardo Saverin. Em 2010 o *Facebook* foi tido como a rede social mais visitada, superando até mesmo o Google que possuía a marca de maior número de visitas até então. O *Facebook* permite criar um perfil que inclui dados pessoais e profissionais, à escolha do dono, compartilhar ideias, notícias, divulgar fotos, produtos, estabelecer contato, e ainda, gerar discussões a respeito de variados assuntos (MARTINEZ, 2010).

O psicólogo russo-americano Alexandr Kogan, professor da Universidade de Cambridge, desenvolveu um aplicativo para acessar informações pessoais de usuários em redes sociais para supostos fins acadêmicos. "*This is your digital life*"[31] é o nome do aplicativo com o qual foram coletados dados como: sexo, localização geográfica, redes de amigos e curtidas*,* de mais de 50 milhões de usuários do *Facebook*. Destes, apenas 270.000 deram o seu consentimento para uso desses dados para fins acadêmicos, em troca de uma compensação financeira. Todos os outros usuários faziam parte da rede de amigos de Kogan e sua empresa, a *Global Science Research* (GSR), os dados desses amigos foram acessados sem o consentimento (REASON WHY, 2018).

O número de usuários cujos dados foram captados representa um terço dos usuários ativos do *Facebook* nos EUA e quase um quarto dos possíveis eleitores das eleições de 2016 (REASON WHY, 2018). Posteriormente, Kogan compartilhou esses dados com a *Cambridge Analytica*, uma empresa contratada para trabalhar na campanha eleitoral do candidato à presidência dos Estados Unidos, Donald Trump.

De posse das informações a *Cambridge Analytica*[32], com uso de algoritmos, criou um perfil político dos usuários, para direcionar as mensagens da campanha de acordo com os interesses de cada *profile*, possibilitando a comunicação assertiva com um maior número de eleitores, o que, consequentemente geraria um número maior de votos ao candidato Donald Trump.

---

[31] Esta é a sua vida digital (Tradução Livre).
[32] Empresa de mineração e análise de dados para estratégias de comunicação segmentada. Fonte: https://cambridgeanalytica.org/.

Para Silveira (2019, p. 80) a plataforma *Facebook* possui verdadeira força de manipulação de massas, o autor afirma que “Com mais da metade dos eleitores de um país democrático utilizando diariamente a plataforma para obter informações, interagir e apoiar ou criticar as forças políticas, o *Facebook* tornou-se um dos principais componentes do jogo democrático.”

As informações e dados gerados pelo comportamento no uso da rede social interessa à política e ao mercado de marketing, na medida em que possibilitam traçar perfis de consumo e ideológicos dos usuários.

De acordo com a política de privacidade do *Facebook* ao criar uma conta, os usuários aceitam que a empresa realize a coleta de dados como comunicações, acesso a câmera, conteúdo visualizado, agenda de contatos registros de chamadas, histórico de SMS. Os dados são usados para “fornecer e viabilizar a operação dos Produtos do *Facebook* e serviços relacionados”. Os termos indicam que o *Facebook* compartilha dados com aplicativos e sites de terceiros integrado à sua plataforma[33], exatamente o que aconteceu com o aplicativo desenvolvido por Alexandr Kogan e a *Cambridge Analytica* (BELL, 2016).

O uso dos dados pela *Cambridge Analytica*, obrigou o criador do *Facebook*, Mark Zuckerberg, a prestar esclarecimentos pessoalmente perante o Congresso Nacional dos Estados Unidos[34]. Em declaração oficial o criador da rede social, se declarou responsável pelo que acontece dentro da plataforma: [...] But it's clear now that we didn't do enough to prevent these tools from being used for harm, as well. And that goes for fake news, for foreign interference in elections, and hate speech, as well as developers and data privacy[35].

Zuckerberg afirmou que eventos, como os que envolveram a plataforma, não devem mais ocorrer e que pretende converter a experiência em aprendizado para tornar o *Facebook* mais seguro: “[...] We didn't take a broad enough view of our

---

[33] Sobre o compartilhamento com terceiros a Política de Privacidade do Facebook é extremamente genérica. “Trabalhamos com parceiros externos que nos ajudam a fornecer e a aprimorar nossos Produtos ou que usam as Ferramentas de Negócios do Facebook para ampliar os negócios, o que possibilita a operação de nossas empresas e o fornecimento de serviços gratuitos para pessoas do mundo inteiro. Não vendemos nenhuma de suas informações para ninguém e jamais o faremos. Também impomos fortes restrições sobre como nossos parceiros podem usar e divulgar os dados que fornecemos.” Disponível em: https://pt-br.facebook.com/privacy/explanation.

[34] A audiência está transcrita na íntegra em: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/.

[35] Mas está claro agora que não fizemos o suficiente para evitar que essas ferramentas fossem usadas para causar danos também. E isso vale para notícias falsas, para interferência estrangeira em eleições e discurso de ódio, bem como para desenvolvedores e privacidade de dados. (Tradução livre).

responsibility, and that was a big mistake. And it was my mistake. And I'm sorry. I started *Facebook*, I run it, and I'm responsible for what happens here".[36] Todavia, na prática, a privacidade dos usuários do *Facebook* ainda parece ser violada, na medida em que os usuários desconhecem efetivamente como seus são utilizados.

A partir do ocorrido foi possível verificar uma mudança na postura da empresa em relação ao compartilhamento de dados. As configurações de privacidade[37] do *Facebook* foram alteradas; os usuários podem baixar todo o histórico de sua atividade *online* e regular suas configurações de privacidade de forma flexível.

Contudo, de um modo geral, parece que as empresas pretendem manter o *status quo* "dados em troca de conveniência", apenas oferecendo aos clientes um novo acordo com o qual eles podem concordar ou não, mas sem a oportunidade de exercer uma influência real sobre ele.

O escândalo em torno da *Cambridge Analytica* mostrou que redes sociais são sistemas absolutamente não transparentes, onde as configurações de privacidade padrão permitem o acesso a grandes quantidades de dados que se tornaram a mercadoria mais valiosa da atualidade.

Embora não tenham ocorrido no Brasil, os casos apresentados servem de exemplo de que tanto o poder Estatal, quanto empresas privadas, têm interesse em nossos dados. Como vimos, os mecanismos de captação e uso de informações não são claros, na grande maioria das vezes não é possível optar por não cedê-los, na medida que eles são recolhidos sem nosso conhecimento, ou seja, perdemos o controle sobre nossas informações.

Considerando o conceito de privacidade definido no início do capítulo, as práticas descritas nos casos caracterizam uma verdadeira violação à privacidade.

Não é necessário debater a privacidade como o direito à defesa dos recintos particulares ou do uso de imagem e de voz, porque esses temas já se encontram sedimentados nas normas, na doutrina e nas decisões judiciais.

A era digital possibilitou novas engrenagens de violação à privacidade por meio do uso de dados. Pensando nesse cenário que o próximo capítulo debate o direito à proteção de dados como um dos mecanismos de defesa do direito à privacidade.

---

[36] Não tivemos uma visão ampla o suficiente de nossa responsabilidade, e isso foi um grande erro. E foi meu erro. E eu sinto muito. Eu comecei o Facebook, eu o administro e sou responsável pelo que acontece aqui. (Tradução livre)

[37] Disponível em: https://pt-br.facebook.com/policy.php

## CAPÍTULO II – PROTEÇÃO DE DADOS E O DIREITO FUNDAMENTAL À PRIVACIDADE

As últimas décadas foram marcadas por um progresso tecnológico sem precedentes, a Internet se tornou indispensável frente aos inúmeros benefícios nos mais diversos setores, sejam governamentais ou privados. Nunca se acumulou tantos dados pessoais sobre os cidadãos (VÉLIZ, 2020, p. 208). Computadores, celulares, *smart watch*, assistentes digitais, carros e aparelhos conectados *full time* à internet, gerando e captando dados em tempo real, muitos deles de extrema importância e sigilo, como dados pessoais, cadastrais e patrimoniais, o que evidencia que os usuários são cada vez inseridos em um ambiente de exposição.

Nesse contexto tecnológico a ideia de direito à privacidade no sentido de não ser incomodado, de ser “deixado só” não se mostra suficiente, surge a necessidade de se falar em proteção de dados pessoais como um dos mecanismos de proteção da privacidade. Danilo Doneda (2019) aponta que tratar da proteção de dados sob um viés binário “sigilo/abertura, público/privado” deixa de considerar “a complexidade do assunto”.

É inegável que os usuários de sistemas digitais não têm conhecimento da existência de múltiplos armazenamentos de dados pessoais, quem é capaz de acessá-los e como as informações são utilizadas, assim como não têm controle sobre o armazenamentos desses dados.

Do mesmo modo o potencial de violações à privacidade no meio virtual aumentou significativamente. A coleta e a manipulação de dados por meio cibernético, passou a configurar um risco que não se relaciona necessariamente com a exposição indevida de fatos da vida do indivíduo, mas sim com a possibilidade de uso de informações para finalidades diversas das inicialmente autorizadas, como a indução de consumo, ou até mesmo para fins que podem ser considerados ilícitos, como manipulação resultado de eleições.

O roubo de dados pode resultar em uma conta tão cara quanto o roubo de documentos (VÉLIZ, 2020, p. 208). Violações aos dados pessoais podem ocorrer de diversas formas; vazamento, comercialização, invasão e roubo são alguns exemplos. À medida que as ameaças se tornam cada vez mais sofisticadas, são necessárias salvaguardas reguladoras em resposta.

A chegada das redes sociais trouxe consigo uma hiper exposição de momentos pessoais, íntimos, de vulnerabilidade, de felicidade, há quem afirme que nesse contexto não existe privacidade, na medida em que os próprios usuários se expõem. No entanto, a percepção da privacidade como antiquada e socialmente retrógrada está errada, porque sua ausência impede o exercício de liberdades constitucionalmente protegidas, como a liberdade de escolha e a autodeterminação (COHEN, 2013, p. 1905).

Ademais, a privacidade deve ser vista de uma forma mais ampla, que vai além de um *post* em rede social. Todo o comportamento dos usuários da Internet tem sido mapeado, usado e monetizado sem conhecimento e autorização da grande maioria. Esse é cerne da discussão da privacidade pensada a partir do uso de dados, a escolha de expor um momento pessoal é individual e o usuário tem o direito de que tal fato não seja objeto de uso indevido.

Os casos trazidos no capítulo anterior demonstram a importância da proteção de dados através de normativas, esse tema é tratado no próximo tópico.

## 2.1 Primeiros passos do direito à proteção de dados

Entender o contexto normativo relacionado à privacidade de dados de modo mais completo, requer considerar a própria trajetória da sociedade tecnológica. A relevância da proteção de dados pessoais se dá principalmente no período pós-industrial tomando contornos próprios de acordo com os interesses da sociedade. Nesse cenário, surge a necessidade de abandonar o paradigma patrimonialista do direito à privacidade para estabelecer novos meios de tutelar os interesses da pessoa (DONEDA, 2019).

A tecnologia desempenhou um grande papel no desenho da privacidade como direito. Nova leis foram formuladas e ainda serão criadas em resposta às transformações da tecnologia que aumentam a coleta, disseminação e uso de informações pessoais. Bruno Bioni (2019, p. 118) menciona a necessidade de conciliar interesses econômicos e privacidade “[...] o desenvolvimento econômico e social havia sido redimensionado pela tecnologia da informação e era, especialmente, dependente dos dados pessoais dos cidadãos”.

Danilo Doneda (2019) aponta que o acesso à tecnologia pelo grande público e comércio descentralizou a guarda e processamento de dados de grandes centrais para periféricos individuais. Nesse sentido, o cenário legislativo precisou se adequar e essa realidade trazida pelos novos modelos de tratamento de dados. Segundo o autor: “Procurou-se promover o direito do cidadão ao acesso, correção e cancelamento de seus dados pessoais, reconhecendo-lhes o direito a delimitar sua utilização nos moldes de uma liberdade negativa” (DONEDA, 2019).

As primeiras normas sobre proteção de dados surgiram como resposta à preocupação com o desenvolvimento de sistemas de captação e processamento de informações, em sua maioria administrados pelo Estado. “Naquela época, a saída regulatória foi focar na própria tecnologia que deveria ser domesticada e orientada pelos valores democráticos” (BIONI, 2019, p. 114).

O Congresso dos Estados Unidos aprovou o *Privacy Act* em 1974, a referida lei estabelece as práticas de coleta, manutenção, uso e disseminação de informações sobre indivíduos mantidas em sistemas de registros por agências federais Norte Americanas. O *Privacy Act* permite o acesso e alteração das informações, como também proíbe a divulgação de dados sem o consentimento por escrito do indivíduo, a menos que a divulgação esteja prevista nas exceções, inclusive com sanções cíveis e penais em caso de violação dos dispositivos[38].

A Lei de Hesse, datada do ano de 1974 na Alemanha, é a primeira lei local relacionada a proteção de dados. Escrita a partir de diversos princípios a lei proíbe principalmente a coleta, guarda e uso de dados sem o consentimento do titular ou previsão normativa. O texto criou também uma autoridade - o Datenschutzbeauftrager, ou Comissário para controlar as questões de dados pessoais na relação com a administração pública. (DONEDA, 2019).

O art. 35 da Constituição de Portugal[39], aprovada em 1976, concede aos cidadãos o direito de tomar conhecimento de registos, solicitar informações sobre o uso dos dados e a retificação e atualização dos mesmos.

Vale destaque a Constituição Espanhola, de 1978, que trouxe em seu texto a limitação do uso da informática como mecanismo de defesa da intimidade pessoal e familiar:

[38] Disponível em: https://www.justice.gov/opcl/privacy-act-1974.
[39] Disponível em: https://www.parlamento.pt/parlamento/documents/crp1976.pdf

> Artículo 18
> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

A *OECD - Organization for Economic Cooperation and Development*, no ano de 1980 publicou as "Diretrizes sobre Proteção da Privacidade e o Fluxo Transnacional de Informações Pessoais"[40], estabelecendo as diretivas sobre proteção de dados e sobre o fluxo de informações entre países, proibindo a transferência de informações para jurisdições que não possuam amparo de proteção.

Em segundo momento, amplia-se a preocupação com o uso de dados pela iniciativa privada, na medida em que se percebe a impossibilidade do Estado regular e controlar bancos de dados (BIONI, 2019, p. 115). Surgem então, leis direcionadas tanto para o setor privado e para o próprio titular dos dados.

Na Austrália a Lei de Privacidade data do ano de 1988, é direcionada tanto para o setor público quanto para o setor privado. A lei é fundamentada nos 13 Princípios Australianos de Privacidade (APPs, ou Australian Privacy Principles), que tratam sobre o uso e divulgação de dados, direitos do titular, preservação da qualidade dos dados, transparência e anonimidade.

A partir dos anos 90 a expansão da tecnologia como meio global de informação e comunicação e a ascensão da indústria de banco de dados levaram a uma onda de intervenções legislativas e regulatórias em diversos países destinadas a lidar com problemas emergentes de privacidade[41] (GASSER, 2016, p. 62).

Na União Europeia, a Diretiva 95/46/EC[42], que trata de processamento de dados pessoais foi aprovada em 1995, embora sua vigência tenha iniciado três anos mais tarde. O texto traz diversas determinações para os membros da União Europeia, como a obrigação de edição de leis em matéria de processamento de dados e a criação de uma agência ou a nomeação de comissário de proteção de dados em cada um dos países da UE.

---

[40] Disponível em: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM
[41] Revisão das Diretrizes de Privacidade da OCDE; Regulamento Geral de Proteção de Dados na EU e Lei de Direitos de Privacidade do Consumidor nos Estados Unidos, são exemplos.
[42] Disponível em: https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=CELEX:31995L0046

Cabe destacar também a *Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet* (Hadopi)[43], lei francesa de proteção de direitos na Internet que entrou em vigor no ano de 2010. A Lei Hadopi, como é conhecida, é destinada à proteção de obras criativas e aos direitos autorais, visando diretamente a repressão e o combate à pirataria, cópia e utilização não autorizada de obras.

A Lei Hadopi adotou o procedimento chamado de *three strikes*, que trata da notificação do usuário por três vezes, em caso de reincidência, o usuário pode ter o acesso à internet suspenso. Aqui vale destacar que, para que a lei possa ser praticada como previsto, os controladores da infraestrutura de rede ficam incumbidos do dever de monitoração e controle das atividades de seus usuários, instalando programas de filtragem de conteúdo, o que gera polêmicas em relação à invasão da privacidade dos cidadãos (PEREIRA, 2010).

Tércio Sampaio Ferraz Júnior (1993, p. 445) afirma que a inviolabilidade do sigilo de dados como premissa do direito à privacidade não significa que o Estado é impedido de exercer sua autoridade fiscal, sendo o acesso aos dados permitido, desde que não haja interceptação da comunicação. Em suas palavras:

> A inviolabilidade do sigilo, não sendo faculdade exclusiva da privacidade (é também da segurança da sociedade e do Estado), é *conditio sine qua non* (condição), mas não é conditio *per quam* (causa) do direito fundamental à privacidade. Ou seja, se não houver inviolabilidade do sigilo não há privacidade, mas se houver inviolabilidade do sigilo isto não significa que haja privacidade (pode haver outra coisa, como a segurança do Estado ou da sociedade). O direito à privacidade, em consequência, sendo um fundamento em si mesmo, permite dizer que a privacidade de um indivíduo só se limita pela privacidade de outro indivíduo (como a liberdade de um só encontra limite na liberdade do outro) (FERRAZ JÚNIOR, 1993, p. 445).

Pela percepção de Tércio Sampaio Ferraz Júnior a quebra do sigilo dos dados pela Lei Hadopi é possível pela proteção de direitos autorais, a partir da Teoria do Sopesamento[44]. Porém, na prática a lei pode se revelar um verdadeiro estado de vigilância diante do monitoramento excessivo dos usuários, em outras palavras, invasão de privacidade.

---

[43] Alta Autoridade para a Difusão de Obras e a Proteção dos Direitos na Internet. (Tradução livre)

[44] A lei do sopesamento é formulada por Robert Alexy nos seguintes termos: “quanto maior for o grau de não satisfação ou de afetação de um princípio, tanto maior terá que ser a importância da satisfação do outro”, ou seja, a medida permitida de não satisfação ou de afetação de um princípio depende do grau de importância da satisfação do outro. Dito de modo mais simples, o que se perde de um lado deve ser compensado pelo que se ganha do outro. (LEONARDI, 2011, p. 106)

Conforme já citado, o Brasil e a Alemanha são os responsáveis pela redação da Resolução 68/167 aprovada em 18 de dezembro de 2014 pela Assembleia Geral da ONU, o texto foi inspirado no Marco Civil da Internet, lei brasileira. O Comissão que aprovou a Resolução demonstra a preocupação com a proteção da privacidade na era tecnológica, notadamente quanto às questões relacionadas ao abuso de direito e vigilância por parte dos Estados. De acordo com o documento:

> Noting that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern[45], [...] (ONU, 2014)

O texto ainda discorre sobre a necessidade da implementação efetiva de medidas para a defesa do direito à privacidade, principalmente direcionadas à prevenção de violações dos direitos humanos, inclusive em ambiente digital e prevenção aos mecanismos de vigilância. Com essa perspectiva chama os Estados para que promovam a revisão das suas legislações e das práticas relacionadas à coleta de dados pessoais (ONU, 2014).

No Brasil, a primeira lei de âmbito nacional[46] que trata especificamente sobre dados é a Lei nº 7.232/1984[47] – denominada de Lei da informática, que assim dispõe no art. 2º, inciso VIII:

> Art. 2º A Política Nacional de Informática tem por objetivo a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira, atendidos os seguintes princípios:
> [...]

---

[45] Observando que o rápido ritmo de desenvolvimento tecnológico permite que todos os indivíduos em todo o mundo para usar novas tecnologias de informação e comunicação e no ao mesmo tempo, aumenta a capacidade de governos, empresas e indivíduos de realizar vigilância, interceptação e coleta de dados, o que pode violar ou abusar direitos humanos, em particular o direito à privacidade, conforme estabelecido no artigo 12 do Declaração Universal dos Direitos Humanos e artigo 17 do Pacto Internacionais sobre Direitos Civis e Políticos e, portanto, é uma questão de crescente preocupação, [...] Tradução livre.

[46] Os Estados do Rio de Janeiro e de São Paulo editaram as primeiras leis estaduais sobre proteção de dados: a Lei Estadual nº 824/1984 do Rio de Janeiro, que "Assegura o direito de obtenção de informações pessoais contidas em bancos de dados operando no Estado do Rio de Janeiro e dá outras providências"; e São Paulo, a Lei Estadual nº. 5702/1987, que "Concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa".

[47] Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L7232.htm.

> VIII - estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas; [...]

Conforme já mencionado, nossa Carta Maior prevê o direito à privacidade (art. 5º, inciso X) e à inviolabilidade do sigilo de comunicações, de dados e comunicações telefônicas (art. 5º, inciso XII), prevendo inclusive a garantia de acesso a informações pessoais, e de retificação de dados, constantes de bancos de dados públicos por meio do Habeas Data[48] (art. 5º, inciso LXXII[49]).

O Código de Defesa do Consumidor, Lei n.º 8.078/1990, prevê especificamente em seu art. 43 o direito ao acesso, transparência das informações e correção de dados:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (BRASIL, 1990)

Por sua vez, o Código Civil do ano de 2002 também traz disposições relativas à proteção da imagem e intimidade no art. 20 e art. 21. Apesar de os dados pessoais não serem abordados de forma explícita, é possível dizer que se relacionam com a

---

[48] Regulado pela Lei nº 9.507 de 1997.

[49] LXXII - conceder-se-á *habeas data:*
a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

proteção do Código Civil, especialmente porque ele regula a exposição de características – que muitas vezes poderão ser expressas por meio dos dados pessoais – sem a autorização do indivíduo.

No âmbito interno vale mencionar ainda a Lei do Cadastro Positivo, Lei nº 12.414 de 2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

Em maio de 2018, a Diretiva 95/46/CE foi substituída pelo Regulamento n° 2016/679, a nova Lei Geral de Proteção de Dados da União Europeia, mais conhecida como General Data Protection Regulation ou GDPR.

A GDPR entrou em vigor em 25 de maio de 2018, ao mesmo tempo em que mantém a abordagem regulatória geral da Diretiva 95/46/CE, a GDPR apresenta uma série de novas obrigações de conformidade, incluindo sanções mais elevadas do que as anteriormente previstas.

O Regulamento mudou a sistemática que coordena a aplicação da normativa sobre o tema no espaço jurídico europeu, dado que o GDPR, normativa comunitária, é diretamente aplicável em todos os países-membros da União Europeia, não sendo necessária a transposição de seus termos para o direito interno de cada jurisdição. (DONEDA, 2019).

O legislador da GDPR optou por manter a normativa baseada em princípios e direitos, ou seja, para manter seu amplo escopo, a GDPR utiliza princípios gerais a partir dos quais a conformidade deve ser deduzida no processamento dados. Significa dizer que as organizações devem avaliar suas operações e implementar as medidas necessárias para cumprir a lei de forma contínua, garantindo que o nível de conformidade seja proporcional ao nível de risco inerente às operações de processamento. Um dos princípios inovadores trazidos pela GDPR é o princípio da responsabilidade, que exige que as entidades que processam dados pessoais assumam uma postura proativa em relação ao cumprimento da lei.

Contudo, o regulamento contém cláusulas que permitem aos Estados-Membros tomarem decisões sobre a implementação da GDPR, o que pode levar a uma fragmentação de regras na aplicação interna.

A preocupação com a proteção de dados está diretamente relacionada ao contexto da evolução tecnológica, desde a chegada da imprensa e da fotografia, nessa época a preocupação primordial era em relação ao uso de imagens não

autorizada e a legislação da época reflete a ideia de proteção à privacidade. Com a chegada da Internet e o uso de dados para controle de cidadãos pelo Estado e iniciativa privada, a legislação evolui no sentido de proteger o cidadão do abuso estatal. Em mais um passo da era digital surgem os telefones celulares e com eles milhões de dados dos usuários passam a ser captados e monetizados para fins comerciais. Nesse cenário a legislação busca regrar o uso dos dados, contudo a raiz dessas normativas continua sendo a proteção da privacidade do indivíduo.

Nos próximos itens duas leis importantes relacionadas à proteção de dados serão apresentadas; o Marco Civil da Internet e a Lei Geral de Proteção de Dados.

## 2.2 O Marco Civil da Internet

A preocupação com os riscos decorrentes da ausência de uma normativa de regulamentação do uso da Internet no Brasil, movimentou o legislativo para a edição da Lei 12.965/2014. Inegavelmente um panorama de insegurança jurídica não é algo que contribui para a sociedade como um todo e tampouco ao desenvolvimento da Internet no Brasil (LIMA, 2010, p. 40).

O Marco Civil da Internet foi discutido e elaborado de forma aberta e publicado no Diário Oficial da União de 24 de abril de 2014, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no Brasil. Entrou em vigor em junho de 2014, decorridos 60 dias da sua publicação oficial (PINHEIRO, 2010, p. 41).

A Lei 12.965/014 trouxe diversas inovações, dentre as quais a mais importante para o presente estudo; o princípio da proteção de dados pessoais na Internet (art. 3, III[50]). Até o implemento da lei, os dados eram coletados e tratados quase que instantaneamente, sem limitações expressas, porém, com a inovação legal, as informações dos usuários não podem ser usadas para um fim diverso daquele para o qual foram fornecidas (PINHEIRO, 2010, p. 45).

O mesmo artigo que reconhece a proteção de dados pessoais como um princípio indica que sua proteção deve se dar nos termos da lei (art. 3º, III), ou seja,

[50] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
[...]
III - proteção dos dados pessoais, na forma da lei;

faz referência à criação de uma lei específica para tratamento dos dados pessoais, deixando evidente que não foi intuito do legislador esgotar o tema.

O Marco Civil, traz diversas previsões dirigidas aos provedores de internet. O art. 7º, inciso VII, determina que desde que haja consentimento livre, expresso e informado do usuário, o provedor poderá fornecer a terceiros os seus dados pessoais, registros de conexão e de acesso a aplicações de internet. A lei institui ainda, que os contratos deverão conter, de forma destacada das demais cláusulas, o consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais dos usuários (art. 7º, IX). Para além, o provedor da conexão deverá guardar sigilosamente os registros de conexões, em ambiente controlado e seguro, pelo prazo de um ano, não podendo transferir a responsabilidade para terceiro. Em ambos os casos uma ordem judicial poderá determinar a guarda dos dados por período maior do que o estipulado em lei (art. 13 e art. 15).

Os provedores de aplicativos da internet (aqueles que oferecem qualquer tipo de funcionalidade a seus usuários através da Internet, como redes sociais, sites de comércio eletrônico etc.) devem armazenar registros de acesso por pelo menos seis meses. Nesses casos, os *logs* de acesso devem incluir a data, hora e duração das conexões com o aplicativo da Internet feitas por um determinado endereço IP (PASQUALE, 2016)

Para compatibilizar princípios normativos vigentes, garantindo o exercício do direito fundamental à liberdade de expressão e impedir mecanismos de censura, o Marco Civil prevê, em seu art. 18 que o provedor não será responsabilizado civilmente por danos decorrentes de conteúdo gerados por terceiros. Contudo, essa isenção de responsabilidade encontra um limitador, previsto no art. 19, que determina que o provedor poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial, não tomar as medidas necessárias para tornar indisponível o conteúdo indicado como infringente.

Ao julgar um caso de ofensas em página de rede social, o Superior Tribunal de Justiça apontou que:

> “A internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e infenso à responsabilidade pelos abusos que lá venham a ocorrer. [...] No mundo real, como no virtual, o valor da dignidade da pessoa humana é um só, pois nem o meio em que os agressores transitam nem as ferramentas tecnológicas que utilizam conseguem transmudar ou

> enfraquecer a natureza de sobre princípio irrenunciável, intransferível e imprescritível que lhe confere o Direito brasileiro" (BRASIL, STJ, 2010)

Stefano Rodotá (2008, p. 74-75) lembra da importância de compatibilizar os princípios constitucionais. Para o autor, a liberdade de expressão é condição para a proteção e desenvolvimento da personalidade e o princípio da liberdade constitucional consubstancia-se em liberdade de exercício da vida privada.

Em síntese o Marco Civil da Internet, buscou preservar o equilíbrio entre direitos e garantias de usuários e provedores de internet definindo regras e princípios. Considerando que não havia qualquer normativa relacionada diretamente à proteção de dados no Brasil, a Lei 12.965/2014 representa importante avanço.

## 2.3 Lei Geral de Proteção de Dados

O valor comercial dos dados pessoais levou a maioria das empresas adotar uma mentalidade de "colete primeiro, pergunte depois" (HARTZOG, 2018, p. 5). É nesse cenário que a Lei Geral de Proteção de Dados surgiu, no Brasil, apesar de alguns pontos negativos, ela traz uma série de inovações relacionadas ao tratamento dos dados e proteção à privacidade.

A recente Lei nº 13.709/2018, ou LGPD, como ficou conhecida, estabelece regras para a coleta, uso, processamento e armazenamento de dados pessoais no Brasil. Com forte influência das normativas sobre proteção de dados da Comunidade Europeia, a LGPD estabelece diversos direitos fundamentais relacionados à tutela dos dados pessoais (art. 2º, VII[51]).

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das

[51] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

> informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis (PINHEIRO, 2018).

Conforme determina o art. 3º, a Lei é aplicável a qualquer atividade de processamento de dados pessoais realizada por pessoa física ou jurídica, independentemente dos meios de processamento e da localização da sede do processador, desde que o processamento seja realizado no Brasil, a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços localizados no território nacional, ou caso os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

A LGPD possui aplicação tanto no setor público quanto no privado. A norma traz o conceito de dados pessoais e a lista de situações que autorizam seu uso, além dos princípios gerais de proteção de dados e os direitos básicos dos titulares como direito de acesso, exclusão de dados e retificação, como também, as obrigações e limites aplicáveis ao tratamento de dados.

Em síntese, a LGPD traz um amplo leque de possibilidades para sua aplicação, justamente porque a tecnologia ampliou os modelos e meios de tratamento de dados pessoais, a ideia é reduzir lacunas para que nenhum agente possa alegar que não se encaixa na previsão normativa. Nesse sentido, qualquer agente que trata dados pessoais deverá observar a lei.

> A LGPD procurou harmonizar o direito dos titulares dos dados à privacidade e à autodeterminação informativa com o dinamismo de uma economia cuja matéria-prima são os dados. O ambiente de equilíbrio por ela estabelecido – que, fundamental remarcar, deve ser seguido tanto pelo poder público quanto pela iniciativa privada – prevê que o tratamento dos dados pessoais deve seguir diversos princípios básicos para ser justificável e legal. Deve, por exemplo, possuir finalidade específica, ser proporcional, ser realizado com segurança e de forma não discriminatória. Da mesma forma, o cidadão/titular dos dados possui uma série de direitos os quais pode invocar em caso de tratamento em desconformidade, como exigir correção, suspensão do tratamento, retirada ou revogação de aplicações e serviços. (NAZARENO; PINHEIRO, 2020, p. 13).

A atividade de processamento deve ser realizada com fundamento em bases legais, nesse rol incluem-se outras normativas legais, de acordo com as hipóteses previstas no art. 7º:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária:
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

No tocante ao consentimento, a LGPD impõe requisitos específicos: o consentimento deve ser prévio, informado e inequívoco. Para dados sensíveis, além desses requisitos, o consentimento deve ser específico e fornecido separadamente de outros consentimentos.

Vários outros direitos foram previstos aos titulares dos dados, como o direito de obter informações sobre o processamento de dados, o direito de acessar, retificar e apagar dados, o direito de retirar o consentimento, de receber informações sobre compartilhamento, o direito à portabilidade de dados e o direito de obter a revisão de decisões automatizadas.

A LGPD define duas categorias de agentes de tratamento de dados, os 'controladores' e 'operadores'. Inspirada na definição estabelecida no Regulamento Geral sobre a Proteção de Dados (GDPR), a LGPD define controladores como “pessoa física ou jurídica, pública ou privada, responsável pelas decisões relativas ao processamento de dados pessoais” e operadores como “pessoa física ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”.

Os agentes de processamento devem respeitar os princípios de processamento de dados estabelecidos na LGPD e adotar medidas técnicas e organizacionais para proteger os dados pessoais contra incidentes de dados. De acordo com a Lei, os controladores de dados devem: definir e documentar a base legal para o processamento de dados pessoais (registro de processamento); garantir a implementação de mecanismos para cumprir os direitos dos titulares de dados; relatar

violações de dados e incidentes de segurança ao Controle de Processamento de Dados e, em alguns casos, aos titulares de dados afetados; realizar avaliações de impacto na privacidade e nomear um responsável pela proteção de dados, encarregado de lidar com dados pessoais dentro da organização.

Além disso, os controladores de dados devem disponibilizar ao titular um aviso de privacidade claro e detalhado sobre os objetivos do processamento de dados; sua forma e duração; contato do controlador; informações sobre eventuais compartilhamentos; responsabilidades dos agentes de processamento e direitos dos titulares dos dados.

Se o aviso de privacidade for redigido de forma a reduzir significativamente os direitos de privacidade reconhecidos por lei, é possível que seja considerado inválido. Mesmo antes da LGPD, os tribunais brasileiros têm derrubado sistematicamente as disposições de aviso de privacidade que implicam uma renúncia de todos ou substancialmente todos os direitos de privacidade de um indivíduo (PORTO, 2019).

Conforme O´Neil (2016) as organizações que processam dados pessoais devem observar os requisitos de cibersegurança impostos pela LGPD. Os controladores e processadores de dados devem adotar medidas técnicas e organizacionais para proteger os dados pessoais contra acesso não autorizado e contra destruição acidental ou ilegal, perda, alteração, comunicação, transmissão ou qualquer outra ocorrência resultante do processamento inadequado ou ilegal de dados (um incidente de dados). Exceto em circunstâncias limitadas, incidentes de dados podem acionar responsabilidades[52]. Pasquale (2016) destaca que a LGPD exige que os controladores e processadores de dados adotem medidas de proteção de dados desde a criação de qualquer nova tecnologia ou produto, o que exigirá que as organizações adotem uma abordagem de privacidade por *design*.

A LGPD surge no cenário brasileiro a partir de uma tendência mundial de novas legislações voltadas especificamente à proteção de dados, notadamente após diversos escândalos envolvendo grandes corporações e governos. Embora merecedora de destaque e elogios a normativa nacional deve ser constantemente debatida para fins de aprimoramento.

[52] O Código do Consumidor também estabelece que as empresas devem tomar todas as medidas razoáveis para oferecer produtos e serviços seguros e sem defeitos. Portanto, se a organização não implementar medidas de segurança apropriadas um produto ou serviço poderá ser considerado defeituoso.

### 2.3.1 Dados pessoais

Os dados pessoais e a sua análise jurídica ganharam relevância pela popularização de novos modelos de negócio que fazem uso deles para produzir e vender informações sobre usuários (MALDONADO; BLUM, 2019).

Um dado nada mais é do que um elemento em seu estado puro, ou seja, que ainda não passou por uma análise e interpretação. De acordo com Oliveira (2014, p. 36) “é qualquer elemento identificado em sua forma bruta que, por si só, não conduz a uma compreensão de determinado fato ou situação”.

É importante destacar que parte da doutrina faz uma diferenciação entre “dado” e “informação”. O conceito de dado não se liga à inteligibilidade do mesmo para um leitor, ou seja, é irrelevante a capacidade do leitor de certo dado de entender o mesmo, sendo esta uma operação intelectual posterior. Com efeito, para ser considerado dado, nem mesmo é necessário que qualquer pessoa saiba interpretá-los, como é o caso de algum escrito em uma língua já esquecida. No atual contexto, a estruturação de um banco de dados é o que possibilita seu processamento automatizado, por meio de computadores e suas diversas formas de sistemas (MALDONADO; BLUM, 2019).

Informação pode ser descrita como o resultado obtido da organização e análise dos dados. Setzer (2015, p. 1), entende que “Informação é uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que está na mente de alguém, representando algo significativo para essa pessoa”. Para o autor se trata de um conceito mais aberto do que o de “dado”. O processo informacional é intelectivo, posto que pressupõe um processo semântico entre significado e significante, dependendo, em larga escala da subjetividade daquele que recebe a informação para seu processamento. Ainda, ele destaca que a informação pode, ou não, pressupor o recebimento de dados. Ou seja, o processo de geração de informações pode decorrer da atribuição de um significado a um determinado dado ou, ainda, mediante percepção direta de fatos (SETZER, 2015).

Considerando os diversos entendimentos, percebe-se que as diferenças entre dados e informações são de caráter estrutural. Enquanto aqueles caracterizam-se como elemento sintático, ou seja, uma representação simbólica de algo real, estas

últimas são semânticas, ou seja, trata-se de um processo de atribuição de significado a um significante, sendo este simbólico ou não (SETZER, 2015).

Para Danilo Doneda (2010, p. 19) “dado” teria uma ideia de fragmento e primariedade, informação em “estado potencial”, uma espécie de “pré-informação”. Já informação, seria o resultado da cognição, depuração do dado.

A doutrina não apresenta um conceito unânime para os termos “dado” e “informação”, apontando as similitudes ou diferenças, para fins deste trabalho se reconhece a diferença entre ambos seguindo a linha de entendimento de Danilo Doneda. Entretanto, apenas para viabilizar a leitura do texto, considerando a inexistência de sinônimos adequados, os termos “dado” e “informação” poderão ser utilizados como sinônimos entre si, na medida em que o texto defende a proteção de dados e informações relacionadas ao seu titular.

A Lei Geral de Proteção de Dados traz a definição legal para dados, no “art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; [...]”.

A Diretiva 95/46/CE da União Europeia que trata da proteção de dados pessoais define dados pessoais como:

> (1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[53]

Para a Lei, é o vínculo entre o dado e o titular, que o torna um dado pessoal. Nesse sentido, Pierre Catala (1983, p. 20) afirma que ainda que o indivíduo não seja o criador da informação, se há nexo entre ambos ele é seu legítimo titular. Para o autor “Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade”. Nessa mesma linha Danilo Doneda (2010, p. 24) explica que “[...] o mecanismo pelo qual é possível caracterizar uma determinada informação como

[53] (1) ‘Dados pessoais’, qualquer informação relativa a uma pessoa singular identificada ou identificável (‘titular dos dados’); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos para o físico, fisiológico, identidade genética, mental, econômica, cultural ou social dessa pessoa física; (tradução livre).

pessoal: o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta".

De acordo com a LGPD os dados pessoais englobam uma outra categoria de dados, os chamados dados sensíveis, que são objeto de regras próprias, como veremos a seguir.

### 2.3.2 Dados Sensíveis

Para a Lei Geral de Proteção de Dados a definição de "dado sensível" é trazida no art. 5º, inciso II:

> [...] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...] (BRASIL, 2019).

Contudo, o termo "dado sensível" não é uma novidade no ordenamento jurídico brasileiro, a Lei nº 12.414/2011 - Lei do Cadastro Positivo, no art. 3º, § 3º, inciso II, determina que são proibidas as anotações em cadastros creditícios relacionadas a "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

Dados sensíveis significam qualquer informação relacionada a um titular que tratam de origem racial ou étnica, crenças religiosas, opiniões políticas, participação em sindicatos ou organizações religiosas, filosóficas ou políticas, saúde, vida sexual, genética ou biometria (POWLES; HODSON, 2017).

Nesse sentido, fica evidente que uma eventual violação de dados sensíveis é muito mais prejudicial e capaz de gerar graves consequências. A LGDP reflete essa preocupação na norma fazendo uma distinção entre dados pessoais e dados sensíveis impondo uma barra mais alta para permitir o processamento desse tipo de dados, a Lei traz uma seção sobre o tratamento de dados pessoais sensíveis, estabelecendo limitações específicas, bem como, determinando claramente a necessidade de consentimento para o uso dessa modalidade de dados.

Como exceção à regra do consentimento a LGPD possibilita o tratamento de dados classificados como sensíveis nas hipóteses previstas no art. 11. Caitlin Mulholland (2018, p. 168) lembra que nos casos previstos no art. 11 o consentimento seria dispensado em razão dos interesses públicos em detrimento dos interesses individuais, mesmo quando se trata de direitos fundamentais. A autora faz uma crítica importante a esta brecha da legislação mencionando que "[...] a proteção do conteúdo dos dados pessoais sensíveis é fundamental para o pleno exercício de Direitos Fundamentais, tais como os da igualdade, liberdade e privacidade" (MULHOLLAND, 2018, p. 168).

Para fins deste trabalho, dado e informação serão considerados como sinônimos, assim, independentemente de sua origem ou natureza de dado sensível, se dado ou informação estiverem relacionados a uma pessoa natural, serão considerados de forma igualitária.

Apresentadas as questões relacionadas aos dados, é necessário debater o tema autodeterminação informativa na medida em que o conceito está relacionado diretamente ao controle de dados e informações pessoais.

## 2.4 Autodeterminação informativa

O termo "autodeterminação informativa"[54] foi utilizado pela primeira vez em uma sentença do Tribunal Constitucional da Alemanha em 15 de novembro de 1993[55] em um caso cujo objeto era a Lei do Censo de 1983[56]. A lei foi criada com o intuito de preencher o cadastro dos cidadãos alemães existente nos órgãos da administração pública, captando dados sobre endereço de moradia trabalho profissão, para entender o crescimento populacional e demográfico. No caso em comento, a possibilidade de divulgação de informações obtidas pelo censo levantou controvérsia quanto à disponibilidade dos dados dos cidadãos indiscriminadamente, gerando um ambiente de insegurança e temor diante de um estado intrusivo da esfera privada dos cidadãos (SCHWARTZ, 1989, p. 688).

[54] Laura Schertel Mendes (2020, p. 2) menciona que o termo "autodeterminação informativa", ainda que reconhecido especificamente neste caso, foi construído a partir de diversos julgados da Corte Alemã.
[55] Decisão disponível em: https://www.servat.unibe.ch/dfr/bv065001.html
[56] A controvérsia do caso gira em torno da lei de recenseamento da população, cujo processamento, armazenamento e transmissão em meios eletrônicos de dados pessoais tomou proporções não tangibilizadas.

A decisão entendeu que a autodeterminação individual pressupõe que o titular tenha liberdade para permitir quais ações possam ser tomadas a partir de seus dados, em outras palavras, a autodeterminação pressupõe um comportamento do indivíduo, consubstanciado na liberdade de tomar decisões quanto ao processamento de seus dados, inclusive em meios digitais. Para o Tribunal "[...] a autodeterminação é uma condição funcional elementar de uma comunidade democrática livre baseada na capacidade de agir e participar de seus cidadãos.[57]" E ainda chega à seguinte conclusão: "Nas circunstâncias do moderno processamento de dados, o livre desenvolvimento da personalidade requer a proteção do indivíduo contra a coleta, armazenamento, uso e transferência ilimitados de seus dados pessoais".[58]

O direito à autodeterminação não seria compatível com uma ordem social ou jurídica que impossibilitasse seu exercício, na medida em que comprometeria tanto o desenvolvimento individual, quanto o bem comum, visto que a autodeterminação é uma condição funcional elementar de uma sociedade democrática livre, baseada na capacidade de agir e participar de seus cidadãos (ALEMANHA, 1983).

Laura Schertel Mendes (2020, p. 10), por outro lado, destaca que a proteção abstrata ao direito da personalidade garante proteção ao indivíduo nos casos de conflitos carentes de normativa, esse seria o ponto de origem da autodeterminação informativa. Para a autora o "direito à autodeterminação informativa está intimamente ligado à própria história da proteção da personalidade como direito fundamental, na medida em que o Tribunal Constitucional o desenvolveu como um desdobramento do direito ao livre desenvolvimento da personalidade" (MENDES, 2020, p. 2).

De certa forma, o Tribunal Constitucional Alemão balizou o direito à autodeterminação informativa/informacional com base no direito geral da personalidade (BIONI, 2019).

Em linhas gerais, o direito à autodeterminação informativa, se consubstancia na defesa, individual ou coletiva, em face dos desvios de finalidade na captação e tratamento dos dados pessoais. Reconhecer a autodeterminação informativa como um dos mecanismos de defesa da privacidade é fator fundamental no atual cenário da sociedade digital.

---

[57] No original: Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.
[58] No original: unter den modernen Bedingungen der Datenverarbeitung den Schutz des Individuums vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.

De outro lado, a razoabilidade tem sido entendida como limitação lógica aos direitos individuais, servindo como contraponto ao sistema do “tudo ou nada”, de exclusividade de direitos, ou seja, no caso concreto, aferindo-se objetivamente os meios e os fins, o aplicador da norma deve atentar-se para critérios aceitáveis de exercício dos direitos (MALDONADO; BLUM, 2019). Nesse sentido, Konrad Hesse:

> [...] para poder cumprir sua função na realidade social, os direitos fundamentais precisam, em maior ou menor grau, de um desenvolvimento concretizador pelo ordenamento jurídico: para que a situação jurídica regulada como direito fundamental se torne real e efetiva no seio da sociedade faz-se necessário estabelecer por todos os meios não somente normas materiais mais minuciosas, mas também pôr de pé formas de cooperação e normas de procedimento (HESSE, 2009 p. 52).

A divulgação de dados pessoais alcançou discussões notáveis no meio jurídico e social, a autodeterminação informativa se insere como um direito ou princípio em que o indivíduo controla a utilização de seus dados pessoais. (MENDONÇA, 2014).

A Lei Geral de Proteção de Dados prevê a autodeterminação informativa como um de seus fundamentos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> [...]
> II - a autodeterminação informativa; (BRASIL, 2018)

O Acordo de Santa Cruz de La Sierra, assinado pelo Brasil em 12 de julho de 2004 e promulgado pelo Decreto nº 6659/2008 em seu art. 45 reconhece:

> 45. Estamos também conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras iberoamericanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Proteção de Dados, aberta a todos os países da nossa Comunidade.

Stefano Rodotà (2008, p. 14) aponta que a proteção de dados é uma das ferramentas essenciais para o livre desenvolvimento da personalidade, para ele “A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio” (RODOTÀ, 2008, p. 14).

Nessa mesma ideia de proteção dados como exercício de direitos fundamentais da personalidade, Caitlin Mulholland (2018, p. 171) entende que a tutela da

privacidade é cerne constitucional para a proteção de dados, na medida em que “dados são elementos constituintes da identidade da pessoa”, portanto, merecem proteção, para o desenvolvimento e fortalecimento da dignidade humana.

No Brasil, além da previsão normativa o judiciário já se manifestou no sentido de reconhecimento do direito à autodeterminação informativa ao analisar a MP 954/2020.

### 2.4.1 Autodeterminação informativa e a paradigmática decisão na Ação Direta de Inconstitucionalidade nº 6.387

Ainda que o Supremo Tribunal Federal já tenha proferido decisões em matéria de privacidade, sigilo de comunicações e dados, inexistia acórdão tratando expressamente da tutela constitucional do direito à autodeterminação informativa. Assim, a decisão da Corte proferida na ADI nº 6.387, possui relevância sem precedentes.

O ano de 2020 foi impactado pela escalada de contaminação do vírus Sars-cov-2, ou COVID-19, ou ainda, Coronavírus. A Organização Mundial de Saúde declarou a situação como pandemia, levando os governos a adotar providências para o combate à disseminação da doença.

Nesse sentido, foram tomadas medidas governamentais visando ao aumento da vigilância e monitoramento da população, de modo a controlar os avanços do COVID-19. A MP 954/2020, que dispõe sobre o compartilhamento de dados, segue nessa linha, embora com outro objetivo: possibilitar ao IBGE acesso a informações para produzir estatísticas oficiais durante o período de isolamento social.

Diante do cenário da MP nº 954, diversas ADIs foram propostas no Supremo Tribunal Federal[59], defendendo que o compartilhamento de dados nos moldes da Medida Provisória, traz graves riscos para a privacidade dos cidadãos e para a própria democracia brasileira, violando o artigo 5º, incisos X, XII e LXXII da Constituição Federal.

[59] ADI 6.387, 6.388, 6.389, 6.390 e 6.393.

Nos autos da Ação Direta de Inconstitucionalidade nº 6.387 de autoria da OAB Federal, foi proferida a decisão cautelar da Ministra Rosa Weber[60].

A inicial da ADI aponta que a MP nº 954 apresenta vícios de inconstitucionalidade formal, por inobservância dos requisitos constitucionais para edição de Medida Provisória, e de inconstitucionalidade material, diante da violação das regras constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa.

Ao conceder a medida cautelar a decisão da Ministra Rosa Weber delineou a matéria no seguinte sentido:

> Cumpre, pois, equacionar se a MP n. 954/2020 exorbitou dos limites traçados pela Constituição ao dispor sobre a disponibilização dos dados pessoais de todos os consumidores dos serviços STFC e SMP, pelos respectivos operadores, a entidade integrante da Administração indireta.

A decisão entendeu que a MP/954 não delimita o objeto da estatística a ser produzida, nem a finalidade[61] específica, tampouco a amplitude, ainda, que o artigo trate sobre a finalidade e o modo de utilização dos dados objeto da norma, igualmente não esclarece a necessidade de disponibilização das informações nem como serão efetivamente utilizados.

A relatora destaca que informações, relacionadas à identificação de pessoa natural, "configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X

---

[60] Recentemente, a Corte Alemã enfrentou questão semelhante. Na decisão publicada em 17 de julho de 2020, o Tribunal Constitucional Federal declarou a inconstitucionalidade da Seção 113 da Lei de Telecomunicações, ao entender que a norma, da forma como redigida, fere tanto o direito geral de personalidade dos titulares dos dados pessoais, quanto o sigilo das comunicações, direitos básicos da autodeterminação informativa. Pela Seção 113, as autoridades de segurança podem solicitar informações, por meio dos chamados inventários manuais, sobre dados do cliente, mas não sobre o tráfego no sentido de dados de comunicação, do assinante de uma conexão telefônica ou um endereço IP atribuído em um momento específico. De acordo com o Tribunal, referida transmissão é permitida pelo direito constitucional, contudo, os parâmetros para a admissibilidade de tal medida são definidos em limites desproporcionais, na medida em que a lei não trouxe de forma clara e suficiente, os fins para os quais as informações coletadas seriam utilizadas. A partir da decisão do Tribunal, os nomes dos clientes telefônicos e endereços IP dos usuários da Internet só podem ser consultados e avaliados pelas autoridades de segurança sob condições estritas.

[61] A decisão da Ministra está em linha com o princípio da transparência previsto na Lei Geral de Proteção de Dados, que em seu art. 6º, inciso VI, determina que as atividades de tratamento de dados pessoais deverão observar a boa-fé e o princípio da transparência.

e XII)". Nesse ponto da decisão resta claro o entendimento da Corte no sentido de que os dados pessoais também estão protegidos pelo manto do direito à privacidade.

Prossegue a decisão indicando que o tratamento de dados deve observar os ditames constitucionais. "Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais."

Este ponto da decisão merece destaque, na medida em que a interpretação da relatora é no sentido de que o direito à autodeterminação informativa integra os direitos da personalidade.

O acórdão ainda entende que a ausência da finalidade, impede a correta avaliação dos requisitos da adequação e necessidade, desatendendo assim, a garantia do devido processo legal (art. 5º, LIV, da CF/88), em sua dimensão substantiva. Prossegue a Ministra afirmando que:

> [...] a MP n. 954/2020 não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, seja no seu tratamento. Limita-se a delegar a ato do Presidente da Fundação IBGE o procedimento para compartilhamento dos dados, sem oferecer proteção suficiente aos relevantes direitos fundamentais em jogo. Enfatizo: ao não prever exigência alguma quanto a mecanismos e procedimentos para assegurar o sigilo, a higidez e, quando o caso, o anonimato dos dados compartilhados, a MP n. 954/2020 não satisfaz as exigências que exsurgem do texto constitucional no tocante à efetiva proteção de direitos fundamentais dos brasileiros.

Lembra a Ministra que a Lei Geral de Proteção de Dados, norma definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais, ainda não se encontrava vigente, pontuando que, embora não seu olvide a gravidade da crise sanitária e urgência "de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição".

Acompanhando integralmente a relatora, o Ministro Alexandre de Moraes apontou que os direitos e as garantias fundamentais não são absolutos e encontram limites nos demais direitos consagrados na Constituição. Contudo, a

relativização desses direitos deve observar os princípios da razoabilidade e da proporcionalidade, o que não ocorre, a seu ver, na hipótese do texto da MP. O Ministro Gilmar Mendes apontou que a Organização Mundial da Saúde (OMS), no seu regulamento sanitário internacional, incorporado ao ordenamento jurídico brasileiro por meio do Decreto 10.212/2020, afasta a possibilidade de processamentos de dados desnecessários e incompatíveis com o propósito de avaliação e manejo dos riscos à saúde. Por sua vez, o Ministro Luiz Roberto Barroso acrescentou que a providência deveria ter sido precedida de debate público acerca da necessidade, da relevância e da urgência[62].

A preocupação primordial no uso de dados pelo Estado deve ser a efetividade dos direitos humanos, o que pressupõe focar o design, desenvolvimento e uso com base no respeito à dignidade e aos direitos humanos (CORVALÁN, 2017).

Vale mencionar que o caso trata sobre a coleta de dados feita pelo Estado o que torna essa decisão um marco fundamental à defesa da privacidade e à proteção de dados, assunto que será debatido a seguir.

## 2.5 Proteção de dados como defesa do direito à privacidade

Tratar de privacidade no contexto da tecnologia digital e economia de dados passa pela necessidade de remodelar o próprio conceito de privacidade como já destacado neste estudo. Da ideia de separação, “meu mundo” apartado do restante, é necessário pensar em uma ideia de controle do “meu mundo”, ou seja, não basta que haja um reconhecimento ao direito de privacidade, para uma efetiva proteção do *self*, esse direito deve ser efetivo, permitindo ao indivíduo o controle de todos os aspectos do seu próprio ser, inclusive dados e informações.

Contando ou não com a previsão expressa na Constituição Federal, o esforço a ser empreendido pela doutrina e pela jurisprudência deve se consolidar pelo favorecimento de uma interpretação dos incisos X e XII do art. 5º mais fiel ao nosso tempo, nesse sentido:

---

[62] Acompanharam a relatora, o presidente Dias Toffoli, os Ministros Celso de Mello, Edson Fachin, Luiz Fux, Ricardo Lewandowski e a Ministra Cármen Lúcia.

> [...] reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à comunicação de dados. Dessa forma, seria dado o passo necessário à integração da personalidade em sua acepção mais completa nas vicissitudes da Sociedade da Informação (DONEDA, 2011, p. 106).

Tércio Sampaio (1993, p. 457) aponta que a privacidade e a proteção de dados estão relacionadas à própria cidadania e segurança do indivíduo. Nossas vidas cada vez mais têm sido influenciadas pelo processamento de dados, a economia é orientada a partir de dossiês digitais, que obrigatoriamente se relacionam diretamente com um titular, o que justifica reconhecer os dados pessoais como direito da personalidade (BIONI, 2019, p. 65).

A discussão sobre os dados pessoais e sua correta alocação jurídica não foge ao campo de discussão dos direitos da personalidade. Com efeito, os problemas jurídicos atrelados aos dados pessoais surgiram, num primeiro momento, ligados à privacidade que é um dos mais tradicionais direitos da personalidade, pois se objetivava proteger o indivíduo contra exposições indevidas dos fatos que integram a vida privada e a intimidade (BITTAR, 2015. p. 107).

Solove (2008) entende que os dados pessoais devem ser protegidos considerando a mesma natureza da propriedade intelectual, explicando que, diferentemente da propriedade física, a propriedade intelectual protege a expressão de ideias, ou seja, os direitos autorais fornecem controle sobre a maneira particular como ideias são expressas. O autor lembra que essa noção de autoria vem de Locke, no sentido de que alguém ganha um direito de propriedade sobre algo quando emana de si mesmo. Nessa analogia “informação pessoal” é uma extensão da personalidade porque advém da construção da história de cada indivíduo, segundo o autor “geramos informações à medida que desenvolvemos nossas personalidades”.

Reconhecer que os dados pessoais compõem as características da personalidade e como tal são protegidos pela normativa Constitucional da privacidade é caminhar junto com a evolução da sociedade. Como aponta Bruno Bioni (2008, p. 274), é necessário um dirigismo informacional, por meio de ação regulatória *“ex ante*”, buscando empoderar o cidadão com o controle dos próprios dados.

Os primeiros anos do século XXI foram caracterizados por uma perda progressiva de privacidade. Dois fenômenos convergiram para dar origem à economia de dados: a percepção de que rastros de dados de usuários interagindo com a tecnologia poderiam ser usados para desenvolver publicidade personalizada e uma preocupação com a segurança que levou as autoridades a usarem tais dados pessoais para fins de vigilância e policiamento (VÉLIZ, 2020, p. 3).

Mas foram os últimos anos que testemunharam uma preocupação crescente com a privacidade e a importância do controle de dados. Conforme o mau uso de informações foram reveladas, a exemplo do caso *Cambridge Analytica*, os cidadãos começaram a entender a dimensão e o custo real do uso de tecnologias digitais.

À medida que entendemos o quão vulneráveis nos tornamos à partir da economia de dados, devemos questionar o uso de nossas informações, é inegável que a privacidade de dados e informações se tornou um elemento fundamental na atualidade.

Leonardi (2011. p. 95) lembra que as normas Constitucionais não afastam princípios e garantias adotados por ela, tampouco princípios e direitos de tratados internacionais de que o Brasil é signatário[63]. É de suma importância essa menção, na medida em que a "privacidade é reconhecida como um direito fundamental em praticamente todos os tratados e convenções internacionais de direitos humanos ratificados pelo Brasil".

Nessa mesma linha, Mendes (2014, p. 29) destaca que a evolução do conceito de privacidade é notada principalmente a partir dos anos 70, com novas normas e decisões judiciais sobre a matéria, além da aprovação de acordos internacionais e transnacionais em diferentes níveis. A autora pontua que "todos esses instrumentos compartilham o conceito segundo o qual os dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela jurídica."

[63] Nesse sentido: Enunciado 274 do Conselho da Justiça Federal, adotado na IV Jornada de Direito Civil: "Os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil, são expressões da cláusula geral da tutela da pessoa humana, contida no art. 1o, III, da Constituição (princípio da dignidade da pessoa humana)". Disponível em: https://www.cjf.jus.br/enunciados/enunciado/219.

Dessa forma, considerando que o dado pessoal tem atributo de personalidade, é certo que se encontra sob o manto da tutela jurídica. Ou seja, não importa sobre quais dados estejamos falando, se ele pertence a alguém que é sujeito de direito e destinatário da lei o dado deve igualmente receber guarida legal.

Quando se trata de privacidade pensada a partir de dados, a questão toma outras proporções, principalmente porque a captação e tratamento desses dados envolve o uso de tecnologia, principalmente algoritmos. Diversos modelos de algoritmos foram desenvolvidos para captar, armazenar, classificar, tomar decisões e resolver problemas a partir de dados. Acontece que, em sua grande maioria, essas ferramentas operam sem a transparência necessária, captando informações, controlando e direcionando o rumo de nossas vidas.

O estudo trata no terceiro capítulo sobre a problemática dos algoritmos. Como eles podem se tornar mecanismos de violação da nossa privacidade, quais mecanismos devemos fomentar para uma proteção efetiva e quais as demandas que o Direito pode ajudar a resolver.

## CAPÍTULO III – ALGORITMOS

O direito surgiu com a necessidade da regulamentação da vida em sociedade, para defender os interesses relacionados ao ser humano em primeiro lugar, posteriormente, a propriedade e os aspectos cotidianos. Sempre que um fato social se torna relevante, ou seja, interfere na seara humana, se torna igualmente importante ao mundo jurídico. Cada época possui suas peculiaridades, tornando a análise jurídica dos fatos cada vez mais complexa e interdisciplinar.

À medida que a tecnologia de implementação de sistemas com uso de algoritmos evolui e define uma nova realidade é necessário estudar e entendê-los. Como aplicativos de navegação, dentro de um universo de rotas possíveis, pode encontrar o caminho mais rápido em segundos? De que o modo o *Google* sugere os termos da minha pesquisa, e acerta na maioria das vezes? A resposta para essas questões é: algoritmos.

Falar de algoritmos com quem trabalha no setor de segurança da informação, ou com análise de dados é tarefa fácil. O desafio de investigar tecnologia sob o viés do direito passa pela dificuldade em converter termos técnicos em termos que sejam compreendidos por quem não possui vivência na área.

Não é possível investigar se o uso de algoritmos no tratamento de dados afeta o direito à privacidade se não entendermos o que são algoritmos, como sua presença influencia todas praticamente todas as áreas da vida atualmente.

Métodos construtivos para resolver problemas matemáticos são pensados desde os primórdios (SILVEIRA, 2019, p. 19). A palavra algoritmo é muito conhecida nas ciências da matemática e computação. Em matemática, é associada aos processos de cálculo. “Em sua origem, algoritmos são sistemas lógicos tão antigos quanto a matemática.” (REIS, 2020, p. 58). “A regra de multiplicação que aprendemos na escola e que permite obter o produto de dois números de vários dígitos, com papel e lápis, é um algoritmo simples (FANJUL, 2018). Na computação, é conexa a um conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas (MANZANO; OLIVEIRA, 2000, p. 7).

Para esta pesquisa importa o conceito e uso dos algoritmos na computação ou como se fala atualmente, na tecnologia de informática.

Um algoritmo é um procedimento computacional bem definido que leva algum valor, ou conjunto de valores, como entrada e produz algum valor, ou conjunto de valores, como saída (CORMEN, et al., 2012, p. 7).

> [...] o termo algoritmo, do ponto de vista computacional, pode ser entendido como regras formais, sequenciais e bem definidas a partir do entendimento lógico de um problema a ser resolvido por um programador com o objetivo de transformá-lo em um programa que seja possível de ser tratado e executado por um computador, em que dados de entrada são transformados em dados de saída (MANZANO, 2000, p. 9).

Paulo Reis (2020, p. 130) descreve que os algoritmos representam um modelo, dentre diversas possibilidades, para representar matematicamente modelos estruturados de processos. Algoritmos são utilizados desde a solução de problemas simples[64], como por exemplo, calcular a média aritmética de notas escolares, cálculos de juros em operações bancárias, converter anos em dias ou meses, como também para questões mais complexas, como antever jogadas do adversário em partidas de xadrez[65], diagnósticos de doenças como o câncer[66], delinear parâmetros de busca e resultados em pesquisas na internet, ou definir, a partir de uma combinação de características físicas e psicológicas, indicadores preditivos de atração entre indivíduos[67].

Vale lembrar que os algoritmos por si só, não são a solução do problema, mas sim, o caminho que conduz a solução. Por exemplo, no caso dos algoritmos que investigam a presença de câncer, o programa, desenhado a partir de um banco de dados, detecta a existência dos parâmetros que caracterizam a doença, esse

---

[64] O robô humano da Hanson Robotics, Sophia, conta com uma combinação de ciência, engenharia e arte, Sophia é simultaneamente um personagem de ficção científica criado por humanos que descreve o futuro da IA e da robótica, e uma plataforma para robótica avançada e pesquisa em IA. A personagem Sophia captura a imaginação do público global. Ela é o primeiro robô cidadão do mundo e o primeiro robô Embaixador da Inovação do Programa de Desenvolvimento das Nações Unidas. Sophia é hoje um nome conhecido, com aparições no Tonight Show e Good Morning Britain, além de falar em centenas de conferências ao redor do mundo. Sophia também é uma estrutura para pesquisa de robótica e IA de ponta, particularmente para entender as interações entre humanos e robôs e seus potenciais aplicativos de serviço e entretenimento. Por exemplo, ela tem sido usada para pesquisas como parte do projeto Loving AI, que busca entender como os robôs podem se adaptar às necessidades dos usuários por meio do desenvolvimento intra e interpessoal. Fonte: https://www.hansonrobotics.com/sophia/.

[65] Em 1997, o supercomputador Deep Blue, da IBM, conseguiu derrotar o então campeão mundial de xadrez, o russo Garry Kasparov. Com a capacidade de simular em torno de 200 milhões de possíveis posições por segundo, o computador previa o comportamento do adversário várias jogadas à frente.

[66] Novos algoritmos de Inteligência Artificial para diagnóstico de câncer de pulmão. t4h.com.br/noticias/novos-algoritmos-de-inteligencia-artificial-para-diagnostico-de-cancer-de-pulmao/.

[67] Como os algoritmos dos apps de paquera tentam prever pares perfeitos. Disponível em: https://www.bbc.com/portuguese/vert-fut-50485893.

resultado aliado aos demais exames e análises é que resulta no diagnóstico final. Para além, algoritmos podem ser desenvolvidos meramente para captação de dados, o chamado *data mining*, ou mineração de dados.

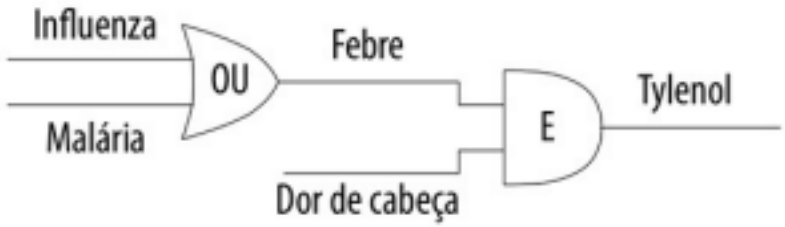
Pensando na aplicação prática dos algoritmos, Paulo Reis (2020, p. 58-59), descreve a construção de um algoritmo, de acordo com o autor, inicialmente é necessário delimitar o problema a ser resolvido para buscar a solução. Como no exemplo acima, o problema poderia ser definido como; quando as características de alteração mórfica de um órgão ou tecido podem estar ligadas à existência de células cancerígenas? A fase de definição do problema comumente envolve mais de uma área da ciência, como a saúde e a tecnologia, na hipótese.

No exemplo em questão, formulada a pergunta e retiradas as informações de um banco de dados, uma definição possível seria: as alterações de formato do órgão, coloração e presença de nódulos indicam uma probabilidade de formação cancerígena.

A elaboração da sequência de passos, para responder ao problema, é realizada na segunda fase. O algoritmo perfaz um caminho específico para obter a conformidade entre entrada e saída (CORMEN, et al., 2012, p. 5). Em seguida, esse mapa de procedimentos é traduzido para alguma linguagem de programação, possibilitando ao computador compreender e executar os comandos. Essa ‘tradução’ é executada por programadores, são esses profissionais que escrevem os algoritmos ou partes deles (REIS, 2020, p. 58-59).

Usando o exemplo ainda, o algoritmo de acordo com as instruções, detectaria em análise de imagens: alterações de formato do órgão, coloração e presença de nódulos, obtendo o resultado: a probabilidade daquela imagem corresponder à presença de formação cancerígena.

Um algoritmo é uma sequência de instruções que informa ao computador o que ele deve fazer. Pedro Domingos (2015) afirma que “Algoritmos simples podem ser representados por diagramas, com o uso de diferentes símbolos para as operações E, OU e NÃO.”, exemplificando, se influenza ou malária causam febre, e Tylenol cura febre ou dor de cabeça, essa hipótese com o uso de algoritmo s pode ser escrita da seguinte forma:




Fonte: Domingos (2015)

Para entender de um modo bem didático, algoritmos são como uma receita ou tutorial para realizar uma ação, que comumente é dividia em etapas. Para a correta execução, um algoritmo demanda um conjunto de instruções precisas e não ambíguas (DOMINGOS, 2015). Um algoritmo é um conjunto de instruções lógicas de tarefas que, a partir de um *input*, organiza e, especialmente produz um *output* em determinada etapa. “Enquanto certos algoritmos atuam em busca de padrões, outros realizam uma sequência de operações mais simples” (SILVEIRA, 2019, p. 20).

Segundo Domingos Reis (2020) há diversos modelos de algoritmos atualmente: inteligência artificial (*Artificial Intelligence*), aprendizado de máquina (*Machine Learning*), aprendizado profundo (*Deep Learning*), redes neurais (*Neural Networks), Internet das Coisas (Internet of Things).*

*Artificial Intelligence* – Inteligência Artifiicial ou AI, desenvolve sistemas baseados em inteligência humana, como raciocínio, percepção visual e compreensão de linguagem, para executar tarefas como tomada de decisões e solução de problemas, traduções entre outros (ELIAS, 2017).

*Machine Learning* - Aprendizado de Máquina (Machine Learning), desenvolve algoritmos que podem aprender automaticamente a partir de um banco de dados. Em Machine Learning a arquitetura do algoritmo é desenhada de modo que permita ao sistema aprender por conta própria, buscando resultados não previstos nem pelos desenvolvedores. O treinamento do algoritmo exige o envolvimento de um banco de dados. O aprendizado pode ser melhorado inclusive pelo usuário. Como exemplo, o usuário pode distinguir imagens que representam um gato de imagens que não representam um gato. A partir desse banco de informações o algoritmo desenha um modelo para “aprender” e distinguir com precisão uma imagem que contenha um gato, ou não. (ELIAS, 2017).

*Deep Learning* - Aprendizado Profundo, é outro mecanismo de aprendizado, construído baseado na estrutura biológica das funções cerebrais humanas e

interligação dos neurônios, ou seja, procuram imitar o cérebro humano. As redes neurais artificiais (*Neural Networks)*, assim como os neurônios humanos, se ligam a outras redes em diversas camadas, para reconhecimento de imagens por exemplo (ELIAS, 2017).

A *Internet of Things* (IoT) – Internet das Coisas, é relacionada à rede de objetos físicos que fazem uso de sensores, *softwares* e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas. Os objetos físicos, "coisas" vão desde objetos domésticos a ferramentas industriais sofisticadas (ORACLE).

A promessa dos algoritmos de aprendizagem é observar e aprender até o que o próprio cérebro é incapaz através da análise de dados, para entender padrões de organização social e prever comportamentos. O uso de algoritmos de aprendizagem permite desenhar perfis de usuários, classificando-os por padrões de consumo. É possível também identificar o melhor modelo de comunicação com o usuário, linguagem, cor, slogans tornando o perfil digital de usuários cada vez mais apurado para direcionar comunicação e manipular preferências.

Silveira (2017, p. 271-272) lembra que apesar de imateriais e invisíveis, os algoritmos são originalmente arquitetados para uma finalidade específica, essa arquitetura pode sofrer alterações a partir do usuário ou do próprio software caso sua estrutura disponha de autocorreção e aprendizagem.

Nesse universo dos algoritmos, certamente o mais conhecido, seja o Page Rank, criado em 1998 pelo Google, que basicamente rastreava a *Web* medindo a importância de um site pela quantidade de outros sites a ele vinculados, assim apresentava o resultado da pesquisa pela ordem de importância (FANJUL, 2018).

Desde 2009 o algoritmo do *Google* foi remodelado para sugerir conteúdo com base nas características de cada usuário, de modo que usuários com diferentes comportamentos podem encontrar diferentes respostas ao pesquisar um mesmo termo. Já no ano de 2008, o Google detinha patentes para algoritmos de personalização – códigos capazes de decifrar características pessoais para adaptar resultados de pesquisas (SILVEIRA, 2019, p. 21).

## 3.1 Aceita um *cookie*?

Muito se fala em *cookies* de navegação, atualmente todo site que o usuário da Internet acessa possui um lembrete sobre aceite de *cookies*. Mas o que é exatamente um *cookie*?

De acordo com o Google "*cookie*" é um pequeno arquivo salvo no computador para armazenar as preferências, configurações e outras informações usadas em páginas da web. Em outras palavras, *cookies* são pequenos arquivos de texto armazenados em navegadores web (Chrome, Safari, Firefox, Internet Explorer), quando o usuário acessa um site enquanto navega pela Internet. Os *cookies* armazenam informações sobre as interações do usuário na página memorizando preferências. Como permanecem no navegador possibilitam o rastreamento de comportamento também em outras páginas acessadas.

Segundo Lessig (2006, p. 48), no ano de 1994, a empresa Netscape incluiu um protocolo que possibilitou inserir um arquivo em computadores no momento do acesso aos servidores web. Esse arquivo é o "*cookie*" que torna possível para o servidor autenticar se a mesma máquina acessou o site em outro momento como também acompanhar o acesso dela a outras páginas. Assim, uma pequena alteração no protocolo de interação cliente-servidor passou a permitir que os sites monitorem e rastreiem seus usuários.

Os *cookies* possibilitam o acesso a dados cruzados de diferentes fontes, na medida em que eles "seguem" o usuário na sua trajetória de navegação. Exemplificando; o usuário insere dados como nome e e-mail em um site, aceitando os *cookies* de navegação, em outro site insere dados de cartão de crédito ou produtos em um carrinho de compras, assim vai distribuindo informações, os *cookies* podem captar todos esses dados e armazená-los.

Dependendo da data de validade, os *cookies* podem ser classificados como "sessão" que expiram quando um usuário sai do navegador no final de uma sessão online, ou "persistente" que permanecem armazenados no computador de um até uma determinada data de expiração, o que pode ser anos (SIEBECKER, 2003, p. 897).

A imagem seguinte foi retirada de um site de pesquisas acadêmicas, se trata do aviso de *cookies*, onde estão relacionados quais *cookies* o site utiliza e por quanto tempo, a imagem mostra apenas um deles. Esse é um *cookie* do *YouTube,* que basicamente capta dados de navegação para sugerir vídeos em sua própria plataforma.


Dois dados devem ser destacados na imagem; primeiro: a duração dos *cookies* – 6.196 dias, isso significa que basta que o usuário acesse a página e clique em aceitar *cookies* uma única vez para que eles permaneçam instalados por mais de 15 anos captando dados. Segundo: o aviso menciona que o *YouTube* coleta dados do usuário, agregando-os a dados de outros serviços do *Google* para exibir publicidade direcionada em seus próprios sites ou sites de terceiros. Isso significa que o *Youtube* capta dados do usuário, incorpora aos dados do *Google* e cria um perfil do usuário para direcionar publicidade em seus sites e de terceiros, ou seja, monetiza esses dados por meio do perfil criado vendendo-o a outras empresas.

Dados captados por cookies, ou por outros modelos de algoritmos, são armazenados em grandes bancos de dados, esses dados são mais conhecidos como *Big Data*[68]*,* que nada mais é do que captação de dados em grande volume, possibilitando localizar e analisar informações a partir de diferentes fontes. Conforme MANYIKA et al. (2011)*:* "*Big Data* refere-se aos conjuntos de dados cujo tamanho está

[68] Em 2014, a Serasa lançou uma nova classificação da população brasileira voltada principalmente ao marketing e aos sistemas de crédito e seguros, denominada Mosaic Brasil. Cruzando mais de 400 variáveis, o Mosaic utilizou algoritmos para agrupar os segmentos da sociedade com características semelhantes, permitindo descrever e discriminar esses segmentos em termos de estilo de vida, localização, comportamento de consumo e financeiro. Com essa aplicação de modelos matemáticos e estatísticos, a Serasa Experian enquadra os brasileiros em 11 grupos e 40 subgrupos. (SILVEIRA, 2019, p. 27).

além da capacidade de ferramentas típicas de software de banco de dados para capturar, armazenar, gerenciar e analisar".

A tecnologia baseada em *cookies* é utilizada para uma grande variedade de finalidades e se tornou uma ferramenta poderosa para o comércio virtual. Sempre que visitamos um site, somos bombardeados por anúncios, banners de produtos e serviços piscando. Com base em dossiês digitais, criados a partir do comportamento do usuário na rede e captado por *cookies*, mais de sessenta bilhões de anúncios por mês são cuidadosamente selecionados e enviados pela empresa de publicidade na Internet a DoubleClick Inc.[69] (SIEBECKER, 2003, p. 893).

## 3.2 Relação entre algoritmos e perfil digital

No século XIX, Allan Turing[70] sustentava que "é inteligente uma máquina que é capaz de iludir e passar por inteligente aos olhos dos homens".

Os algoritmos estão remodelando a ciência, a tecnologia, os negócios e a política. Para Paulo Reis (2020, p.17), o desenvolvimento de soluções baseadas no uso de tecnologia e algoritmos facilita o dia a dia, quase todos os habitantes são donos de pelo menos um celular, grande parte da população desenvolve seu trabalho com o uso de ferramentas tecnológicas, do mesmo modo a maioria dos governos já faz uso de diversos mecanismos baseados em tecnologia para identificar seus cidadãos e armazenar dados.

Cada vez mais, as organizações públicas e privadas estão produzindo grandes quantidades de dados provenientes de diferentes fontes. Contudo, a simples coleta deles, não é de grande utilidade, ou seja, os dados precisam estar armazenados e organizados de modo que possam ser processados para agregar-lhes valor (VIANNA; DUTRA; FRAZZON, 2016).

As redes sociais por exemplo, demandam o gerenciamento de grande quantidade de dados não estruturados[71], gerados diariamente por milhões de usuários

[69] A DoubleClick foi comprada pelo Google em 2008, ocasionando diversas discussões sobre o monopólio de dados.
[70] Alan Mathison Turing (1912-1954), matemático britânico, pioneiro da computação é considerado o pai da ciência computacional e da inteligência artificial. Fonte: https://www.ebiografia.com/alan_turing/.
[71] Dados estruturados são aqueles organizados e representados com uma estrutura rígida, a qual foi previamente planejada para armazená-los. Qual é o oposto de uma estrutura rígida e previamente

em busca do compartilhamento de informações, conhecimentos e interesses (LÓSCIO, 2011). É justamente nesse contexto que surge a importância da análise de dados e onde entra o uso de algoritmos. Dados podem ser usados para criar um "perfil digital" de cada usuário, para criar produtos e serviços personalizados. Por exemplo, um site de notícias capta todo o comportamento do usuário na sua página, (cliques, notícias mais acessadas, tempo de navegação, localização do usuário etc.), e a partir do resultado da análise desses dados, pode direcionar ao leitor matérias e publicidade segmentada que sejam de seu interesse (MANZANO; OLIVEIRA, 2000, p. 25).

O indivíduo acorda pela manhã, com o despertador do celular, que, conectado a um aplicativo, seleciona a sequência de músicas a partir do histórico de buscas. Toma café e aproveita para pesquisar no Google aquele item de desejo; uma viagem. Checa as redes sociais, distribuindo alguns *likes*, então, uma propaganda de site de viagens aparece na sua rede social, que coincidência! Ele sai para trabalhar, no caminho aproveita para ver alguns vídeos no YouTube, eis que surge a propaganda de uma companhia aérea com promoção de voos justamente para o lugar pesquisado mais cedo.

No trabalho, recebe no *Slack* notificações de reuniões organizadas pelo *Google Calendar* e realizadas através do *Google Meet*, utiliza o domínio de e-mail do *Gmail*, salva documentos no *Google Drive*. No horário do almoço, chama um Uber para ir até o restaurante, o pagamento é feito com o cartão de crédito, cujos dados estão salvos no aplicativo. Almoça no restaurante de comida italiana favorito, cuja segurança é realizada por circuitos câmeras internas, posta uma foto do prato no *Facebook* e *Instagram*, paga com cartão de crédito e solicita CPF na nota. Na saída recebe uma notificação do *Google Maps* "O que você achou do restaurante italiano?". Ao sair do trabalho vai para academia, usando um *smart watch* para monitorar as atividades físicas, gasto calórico, batimentos cardíacos etc., enquanto ouve suas músicas favoritas no *Spotify*. Fim do dia, chega em casa, enquanto come o jantar que foi pedido pelo *IFood*, acessa a *Netflix* e verifica as recomendações da semana buscando algo para assistir. Por fim, verifica as notícias, de novo aquela propaganda do site de

---

pensada? Uma estrutura flexível e dinâmica ou sem estrutura. Exemplo mais comum? Um documento ou um arquivo. Assim, é fácil concluir que as redes sociais, as quais possuem um enorme volume de dados, como textos, imagens e vídeos criados diariamente por usuários, representam outro exemplo de dados não estruturados. Atualmente, mais de 80% do conteúdo digital gerado no mundo é do tipo não estruturado. Texto adaptado. Fonte: https://universidadedatecnologia.com.br/dados-estruturados-e-nao-estruturados/.

viagens, abre uma página e é quase impossível ler o conteúdo, dada a quantidade de notificações solicitando localização, inserção do e-mail para receber novidades, aceite de *cookies* de navegação, propagandas etc.

Tentado pela propaganda da empresa de viagens, achando que se trata de um recado do universo, resolve comprar o pacote mesmo sabendo que as finanças não permitem, parcela no cartão, os dados estão salvos no *Google Pay*. Conversa com a esposa sobre o destino das férias, afirmando que precisa comprar um chapéu novo, ao checar o site de fofocas sobre famosos; uma propaganda do mais novo modelo de chapéu que está em promoção, os fatos do dia se tornam objeto de uma postagem no *Twitter*: "Quanta coincidência". Mas será mesmo que se tratava de mera coincidência?

Em um único dia, várias empresas com as quais o indivíduo interagiu atualizaram seus bancos de dados com informações sobre ele. Elas sabem onde ele esteve, o que comeu, o que leu, o que digitou, com quem falou e os anúncios que assistiu. Esses dados foram coletados e rastreados pelos vários aplicativos que o usuário acessou, mas também por aqueles ativos em segundo plano. O usuário não tem o conhecimento necessário sobre o volume e a natureza dos dados coletados do mesmo modo não deu permissão de forma intencional para que a captura ocorresse.

A rotina do indivíduo acima descrito, que é comum a milhares de pessoas no mundo todo, gera inúmeros dados que são captados por meio de algoritmos, também são eles que direcionam o marketing do produto pesquisado, verificam a disponibilidade de crédito no cartão, indicam a melhor rota em sistemas de navegação, realizam as checagens de segurança da transação financeira e sugerem conteúdo conforme o gosto do usuário[72]. Atualmente inexistem, ferramentas que possibilitam ao usuário detectar claramente tais mecanismos e como eles funcionam.

Os brasileiros estão entre os usuários que permanecem mais tempo conectados consumindo informações através da tecnologia de comunicação. De acordo com a Pesquisa Nacional por Amostra de Domicílio (PNAD, 2017), 78% dos brasileiros com 10 anos ou mais de idade possuem um *smartphone* como principal meio de acesso à internet, com três objetivos básicos: a comunicação com outras

[72] Emmanuel Macron conseguiu vencer a eleição da França com o uso de algoritmos que permitiram identificar distritos e bairros que eram os mais representativos do país como um todo. Guiando a equipe na realização de 25 mil entrevistas usadas para estabelecer as prioridades e estratégias de sua campanha. Fonte: https://www.bbc.com/portuguese/geral-42908496. Texto adaptado.

pessoas (83,2%), as atividades de lazer (68,6%) e educação e aprendizado (65,9%) (PNAD, 2017).

Esses resultados também foram constatados pela Pesquisa Brasileira de Mídia (2016), que complementa com informações sobre o tempo de uso da internet pelos brasileiros, apontando que adolescentes e adultos jovens (16 a 24 anos) a utilizam por 6h17min semanais em média, além disso, destaca-se o uso das redes sociais *Facebook* (83%), *Whatsapp* (58%), *Youtube* (17%), *Instagram* (12%) e *Google* (8%), como as mais citadas pelos participantes da pesquisa (PESQUISA BRASILEIRA DE MÍDIA, 2016).

Fernanda Bruno (2013, p. 123-124) destaca que é a própria estrutura da Internet que possibilita a captura de dados, na medida em que toda ação, postagem, navegação, busca, clique em links, downloads, produção ou reprodução de conteúdo, deixa rastros suscetíveis de captura. Para além, dados se tornaram o combustível da economia digital, eles são comprados e vendidos por *data brokers* para os mais diversos fins a empresas interessadas, principalmente, em traçar perfis individuais.

Ao definir o endereço de destino em um aplicativo de navegação o algoritmo capta os dados por meio do GPS do celular e as informações inseridas pelos outros usuários, como acidentes ou congestionamentos. A partir desse banco de dados o algoritmo traça o melhor trajeto até o destino escolhido (SILVEIRA, 2019, p. 18).

No caso da geolocalização ainda que não seja fornecida diretamente, ela pode ser revelada pelo comportamento do usuário, por meio de um *post* ou uma curtida. Diversos outros atributos podem ser mensurados a partir do comportamento do usuário, nessa dinâmica os algoritmos fazem o trabalho de analisar, buscar padrões e apresentar respostas. Bruno Ricardo Bioni (2019, p. 20), aponta que “o usuário da rede é, portanto, a todo momento monitorado, acumulando-se uma série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária”

O acúmulo de dados cria uma identidade digital ou *profiling*, descrita por Danilo Doneda (2020), como aquela em que “os dados pessoais são tratados, com auxílio de métodos estatísticos, técnicas de inteligência artificial e outras mais, com o fim de obter uma ‘metainformação’”, ou seja, “síntese dos hábitos, preferências pessoais e outros registros da vida da pessoa” (DONEDA, 2020, p. 173).

Bruce Schneier (2015) destaca que diversas inferências podem ser tiradas a partir de dados. Segundo o autor alguns deles são óbvios, a geolocalização pode

demonstrar quais são os restaurantes favoritos de alguém, a lista de sites visitados revela diversos interesses. Outros pressupostos são mais sutis, como a lista de supermercado que pode revelar condições de saúde, religião ou hábitos etílicos. Empresas de marketing buscam predizer, a partir do histórico de navegação, se alguém vai se casar, comprar uma casa, sair de férias.

Sobre a coleta e uso de dados de usuários de redes sociais, Stefano Rodotá (2008, p. 62) aponta:

> [...] torna-se possível não só um controle mais direto do comportamento dos usuários, como também a identificação precisa e atualizada de certos hábitos, inclinações, interesses, preferências. Daí decorre a possibilidade de uma série de usos secundários dos dados, na forma de 'perfis' relacionados aos indivíduos, família, grupos.

Nesse mesmo sentido, Bruno Bioni (2019, p. 23) destaca que o serviço de troca de mensagens *Whatsapp* viabilizou o aumento da comunicação virtual, criando modos de comunicar emoções, por meio de ícones ilustrativos, os chamados *emoticons.* Para o autor o uso dessas expressões para interagir nas diversas redes sociais possibilita o desenho de um perfil de nossas emoções.

Segundo Stefano Rodotà (2008, p. 240) o corpo físico está se tornando uma via de acesso para um corpo eletrônico formado pelo conjunto de dados pessoais e o que mais interessa para questões de segurança ou ações de mercado. O corpo humano natural, assim, é equiparado a um objeto qualquer, passível de observação, acompanhamento e controle à distância, por meio de sofisticados sistemas informáticos integrados a tecnologias de satélite e radiofrequência.

A coleta e exploração de dados pessoais se tornou uma vantagem competitiva, permitindo a empresas como *Google* e *Facebook* dominar os mercados online. No início dos anos 2000 o Google iniciou o desenvolvimento de algoritmos de inteligência artificial para extrair informações sobre o usuário, os dados eram coletados por meio de endereços I.P. com o uso de *cookies*. Posteriormente as informações serviram para uso em publicidade direcionada[73], até hoje essa é a principal fonte de lucro do Google. Dados coletados e gerenciados são uma arma poderosa, os chamados *data brokers*[74] captam informações individuais, convertem em pontuações, classificações, cálculos

[73] Descrição da patente disponível em: https://patents.google.com/patent/US20050131762A1/en.
[74] Bancos de dados, o Serasa é um exemplo de banco de dados monetizado.

de risco e desenham os mais diversos tipos de perfis[75], para posterior monetização, acarretando significativos impactos à direitos dos usuários.

### 3.2.1 Superendividamento da sociedade de consumo

É por meio de algoritmos de automação que o comércio eletrônico personaliza seu conteúdo, por exemplo a *Netflix* faz recomendações de filmes e a *Amazon* sugestões de produtos. É inegável que a personalização oferece vantagens para os usuários: por exemplo, quando o usuário faz uma busca com um termo ambíguo, como “machado", a *Amazon* pode sugerir a ferramenta de marcenaria ou as obras do escritor Machado de Assis. A resposta para a pesquisa desse termo considera o perfil do usuário.

Por outro lado, a personalização também pode ser usada em prejuízo do usuário, manipulando a ordem dos produtos exibidos para direcionar o usuário a efetivar a compra de uma marca específica, ou de um produto mais caro, ou até mesmo induzindo-o a realizar uma aquisição por impulso. Processos automatizados e processados por algoritmos, se tornam cada vez mais nebulosos e menos responsáveis, constituindo um risco de discriminação e segregação oculta, além de minar a privacidade e liberdade de escolha (SILVEIRA, 2019, p. 95).

É inegável que o consumo é influenciado não apenas pela necessidade, mas também pelo desejo do usuário, pela ansiedade de consumir algo que lhe foi sugerido, ou mesmo na busca por ostentação. O sociólogo Zygmunt Bauman pontua que o consumismo é um modelo de arranjo social:

> [...] resultante da reciclagem das vontades, desejos e anseios humanos rotineiros, permanentes [...], transformando-os na principal força propulsora e operativa da sociedade, uma força que coordena a reprodução sistêmica, a integração e a estratificação sociais, além da formação de indivíduos humanos, desempenhando ao mesmo tempo um papel importante nos processos de auto identificação individual e de grupo (BAUMAN, 2008, p. 41).

[75] Perfil de risco, perfil de consumo, perfil emocional, perfil político, perfil religioso são alguns exemplos de perfis que podem ser criados a partir de dados.

Para Bauman (2008, p. 20) há uma tendência na sociedade de transformar pessoas em mercadorias, onde relações sociais se baseiam em consumo: “na sociedade de consumidores ninguém pode virar sujeito sem primeiro virar mercadoria, e ninguém pode manter sua subjetividade sem reanimar, ressuscitar e recarregar de maneira perpétua as capacidades esperadas e exigidas de uma mercadoria vendável”. O filósofo aponta que os consumidores na busca de sua autoafirmação são atraídos pela perspectiva de encontrar bens e produtos para se fazerem “aptos a serem consumidos” – e, assim, valiosos para o mercado (BAUMAN, 2008, p. 82).

Paulo José da Costa Jr. (1970, p. 18) aponta que na sociedade de massas a tecnologia e a vida urbana tornaram o homem mero componente anônimo e desvalorizado em uma “complexa engrenagem industrial”. Assim, a exibição ao olhar alheio de sua vida privada causaria uma sensação de superação da própria mediocridade.

O objetivo de uma sociedade de consumo é permitir que todos os desejos, fantasias, projetos, paixões e exigências se materializem em signos, logomarcas, códigos, símbolos e aquisição de objetos (ALLÉRÈS, 2000).

O consumo supérfluo, ou consumo hedônico, pode ser entendido como aquele que se deu por impulso, pois se observa que a cada dia os significados dos materiais e a simbologia que os produtos hoje representam são vivenciadas através das experiências que trazem prazeres instantâneos aos consumidores. Segundo Lima (2010, p. 35), o hedonismo “É movido pelo desejo de artigos que ultrapassam em muito aquilo que seria necessário para a sua manutenção biológica. Mais do que para satisfazer necessidades, os produtos ou serviços são adquiridos em nome do conforto e do prazer.” (LIMA, 2010 p. 35).

Para O'Shaughnessy (1987) o ato de comprar se baseia no fato de que a pessoa após adquirir determinado bem será mais feliz. Quando um consumidor busca por um produto para adquiri-lo, por trás disso tem todo um histórico de expectativas que ultrapassam os limites racionais. Seja pela antecipação de uma necessidade futura, pelas propagandas ou até mesmo por questão de necessidade, nesse momento o indivíduo busca por algo que altere seu estado atual. Em um senso comum, hedonista é sinônimo de prazer ou busca por ele. Deste modo, para Claudia Lima Marques (2010, p. 40) o novo provoca no consumidor mais desejo e gera uma necessidade de adquirir produtos que trazem prazer e conforto, produzindo uma insatisfação, uma insaciabilidade naturalizando o ritmo de consumo moderno. Esse

ecossistema de consumo cria o que Han (2019, p. 43) chama de "*doping"* de satisfação.

Contudo, esse modelo de consumo leva, muitas vezes, o indivíduo a despender uma significativa cifra, utilizando crédito e caindo no chamado superendividamento.

O superendividamento pode ser entendido como um estado da pessoa física que tem seu ativo circulante inferior aos valores devidos aos seus credores. Claudia Lima Marques (2010, p. 21) conceitua superendividamento como a "impossibilidade global do devedor-pessoa física, consumidor, leigo e de boa-fé, de pagar todas as suas dívidas atuais e futuras de consumo (excluídas as dívidas com o Fisco, oriundas de delitos e de alimentos) em um tempo razoável com sua capacidade atual de rendas e patrimônio".

Santos (2005, p. 2), o define como: "[...] a situação em que a pessoa física [...] deixa um passivo descoberto, capaz de influir na manutenção de suas despesas mais básicas em sua subsistência". Carpena e Cavallazzi (2006, p. 329) completam o pensamento de Santos ao dizer que quando chega nessa situação "o indivíduo precisa de auxílio para reconstruir sua vida econômico-financeira".

O superendividamento não se restringe ao âmbito jurídico ou patrimonial do indivíduo, ele repercute amplamente no ambiente social e familiar, seu efeito mais imediato é a dificuldade de subsistência e manutenção da qualidade de vida do endividado e de sua família.

O Banco Mundial apontou que o superendividamento dos consumidores é um risco sistêmico macroeconômico. De acordo com a Instituição, o Brasil conta com um número recorde de 67,1% das famílias endividadas. O superendividamento é fenômeno social e jurídico com alto impacto econômico. O devedor incapaz de arcar os débitos presentes e futuros, em razão do alto nível de endividamento em que se encontra, é deixado de fora no mercado de consumo, incapacitando-o de prover o próprio sustento. Além disto ele não consegue obter crédito, diante da existência de restrição cadastral, resultando numa "classe de segregados sociais" (BRITO, ARAÚJO, 2014, p.192).

O fato é que o superendividamento tem suscitado inúmeras preocupações, tanto de ordem econômica quanto social, já que atinge a saúde financeira do sistema econômico. Além de comprometer a dignidade da pessoa que se encontra endividada, afetando sua autoestima e confiança na administração do ambiente familiar, gerando

a destruição da sua vida privada pela incapacidade de suportar o cumprimento de seus compromissos financeiros.

A eficiência na captação, armazenamento, processamento e distribuição de dados, no contexto do capitalismo altamente concentrador de riqueza, possibilitou o surgimento de novos produtos e modelos de negócios. “A busca de compradores é, antes de mais nada, a procura de dados sobre cada um deles” (SILVEIRA, 2019, p. 22).

Os algoritmos entram na dinâmica do favorecimento ao consumo e superendivamento, não apenas na captura de dados e direcionamento de produtos, mas também porque influenciam o consumo de massa através de um verdadeiro bombardeio de marketing no celular, televisor, computador e demais dispositivos.

Nessa problemática os algoritmos utilizados não sofrem qualquer regulamentação ou inspeção. Pela internet é possível encontrar grandes quantidades de informações pessoais, listas telefônicas reversas e bancos de dados de registros públicos. Os profissionais de marketing estão extraindo esses dados com considerável entusiasmo, a julgar pelo aumento significativo de lixo eletrônico e correspondência direcionada nos últimos anos (PETERSEN, 2007). Silveira (2017, p. 24) menciona que a interação entre algoritmos e economia, resultou em novas “posturas e sujeições, afetando e reconfigurando também a economia e o capital.”

É fundamental notar e questionar o modo como a “cultura algorítmica se alimenta para produzir novos hábitos de pensamento, conduta e expressão que provavelmente não existiriam em sua ausência” (REIS, 2020, p. 132).

Nossas escolhas de consumo podem ser moldadas por algoritmos, o perfil digital produzido a partir de nossos dados facilita o bombardeio de marketing. Quem nunca pesquisou determinado produto e posteriormente recebeu e-mail “última chance”, ou diversas notificações do produto na tela enquanto navegava em outros sites e acabou finalizando uma compra de um item desnecessário ou que resultou em arrependimento depois.

Nossos dados alimentam modelos de negócios baseados em formatar perfis digitais, sem nosso consentimento e muitas vezes sem nosso conhecimento. Contudo, não só a iniciativa privada tem interesse em nossos dados, conforme veremos a seguir o Estado também armazena e faz uso de diversos dados de seus cidadãos.

### 3.2.2 Capitalismo de vigilância

Não há dúvidas que a tecnologia facilitou muito a vida, encurtou distâncias e proporcionou meios de comunicação em tempo real. Nos anos 2000, o relacionamento entre pessoas e tecnologia sofreu significativas mudanças. Carregar dispositivos eletrônicos e interagir com eles o tempo todo se tornou comum. Passamos a confiar que o celular e seus diversos aplicativos nos indiquem a direção, nos ajudem a escolher o almoço ou com quem vamos namorar (FINN, 2017).

Na medida em que a coleta e a análise de dados se tornam mais sofisticadas e precisas, os conjuntos de dados crescem para se tornarem o que se chama de *Big Data*, nesse cenário as oportunidades futuras parecem infinitas. Os riscos, no entanto, crescem na mesma proporção.

O filósofo e teórico social Jeremy Bentham idealizou o projeto de uma prisão, chamando-a de “panóptico”, com uma estrutura circular e uma torre de guarda no centro, possibilitando a um único guarda observar os todos os prisioneiros em um determinado momento. No projeto a arquitetura não permite que os prisioneiros possam ver se há alguém na torre, assim, não sabem se estão sendo vigiados, tampouco, se existe um guarda na torre; como resultado, são compelidos a agir como se estivessem sob permanente vigilância. Este projeto se tornou uma metáfora, lançada pelo filósofo Michel Foucault, para o estado de vigilância moderno (HARTZOG, 2018, p. 24).

Essa é a mesma ótica da captação de dados que viabilizou um sistema de vigilância onipresente e ignoramos o que as empresas ou o governo possuem de informações a nosso respeito e como as utilizam.

As tecnologias de vigilância estão se desenvolvendo rapidamente e são cada vez mais usadas em todos os aspectos do cotidiano; segurança doméstica, governamental e corporativa; inteligência e aplicações militares; operações de busca e salvamento e comunicações pessoais são alguns exemplos (PETERSEN, 2007). A polícia usa esses padrões de comportamento em investigações, principalmente em investigações criminais[76].

[76] No caso da investigação da morte da vereadora do Rio de Janeiro Marielle Franco, o Ministério Público solicitou acesso a dois conjuntos de dados armazenados pelo Google. O primeiro conjunto englobava os dados de geolocalização, em uma janela de 15 minutos, de todos os usuários que estavam nos arredores do pedágio da Transolímpica, Zona Oeste do Rio, na noite de 02/12/2018 – local onde o carro usado pelos acusados, Ronnie Lessa e Élcio de Queiroz foi visto pela última vez. O

O *Facebook* pode prever raça, personalidade, orientação sexual, ideologia política, status de relacionamento e uso de drogas apenas com base em curtidas, tudo isso sem o efetivo conhecimento ou consentimento do usuário. Dependendo do país em que se vive, essas informações podem apenas revelar características individuais ou podem resultar em prisão ou morte (SCHNEIER, 2015).

Shoshana Zuboff (2021, p. 83) afirma que o capitalismo de vigilância prospera com a ignorância do público. A autora lembra que no ano de 2009 descobriu-se que o histórico das pesquisas realizada no *Google* são armazenadas por tempo indeterminado. O ex-CEO da corporação, Eric Schmidt ao ser indagado sobre tal prática, afirmou: “A realidade é que os mecanismos de busca, incluindo o Google, retêm, sim, essa informação por algum tempo.” A autora pondera que na realidade é o capitalismo de vigilância quem retém as informações. Para ela, quando esse tipo de declaração é formulado, o público acredita que as práticas tecnológicas de vigilância são inevitáveis (ZUBOFF, 2021. p. 32-33).

Schneider (2015) aponta que governos e empresas captam, armazenam e analisam a enorme quantidade de dados produzidas à medida que a vida digitalizada avança. Com base nesses dados, empresas e governos tiram conclusões que podem impactar nossas vidas de maneiras profundas. Menciona o autor que “Podemos não gostar de admitir, mas estamos sob vigilância em massa”.

Para Carissa Véliz (2020, p. 203) cada passo, palavra pronunciada, pesquisa online, compra, toques na tela e cliques são registrados, analisados e compartilhados por empresas com seus governos. De acordo com a autora:

> Emotional surveillance companies record and analyse what makes you angry when you watch the news, what content online makes you afraid, and they share that data with the authorities. They say such surveillance helps democracy. They say that you don’t need to vote any longer because your government can infer what your political opinion is through data analytics. Your data allows the powerful to make predictions about your future on the basis of which decisions are made as to how you are treated in your society. Whether you get a job, a loan, or an organ donation if you need one is decided by surveillance and predictive algorithms. This is a world in which machines manage you. They order the food you need to stay productive in the workforce when your fridge is running low. They time your efficiency at work, including

---

segundo são os dados de quem fez buscas no Google pela agenda da vereadora Marielle Franco na semana anterior a sua morte. Sete dias antes de ser morta ela divulgou sua agenda nas redes sociais. O MP solicitou informações sobre quem fez buscas com as seguintes palavras-chave: "Marielle Franco", "vereadora Marielle", "agenda Marielle", "agenda vereadora Marielle", "Casa das Pretas", "Rua dos Inválidos 122" e "Rua dos Inválidos”. Texto adaptado. Fonte: cnnbrasil.com.br/nacional/2020/09/30/google-recorre-ao-stf-contra-compartilhamento-de-dados-do-caso-marielle

> your toilet breaks. They tell you to meditate when your stress levels increase. They tell you how many steps you have to take every day for exercise to keep your access to healthcare. (VÉLIZ, 2020, p. 203-204)[77]

Na internet, a vigilância é onipresente. Somos observados continuamente, nossos dados estão sendo armazenados para sempre. É um verdadeiro estado de vigilância da era da informação (SCHNEIER, 2015).

Danilo Doneda (2019) aponta que a chegada das diversas tecnologias possibilitou a implementação bancos de dados, resultando em uma verdadeira vigilância e abuso de poder.

Nas eleições norte-americanas de 2016[78] e nas brasileiras de 2018, o uso de sofisticadas técnicas de segmentação da publicidade eleitoral, principalmente da reunião de grandes quantidades de dados de diferentes origens para definir microssegmentos do eleitorado com a finalidade de disseminar desinformação, boatos e notícias falsas, trouxe dúvidas se a democracia conseguirá sobreviver à destruição de parâmetros da realidade que anulam o debate e substituem-no pelo confronto de pós-verdades (SILVEIRA (2019, p. 34-35).

Para além, o design de tecnologia que afeta nossa privacidade é imperceptível. Não notamos que nossos celulares foram desenvolvidos para serem dispositivos de vigilância, rastreando cada movimento nosso e compartilhando nossa localização com terceiros. As políticas de privacidade em sites e aplicativos costumam ser longas, densas e projetadas para não chamar atenção. Muitas vezes as caixas de preferências de *cookie*s já estão marcadas, basta o usuário clicar em “aceito” (HARTZOG, 2018, p. 2).

Uma *startup* chamada *Clearview AI*, com sede em Nova York, durante dois anos reuniu bilhões de imagens disponíveis na Internet para criar um aplicativo que permite a identificação de pessoas através da fisionomia de seu rosto. O Exército e a

---

[77] Empresas de vigilância emocional registram e analisam o que deixa você com raiva quando assiste às notícias, que conteúdo online o deixa com medo e compartilham esses dados com as autoridades. Eles dizem que essa vigilância ajuda a democracia. Eles dizem que você não precisa mais votar porque seu governo pode inferir qual é sua opinião política por meio de análise de dados. Seus dados permitem que os poderosos façam previsões sobre seu futuro com base nas decisões sobre como você é tratado em sua sociedade. Se você consegue um emprego, um empréstimo ou uma doação de órgãos, se necessário, é decidido por algoritmos de vigilância e preditivos. Este é um mundo no qual as máquinas gerenciam você. Eles pedem os alimentos de que você precisa para se manter produtivo na força de trabalho quando a geladeira está acabando. Eles cronometram sua eficiência no trabalho, incluindo suas pausas para ir ao banheiro. Eles dizem para você meditar quando seus níveis de estresse aumentam. Eles informam quantos passos você deve dar todos os dias para se exercitar e manter seu acesso aos cuidados de saúde. (Tradução livre)

[78] Caso Cambridge Analytica, mencionado anteriormente nesta pesquisa.

Força Aérea dos EUA são usuários desse aplicativo. A empresa alega que as imagens são públicas, portanto, sua captação seria legal (HILL, 2020).

Silveira (2019, p. 72) destaca que sistemas baseados em algoritmos podem afetar a "formação da opinião pública, sobre as possibilidades de articulação coletiva e sobre a capacidade dos governos de vigiar e analisar a movimentação dos adversários e aliados, entre outras ações. Algoritmos são jogadores decisivos nos processos democráticos."

Assim como em outros países[79], o Brasil vem aumentando o uso de tecnologia para rastrear seus cidadãos, sob a justificativa de combate ao crime e em prol da segurança[80], dando mostras de autoritarismo. Em outubro de 2019, o presidente assinou o Decreto nº 10.046/2019, que determina que todos os órgãos federais devem compartilhar dados sobre os cidadãos brasileiros, de registros de saúde a informações biométricas, para consolidá-los em uma base mestre, o chamado Cadastro Base do Cidadão.

A base de informações que podem compor o Cadastro Base do Cidadão é ampla, junto com informações básicas como nome, estado civil, o cadastro incluirá dados biométricos, como perfis faciais, de voz, íris e retina; impressões digitais e das palmas das mãos. Inexiste limitação sobre como os dados de saúde podem ser compartilhados, e a lista inclui até sequências genéticas e dados excluídos ou destruídos.

A justificativa do governo, para a consolidação das informações em uma base mestre, seria reduzir os entraves à troca de informações, aumentar a qualidade e a consistência dos dados armazenados, bem como, melhorar os serviços públicos, reduzir a fraude eleitoral e tornar as políticas públicas mais eficientes.

A assinatura do Decreto nº 10.046/2019 não foi precedida de debate ou consulta pública. A lei precisa estar minimamente adequada à tecnologia, na medida

---

[79] A China lidera o ranking dos países que mais usam a tecnologia para reprimir a população. O Partido Comunista Chinês, coleta uma grande quantidade de dados sobre indivíduos e empresas: declarações fiscais, extratos bancários, históricos de compras e registros médicos e criminais. O regime usa a IA para analisar essas informações e compilar as 'pontuações de crédito social', que procura usar para definir os parâmetros de comportamento aceitável e melhorar o controle do cidadão. Fonte (https://www.anj.org.br/site/component/k2/1-noticias/jornal-anj-online/25942-estudo-detalha-como-a-tecnologia-e-usada-para-fortalecer-a-autocracia.html).

[80] A fronteira com o Paraguai possui câmeras de reconhecimento facial; as câmeras de vigilância instaladas para a Copa do Mundo de 2014 e Olimpíadas de 2016 não foram desinstaladas, além destas medidas, um software foi utilizado durante o carnaval, em várias capitais, para reconhecimento facial. Sobre o software de reconhecimento facial utilizado no carnaval. https://www.zdnet.com/article/brazilian-police-introduces-live-facial-recognition-for-carnival/.

em que a sua existência pode ser mais prejudicial que a sua inexistência. Se a lei não estiver em consonância com a realidade tecnológica, cria a falsa sensação de que um direito está protegido sem que ele realmente esteja (NETO; MORAIS; BEZERRA; 2017, p. 195).

A vigilância não é uma característica abstrata do ambiente ou da cultura, mas tem consequências pessoais tangíveis que precisam ser consideradas. Toda cautela é necessária no uso da lei e da tecnologia para controlar eventos pontuais e passageiros (NETO; MORAIS; BEZERRA; 2017, p. 195). A observância do direito à privacidade, significa respeito à liberdade, à não discriminação e proteção do indivíduo. Respeitar a privacidade é exercício de cidadania indispensável. A análise das restrições a direitos individuais operadas pelo governo durante a vigência dos estados excepcionais é questão de extrema importância, principalmente porque os reiterados mecanismos de suspensão da ordem jurídica revelam a forte tendência de um governo em passar de um Estado Democrático de Direito para um Estado Totalitário (AMARAL; 2005).

Algoritmos permitem a captação, armazenamento e tratamento de dados em larga escala, para os mais diversos fins, seja por governos ou empresas. Como já debatido neste texto, essa relação assimétrica nos mantém sob um permanente estado de vigilância, na medida em que a iniciativa privada e o Estado conhecem praticamente todos os aspectos da nossa vida pessoal, desde dados de consumo, de comportamento, de preferências e nos observam e seguem a partir dos nossos dados biométricos, de deslocamento e localização. Esse sistema de vigilância afeta nosso direito à privacidade na medida em que não há para onde correr.

### 3.2.3 Discriminação

O Dicionário Online[81] traz a seguinte definição para o termo “discriminação”:

> Ação de discriminar, de segregar alguém, tratando essa pessoa de maneira diferente e parcial, por motivos de diferenças sexuais, raciais, religiosas; ato de tratar de forma injusta: discriminação racial. Capacidade de distinguir ou estabelecer diferenças; discernimento. Ação ou efeito de discriminar, distinguir ou diferenciar. Ação de afastar, segregar ou apartar.

[81] Disponível em: https://www.dicio.com.br/discriminacao/.

A Lei Geral de Proteção de Dados determina a aplicação do princípio da não discriminação (art. 6º, IX) no tratamento de dados pessoais. Toda forma de discriminação, seja de cor, raça ou gênero deve ser repudiada e combatida, nem é preciso lembrar que, embora a sociedade tenha evoluído nesse quesito, processos discriminatórios acontecem diariamente. É fato que negros e mulheres são minoria em cargos de alta gestão, recebem menores salários e são preteridos em entrevistas de emprego.

Na tecnologia que desenvolve algoritmos a realidade não é diferente. O viés encontrado em bancos de dados e algoritmos revela uma realidade social. Em entrevista à revista Correio da Unesco[82], Aude Bernheim[83] menciona que vieses de gênero fazem parte de muitas áreas na sociedade a Inteligência Artificial não está isenta de sofrer desses vieses "Os estereótipos contidos nos algoritmos podem ter um impacto negativo na forma como são examinadas as candidaturas de emprego – excluindo as mulheres de cargos técnicos –, as propostas salariais e até mesmo os diagnósticos médicos". Nesse sentido:

> São vários os exemplos de vieses ocasionados pelas bases de dados tendenciosas, como o uso de algoritmos para realizar contratações de emprego que, ao utilizar os bancos de dados nos quais as mulheres ocupavam menos cargos no mercado de trabalho, fez com que a tecnologia valorizasse mais o gênero masculino para uma contratação. (BABO, 2020)

Algoritmos de Inteligência Artificial foram criados para encontrar padrões, como preferências e interesses, automatizando decisões, ou seja, são desenhados para assimilar modelos de comportamento, contudo, essa sistemática pode reforçar comportamentos discriminatórios. Tunes (2019) aponta que diversas pesquisas chegaram à conclusão de que as recomendações formuladas por algoritmos utilizam o interesse por notícias negativas e teorias conspiratórias para aumentar o engajamento de usuários[84].

---

[82] Disponível em: https://pt.unesco.org/courier/suplemento-online/devemos-instruir-os-algoritmos.

[83] Aude Bernheim é cientista e ativista, luta por mais diversidade e inclusão nas ciências. Fonte: https://audebernheim.fr/.

[84] Uma pesquisa publicada na revista *Science* realizada pelo MIT [Instituto de Tecnologia de Massachusetts], aponta emoções extremas como medo e raiva são fatores-chave na disseminação de falsos tweets. Fonte: https://revistapesquisa.fapesp.br/algoritmos-parciais/

Cathy O'Neil formulou uma síntese sobre algoritmos em uma palestra do TED em 2017[85], para ela a tecnologia tem o viés de quem a desenvolveu, "Algoritmos são opinião embutida em matemática" e podem traduzir os mais diversos tipos de interesses e pretensões, discriminatórias ou não.

O viés algorítmico é facilmente verificável quando pesquisado o termo "pessoas bonitas" em imagens no Google, as primeiras respostas trazem imagens de pessoas com características predominantemente caucasianas. O mesmo padrão se repete ao realizar a pesquisa no buscador Bing[86].

A rede de investigação jornalística ProPublica[87] analisou a ferramenta baseada em algoritmos chamada COMPAS (Correctional Offender Management Profiling for Alternative Sanctions[88]), que avalia a probabilidade de reincidência de réus nos Estados Unidos. A análise concluiu que a ferramenta, apresentava resultados tendenciosos no sentido de que os réus negros poderiam se tornar reincidentes em uma proporção quase duas vezes maior que os réus brancos[89].

Sistemas de Inteligência Artificial são alimentados por dados, quem estabelece os parâmetros de captação e seleção para alimentar os bancos de dados são pessoas, que podem conscientemente ou inconscientemente projetar padrões discriminatórios. Assim, não apenas o tratamento pode ser baseado em estereótipos, a própria base de dados já pode estar 'contaminada', resultando em *output* discriminatório. A discriminação pode resultar do próprio processo de mineração de dados (BAROCAS; SELBST, 2016, p. 674).

Substituir o ser humano por uma tecnologia tendenciosa não elimina a discriminação (MARTIN, 2018, p. 841). Até os mais aprimorados sistemas tecnológicos cometem erros, principalmente algoritmos de análise e seleção. Como exemplo, quando uma quantidade de dados não é suficiente para a análise de crédito, o algoritmo pode fazer uso de um atributo superficial, como a localização, para classificar o indivíduo como "alto risco", ou seja, o sujeito pode ser bom pagador, mas reside em uma área considerada de baixa renda, se o banco de dados não é suficiente para averiguar as características de uma forma mais individualizada, ele pode sofrer

---

[85] Disponível em: https://www.youtube.com/watch?v=_2u_eHHzRto&ab_channel=TED.
[86] A pesquisa do termo foi realizada por esta acadêmica em 13/04/2021 as 18:04.
[87] https://www.propublica.org/
[88] Criação de Perfil de Gerenciamento de Infratores Correcional para Sanções Alternativas – tradução livre,
[89] Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

a negativa de crédito em razão de residir em um local onde a capacidade econômica dos moradores é considerada baixa.

Sistemas baseados em algoritmos, principalmente modelos de tomada de decisão, aprendizagem e reconhecimento biométrico, levantam diversas questões relacionadas à violação de direitos, uma vez que esses processos em sua grande maioria fazem uso de informações pessoais sem o consentimento do titular. A natureza opaca desses sistemas impossibilita qualquer questionamento ou correção, sem dúvida, a maior dificuldade é justamente comprovar como uma fórmula algorítmica pode ser discriminatória.

## 3.3 O lado negro da força, o uso de algoritmos viola a privacidade?

Grande parte da tecnologia atual foi desenvolvida para resolver problemas específicos, dentro desse contexto os algoritmos desempenham papel fundamental, cada vez mais softwares executam tarefas e tomam decisões antes tomadas por humanos. Algoritmos podem ser usados para processar uma série de dados e apresentar a probabilidade de que alguém possa se revelar péssima contratação, um tomador de empréstimo arriscado ou um terrorista (O'NEIL, 2016).

A questão é que há um interesse maior em projetar tecnologias e modelos de negócios que maximizam a coleta, o uso e a divulgação de dados pessoais, para as mais diversas finalidades capitalistas. A questão se agrava pela ausência de transparência, nesse contexto de captação e tratamento de dados, principalmente quando se trata de grandes grupos econômicos. Silveira (2019, p. 26) destaca que a expansão de modelos de algoritmos assumiu diversas decisões em nossas vidas, principalmente:

> [...] na gestão das plataformas de relacionamento online e dos aplicativos móveis (controle de postagens nas *timelines* do *Facebook*, filtros etc.); - na estruturação de sistemas de ranqueamento e pontuação (crédito, análise de risco, seguros de saúde e de outros tipos, recursos humanos etc.); - na busca de tendências (consultorias, plataformas, mecanismos de busca, sistemas judiciais); - nos dispositivos de automação (máquinas, robôs, semáforos inteligentes, internet das coisas, grids); - na detecção de fraude (empresas de tecnologia, governos, auditorias etc.); - nas atividades de segurança virtual e presencial (atividades de policiamento, detecção facial etc.); - na definição de compra e venda de ativos (transações de alta

> frequência nas bolsas e mercados de derivativos); - na logística (empresas de transporte, definição de trajetos etc.); - nas ciências (diversas aplicações nos laboratórios, capacidade de predição etc.); - no jornalismo (produção de notícias por algoritmos) (SILVEIRA, 2019, p. 26-27).

Não é possível aferir com precisão até que ponto sofremos inferências dos algoritmos, na medida em que eles passaram a integrar uma significativa parte da nossa vida, sem sequer notarmos. Diariamente trocamos nossos dados por vantagens e conveniências, em grande parte sem a menor consciência disso. Essa conjectura demonstra que o limite entre eficiência e violação não existe, a manipulação acontece com a máscara da coincidência e utilidade como mostrou o exemplo da rotina do indivíduo anteriormente descrita.

Algoritmos são produtos comercializados como soluções eficazes e adequadas, contudo, como já dito, eles “são invenções, e, como toda invenção guarda as intenções dos seus criadores.” (SILVEIRA, 2017, p. 272).

Este é o ponto fundamental quando se fala de algoritmos, eles não são neutros, na medida em que a ideia que dá origem à arquitetura de um algoritmo pertence a um ser humano, que, por sua vez, possui suas próprias crenças e desígnios, o produto segue o padrão do idealizador. Miller (2018) aponta para o fato de que algoritmos são tendenciosos, assim como os humanos, que eles estão substituindo gradativamente. Tradicionalmente os preconceitos institucionais advêm do comando de humanos, com os algoritmos não é diferente. “A grande maioria está debatendo se o tal algoritmo do *Facebook* seria tendencioso. Contudo, essa é uma conversa inútil. Qualquer humano é “tendencioso”. Logo, qualquer criação nossa é, também, “tendenciosa”, ou seja, qualquer algoritmo é “tendencioso”.” (VILICIC, 2020).

Algoritmos são comumente comparados a uma receita de bolo. Usando esse exemplo é necessário mencionar que não é possível distinguir se durante a preparação da receita foi utilizado um ingrediente letal, na medida em que eles estão mascarados no resultado.

Com os algoritmos a lógica é a mesma, eles não são transparentes, o ‘’veneno’’ pode estar em sua arquitetura, mascarado, tornando o resultado contaminado. Vieses algorítmicos podem resultar em captação excessiva de dados, superendividamento, vigilância, discriminação, entre outras diversas consequências negativas, inclusive violações de direitos.

Cada época possuiu suas enfermidades fundamentais (HAN, 2109, p. 6). Quando se fala de dados pessoais, SOLOVE (2008, p. 149) aponta que a violação da privacidade pode acontecer de diferentes modos: (1) na coleta, (2) durante o processamento, (3) pela disseminação e (4) invasão.

Como exemplo, banners de aceite de *cookie*s de navegador comumente trazem o seguinte texto em algum ponto da página em formato de *pop-up*[90] "*A empresa X utiliza cookies e outras tecnologias semelhantes para melhorar a sua experiência em nossa plataforma.*", no entanto, como apontado em tópico anterior, *cookie*s melhoram a experiência de navegação do usuário, mas também captam inúmeras informações e podem permanecer ativos para sempre. Nesse caso, considerando a ideia do bolo envenenado, a captação indevida de dados e o armazenamento por prazo indeterminado, são as características e funções que "contaminam" os *cookies*.

Considerando a ideia de direito à privacidade a partir do controle de dados é evidente e inegável que esse modelo de algoritmo viola tal direito, na medida em que o usuário não está ciente quanto ao real funcionamento do sistema, uma vez instalado, o arquivo pode permanecer sem ser notado, como um parasita, captando e apropriando-se de dados eternamente.

Vale mencionar que no exemplo trazido, o texto do *banner* não é minimamente claro. Com base no texto o usuário poderia entender que o aceite serviria para aquela sessão, para "aprimorar a navegação", embora possivelmente nem isso ele saiba o que significa, apenas pelo tempo que ela durar. No entanto, como dito, *cookies* carregam consigo diversas atribuições que não estão descritas no texto, assim, a falta de transparência quanto às funções dos algoritmos é outro mecanismo de violação à privacidade.

Para agravar a situação, como já apontado, a gama de possibilidades de uso e monetização de dados é gigantesca. A ausência de conhecimento e consentimento do titular também representa uma violação à privacidade, na medida em que ele se torna mero objeto produtor de dados para o lucro de alguém.

No caso da empresa *Clearview AI* citado, embora o banco de dados tenha sido criado a partir de imagens públicas, os titulares não consentiram com a captação e uso. Assim, considerando que o controle de dados é um dos mecanismos de

[90] O *pop-up* é um tipo de janela que se abre no navegador ao visitar uma página.

proteção à privacidade se verifica uma clara violação à privacidade dos titulares das imagens recolhidas.

Nos exemplos apresentados, é possível ver claramente as três formas de violação descritas por Daniel Solove: coleta, processamento e disseminação. No caso do uso de *cookies*, a coleta de dados feita pelos arquivos não foi consentida pelo usuário, na medida em que a partir do texto do banner, ele acreditou que o sistema apenas tornaria a navegação na página mais eficaz. Inexistente autorização para coleta é igualmente inexistente o consentimento para o processamento e disseminação dos dados. No caso da empresa *Clearview AI,* a captação não foi consentida, na medida em que os titulares não foram consultados para autorizar o uso de imagem. Embora o banco de dados tenha sido criado a partir de imagens públicas, o uso igualmente não foi autorizado. A empresa monetizou esses dados, vendendo o serviço de reconhecimento facial para diversos órgãos governamentais dos EUA, mais uma clara violação de privacidade no uso de dados.

O cenário descrito é verdadeiramente complexo, os exemplos utilizados servem de mera ilustração. Com o avanço do uso de códigos na tecnologia, o "fator humano" passa a ser ignorado, assim como o "direito democraticamente estabelecido, as normas sociais, [...]. Tudo é substituído pela decisão fria e apriorística do código, sem intermediários, juízes ou supervisores" (LEMOS, 2005, p. 28).

É imprescindível que os interesses e razões, relacionados ao uso de dados, sejam claros, possibilitando a análise dos seus riscos e efeitos, sob o ponto de vista dos direitos fundamentais para evitar medidas kafkianas, nesse sentido:

> O problema da metáfora de Kafka tem a ver com o processo de tratamento da informação, a utilização ou a análise dos dados, mais do que a sua recolha. O problema não reside tanto na vigilância dos dados, mas na impotência e na vulnerabilidade criadas por uma utilização de dados que exclui a pessoa a eles respeitante, do seu conhecimento, ou da participação nos processos que a concernem. O resultado é o que produzem as burocracias: indiferenças, erros, abusos, frustrações, falta de transparência e de responsabilização (SOLOVE, 2010, p. 22) tradução livre.

Escândalos como do *Facebook* e da *Cambridge Analytica*, nos mostram que corporações e governos não estão preocupados com a privacidade. O uso de tecnologias baseadas em algoritmos sem qualquer restrição legal ameaça diretamente a liberdade e igualdade, dois pilares da democracia constitucional. A liberdade é ameaçada quando a arquitetura de algoritmos é criada para nos vigiar e

rastrear de forma abrangente, tirando conclusões e nos classificando com base em padrões de comportamento. A igualdade é ameaçada quando a tomada de decisão automatizada reflete o mundo desigual em que já vivemos, reproduzindo resultados tendenciosos e discriminatórios sob o manto da imparcialidade tecnológica, resultando em um verdadeiro retrocesso social.

Como já debatido, há diversos outros modelos de algoritmos, é preciso mencionar que nem toda arquitetura de algoritmos possui a capacidade de violar direitos, no entanto, a falta de transparência dessa tecnologia impede a correta e fácil verificação pelo usuário. Assim, se faz necessária a tomada de medidas efetivas para combater os diversos modos de violação à privacidade dentro do universo tecnológico dos algoritmos. Sobre isto tratam os tópicos seguintes.

## 3.4 Remodelando a proteção à privacidade na era dos algoritmos

Grande parte das mudanças sociais, econômicas, políticas e tecnológicas pelas quais a sociedade atravessou, eram inimagináveis. Tanto do ponto de vista positivo quanto negativo. Eletricidade, direitos femininos, o homem pisar na lua, o desastre nuclear de Chernobyl, a Internet, todos esses eventos pareciam impossíveis, mesmo assim aconteceram (VÉLIZ, 2020, p. 175).

Um dos maiores desafios quando se trata de dados pessoais é equilibrar os direitos dos titulares com o benefício potencial que a coleta e a análise e uso de dados podem oferecer (VÉLIZ, 2020, p. 8). Um coro de vozes defende a necessidade de privacidade na tecnologia, no entanto a indústria se opõe vigorosamente às regulamentações governamentais aos seus produtos, argumentando que não existe tecnologia ruim, apenas usuários ruins e que “tecnologia não machuca as pessoas, pessoas machucam pessoas.” (HARTZOG, 2018, p. 5).

Acontece que a maior parte da tecnologia existente, relacionada a algoritmos, não foi desenvolvida para o bem comum, elas representam o interesse de grandes corporações e governos. Assim, o modo como algoritmos exploram dados e a privacidade precisa de uma regulamentação forte (VÉLIZ, 2020, p. 177).

A partir do momento em que somos monitorados por mecanismos que não sofrem qualquer inspeção prévia ou no decorrer do uso e manipulação, a promessa

de democracia e mercado livre soa vazia[91]. Nos últimos anos, o uso de forma abusiva de dados que resultou em claras violações à privacidade, além disto, eventos como o ataque terrorista de 11 de setembro de 2001 nos Estados Unidos, são usados como justificativa para o desenvolvimento de sistemas que estão muito além de mera segurança e se tornaram verdadeiros mecanismos de vigilância, sem controle ou limites. Todos esses fatos justificam a discussão sobre o assunto, não apenas para esclarecer acontecimentos passados, mas para fomentar discussões maduras sobre o tema, para que se transformem em políticas concretas de defesa de direitos fundamentais. Carissa Véliz (2020, p. 176) lembra que os movimentos sociais foram fundamentais para aprovar leis que reconheçam direitos e melhorem a sociedade.

Por outro lado, Guerra menciona que definir modelos de controle em ambientes digitais é tarefa complexa:

> Alguns acreditam que a internet é insuscetível de controle; outros entendem que a autodisciplina permitiria manter a liberdade da rede e, ao mesmo tempo, disciplinar toda forma de comportamento na internet por operadores e usuários; e há aqueles que entendem que, em todo o sistema jurídico, a segurança é um elemento essencial para que as relações intersubjetivas, inclusive aquelas com direcionamento meta-individual, permaneçam em níveis mínimos e aceitáveis de organização pelo meio social, porque a vida coletiva exige comportamentos pautados por normas comuns, que sirvam de critérios orientadores das atividades individuais, que direcionem cada indivíduo consoante previsão do que os outros poderão fazer, e, em caso de necessidade, lhe permitam exigir desses outros certos comportamentos. (GUERRA, 2006, p. 6).

Silveira (2019, p. 94) afirma que a governabilidade e transparência é requisito essencial para que os algoritmos sirvam à democracia. “Invisíveis, ocultos ou obscuros não poderão ser socialmente auditados, portanto não poderão ser democraticamente controlados.”

No Brasil, a Lei Geral de proteção de dados prevê multas e bloqueio de dados em razão de violações por agentes de tratamento, mas o que se verifica na prática é que diversas empresas assumem o risco de sanções porque o uso de dados se mostra muito mais lucrativo.

---

[91] No Brasil, durante as olimpíadas de 2016, o Rio de Janeiro fez uso de câmeras para monitoramento da segurança de atletas e do público. Ocorre que as câmeras foram instaladas tanto pelo Poder Público, como pela iniciativa privada e, mesmo após o fim do evento, as câmeras permanecem ativas captando dados e imagens, sem qualquer legislação que regulamente seu uso. Fonte: https://www.globalsegmg.com.br/seguranca-compartilhada-nas-olimpiadas/

Há muito trabalho a ser feito em relação à privacidade para domar os aspectos mais sombrios da economia de dados. É imprescindível o debate das questões relacionadas a eficácia das leis existentes e o desenvolvimento de novas e melhores normas e práticas pensadas a partir da ética e respeito à privacidade (VÉLIZ, 2020, p. 3-4). Samuel Warren e Louis Brandeis (1890) desde o século passado indicavam que a norma deve possibilitar aos titulares escolher até que ponto seus pensamentos, sentimentos, emoções e produções podem se tornar disponíveis para o mundo em geral, independentemente de qualquer valoração econômica.

A indústria ao criar um produto deve obedecer às regras de segurança, se o objeto se mostra defeituoso ou coloca em risco a integridade do usuário/consumidor a empresa é responsabilizada. O mesmo deve ser aplicado à tecnologia e especialmente aos algoritmos, é necessário garantir que direitos sejam observados no processo de modelação e uso. É fundamental erradicar o preconceito institucional e sua influência perniciosa nos algoritmos de tomada de decisão, notadamente à medida que algoritmos menos transparentes, como de aprendizado profundo, se tornarem mais comuns gerando consequências sociais e políticas (MILLER, 2018).

É evidente que não existe uma solução única, nem mesmo uma solução simples para a realidade complexa dos algoritmos, mas medidas são necessárias e devem ser debatidas. Alguns mecanismos podem ser desenvolvidos dentro dessa ideia de regras e responsabilidade.

É necessário desenvolver mecanismos de detecção de vieses em algoritmos e bancos de dados, para avaliar os sistemas já existentes, mensurando seus pontos cegos e, a partir dos resultados, definir padrões mais seguros e menos discriminatórios. Silberg e Manyka (2019) destacam a importância do desenvolvimento de ferramentas e procedimentos para detectar e tratar vieses tornando os códigos transparentes e imparciais. Pensando nisso, apontam diversas estratégias operacionais como “a melhoria da coleta de dados por meio de uma amostragem mais consciente” e uso de auditoria de modelos e dados.

Doneda (2020) aponta o uso de métodos baseados na própria tecnologia para a tutela dos dados pessoais, conhecida como *Privacy Enhancing Technologies* (PET), caracterizada por recursos tecnológicos que atuam na arquitetura tecnológica da privacidade para impossibilitar, limitar ou mesmo facilitar determinada ação, como exemplo anonimização, redirecionamento e criptografia.

Diversos métodos estão em debate quando se fala de proteção de dados e algoritmos, a grande maioria desses modelos é baseada no tratamento dos dados, ou seja, quando as informações já foram captadas. Mas quando se pensa em efetivação do direito a privacidade é necessário pensar um passo atrás, desde o nascimento desses métodos, para que toda a cadeia de tratamento esteja em consonância com as normas de proteção. Vale lembrar que dois princípios devem ser a base de desenvolvimento de novas tecnologias que fazem uso de dados; a transparência e o consentimento.

### 3.4.1 *Privacy design* aplicado a algoritmos

Como dito, algoritmos estão presentes nas mais diversas ferramentas tecnológicas, é inegável que seu uso trouxe diversos benefícios à sociedade, contudo, possibilitou reflexos negativos quase na mesma proporção. Defensores da economia de dados defendem que privacidade não seria mais relevante, ou não seria tão relevante quanto antes. A experiência revela o contrário, privacidade é sinônimo de segurança. Manter a privacidade no cenário da economia de dados é fundamental para pessoas, empresas e para a própria democracia. Para proteger a privacidade é necessário garantir a segurança dos sistemas digitais (VÉLIZ, 2020, p. 26).

A tecnologia usou a invisibilidade dos algoritmos para corroer a privacidade. O design afeta como algo é percebido, funciona e é usado. As tecnologias são ótimos exemplos de poder do design (HARTZOG, 2018, p. 21).

Nesse sentido, normas e práticas de segurança, incluindo o design, devem ser pensadas a partir da ética de privacidade e segurança de dados. Carissa Véliz (2020, p. 5) defende que desenvolver práticas éticas de dados e técnicas eficazes para proteger dados, são pilares fundamentais para enfrentar os desafios de privacidade na atualidade. A autora lembra que o uso de dados tal como ocorreu no caso *Cambridge Analytica*, abala a confiança em empresas e instituições e, o que é mais preocupante, ameaça a própria democracia. “Os futuros escândalos de dados provavelmente derrubarão empresas e podem desafiar a legitimidade das democracias”.

Por outro lado, Hartzog (2018, p. 5) comenta que há pouco interesse em investir em privacidade na medida em que o usuário não sabe distinguir um aplicativo seguro

e que protege a privacidade de outro não seguro. Desse modo, a indústria de algoritmos ignora as questões relacionadas a privacidade. Para o autor o design da tecnologia é falho e a privacidade do usuário está em risco. Isso não é por acaso considerando que é mais provável que concedamos aos sites e aplicativos permissão para coletar nossos dados pessoais se tivermos que escolher entre cancelar ou aceitar.

Como ponto de ponto partida é fundamental entender como a privacidade pode ser violada, para então, definir estratégias de defesa. Vianna, Dutra e Frazzon (2016, p. 193), enfatizam a importância de mecanismos eficientes, utilizando-os no direcionamento de negócios e estratégias das organizações, minimizando riscos, e apoiando o processo de tomada de decisões**.**

Nesse contexto surge o termo "*privacy design*" ou, privacidade desde o design, desde o início. O conceito de *privacy* design surgiu no Canadá e nada mais é do que um princípio de design de sistemas, em que todo o processo de desenvolvimento é baseado na proteção da privacidade de forma proativa, antecipando o possível problema e resolvendo na origem.

> O Privacy Design é um princípio geral, composto por 7 princípios fundamentais mais específicos, que tem como objetivo antecipar as situações que podem ferir a privacidade das pessoas e evitar que elas aconteçam. O conceito foi desenvolvido por Ann Cavoukian, especialista em privacidade e proteção de dados e "Information and Privacy Commissioner" da província de Ontário, Canadá, entre 1997 e 2014 (MOURA; CABELA; FERRAS, 2020, p. 2).

A criadora do conceito, Ann Cavoukian, também desenhou os princípios de privacy design, que são:

1. Proativo não reativo; preventivo, não corretivo. A ideia é prever eventos de violação de privacidade antes que se materializem.

2. Privacidade como configuração padrão. A proteção da privacidade é padrão em todo o sistema, não é necessário que o usuário tome alguma medida para sua proteção, ela já está inserida no sistema.

3. Privacidade incorporada ao design. A privacidade é incorporada na arquitetura do sistema, sem diminuir a funcionalidade.

4. Funcionalidade total - soma positiva, não soma zero. Privacy by design evita dicotomias, como privacidade x segurança, demonstrando que é possível ter as duas. Não é preciso renunciar a um para ter o outro.

5. Segurança de ponta a ponta - Proteção à todo o ciclo de vida do sistema, inclusive na coleta, gerenciamento e descarte de dados.

6. Visibilidade e transparência – Os sistemas permanecem visíveis e transparentes, tanto para usuários quanto para fornecedores.

7. Respeito pela privacidade do usuário – toda a arquitetura é pensada a partir da experiência do usuário, resultando em um sistema amigável. (CAVOUKIAN, 2009, p.2)

Como bem menciona Lindoso (2019, p. 75) é necessário preocupar-se com a estruturação do algoritmo, na medida em que vieses discriminatórios permeiam a sociedade, tal fato tem reflexos diretos no campo da programação, como já tratado em tratado em tópico anterior.

Moura et al. (2020, p. 3) apontam a importância das estratégias de *privacy design*, que buscam antecipar possíveis vulnerabilidades de violação da privacidade antes mesmo de ocorrerem, assim, não se espera que a violação aconteça, medidas técnicas preventivas visam impedi-las.

> Os princípios ajudam organizações a utilizar os dados pessoais de forma segura e devem ser aplicados em novas tecnologias (inclusive no uso de algoritmos, *big data* e inteligência artificial), ferramentas, processos, sistemas, produtos ou serviços, de qualquer segmento de negócio. Por meio deles, é possível garantir o desenvolvimento tecnológico e a inovação com respeito aos direitos humanos e liberdades fundamentais. (MOURA; CABELA; FERRAS, 2020, p. 4).

Em regra, segundo Hoepman (2014, p. 447-448) o projeto de um *software* ou algoritmo acontece dentro de um ciclo que envolve: desenvolvimento do conceito, análise, design, implementação, teste e avaliação. As estratégias de *privacy desi*gn devem ser observadas a cada passo, mas principalmente na fase de desenvolvimento e de implementação incluindo-se regras e diretrizes condizentes com a proteção de dados de ponta-a-ponta.

O significativo aumento do uso de dados de forma indevida é apenas um dos muitos problemas relacionados à privacidade, crimes cibernéticos e vazamento de informações são problemas que podem ser minimizados com a aplicação de *privacy design*, mas, em se tratando de proteção à privacidade e arquitetura de algoritmos

integrar o conceito de *privacy design* com o direito é fator fundamental. A solução para a proteção da privacidade requer esforços conjuntos e interdisciplinares.

A diversificação de estratégias de processamento de dados, requer novas concepções sobre todo o contexto dos sujeitos na construção de distintas ações para proteção da privacidade (SOLOVE, 2004).

Arquitetar algoritmos com base em *privacy design* requer a colaboração do direito. A interação interdisciplinar, por meio de um relacionamento mutuamente produtivo é um caminho necessário para desenvolver tecnologia com respeito a proteção de dados e ao direito de privacidade. É fundamental desenvolver ferramentas e orientações práticas que apoiem a modelagem de algoritmos pensada a partir do direito à privacidade (HOEPMAN, 2014, p. 451).

Hartzog (2018, p. 5) faz uma crítica importante ao mencionar que a maioria das leis que tratam de privacidade em todo o mundo se mostram deficientes na prática porque ignoram o design. Para o autor os legisladores buscaram estabelecer limites para a coleta e uso de dados pessoais, mas negligenciaram amplamente o poder do design.

O sistema jurídico, incluindo a lei da privacidade, procura aplicar as regras antigas a problemas novos decorrentes da tecnologia. Os atos ilícitos relacionados à privacidade são julgados em grande parte com base em conceitos de delito de privacidade do século XIX (GASSER, 2016, p. 64). Estratégias de defesa à privacidade devem ser baseadas na premissa de que tanto a tecnologia quanto a sociedade e o direito devem trabalhar juntos para resolver problemas contemporâneos, inclusive aprimorando as formas tradicionais de combater crimes cibernéticos (VIANNA; DUTRA; FRAZZON, 2018).

O art. 46[92] da Lei Geral de Proteção de Dados determina que medidas de segurança e proteção de dados pessoais devem ser observadas pelos agentes de tratamento desde a concepção do produto ou serviço até a sua execução, a norma

[92] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

traz uma regra geral. Ainda que a redação do artigo seja ampla, a existência de uma disposição legislativa específica é um importante passo para o desenvolvimento de algoritmos com base na proteção do direito à privacidade, na medida em que consideraria a complexidade de sistemas e ferramentas baseadas em algoritmos.

Vale mencionar que em se tratando de medidas de proteção à privacidade, o desenvolvimento de produtos digitais também deve considerar a transparência e usabilidade, o usuário deve ser informado de forma clara sobre quais dados o sistema capta e para qual finalidade, quem tem acesso a eles e por qual prazo, além de permitir a escolha entre ceder ou não dados sem que a negativa resulte em impossibilidade de uso. Como exemplo, o compartilhamento de localização deveria vir configurado como “desativado” por padrão em aparelhos celulares e a partir das configurações o usuário pode escolher em quais aplicativos pretende ativar a localização. Atualmente é comum que aplicativos solicitem acesso a arquivos pessoais sem que a prestação de serviços esteja relacionada ao acesso a esse tipo de dado.

Desenvolver ferramentas integrando as diferentes áreas possibilita a pavimentação da proteção à privacidade de dados de forma estratégica e sistemática. Nesse contexto, instituições regulatórias podem apoiar pesquisas relacionadas à automação da conformidade tecnológica aos requisitos legais de proteção de dados de forma robusta e eficaz mormente pela fusão de diferentes instrumentos e métodos, tanto no nível legal quanto ao nível de implementação tecnológica (GASSER, 2016, p. 67-68).

É necessário debater e articular uma mudança de paradigma para abraçar o papel multifacetado e funcional da lei e da tecnologia como mecanismo de solução e melhoria. Novas estruturas pensadas a partir do direito e da tecnologia podem ser usadas para fornecer proteção de dados eficiente consistente e robusta, promovendo assim a efetivação do direito fundamental à privacidade.

### 3.4.2 Jurisdição internacional de proteção de dados e privacidade na Internet

Até o final do século XX, a lei, aplicada dentro de um limite geográfico, era basicamente a disciplina criada pelos Estados para reger a vida de sua comunidade. Em regra, o direito internacional tratava da relação entre Nações. Até a chegada da

internet, a fronteira de jurisdição jurídica era correspondente à fronteira geográfica, na medida em que as ações humanas geravam consequência, em sua maior parte, dentro de fronteiras nacionais (JOHNSON; POST, 1996, p. 1368-1370).

A Internet reconfigurou as relações e comunicações sociais, ultrapassando fronteiras e revelando a necessidade de novas definições regulatórias, na medida em que as normativas locais não estão aptas e resolver essas novas demandas. Parte da resposta a essas necessidades internacionais se deu com o crescimento do direito dos tratados e do direito consuetudinário internacional que vincula os Estados membros. Contudo, a efetivação dessas normativas muitas vezes se mostra lenta e ineficaz.

Em diversos caos, particularmente quanto a leis de privacidade e proteção de dados, mais de um Estado poderia ter competência para exercer a jurisdição, o que pode levar a soluções conflitantes e tensões jurisdicionais entre Nações. O exercício da jurisdição torna-se um problema e, consequentemente, uma questão de direito internacional quando um Estado tenta regulamentar questões que vão além do seu próprio território e interesses exclusivamente domésticos (TAYLOR, 2016, p. 5).

A jurisdição está relacionada aos princípios fundamentais do direito internacional público: soberania do Estado e a não intervenção. O princípio fundamental que permite um Estado exercer jurisdição em determinada situação é a territorialidade, ou seja, um Estado pode criar normas apenas dentro de seus limites territoriais. Contudo, o direito internacional público traz alguns princípios que possibilitam exercício de jurisdição extraterritorial dependendo das circunstâncias.

Esses princípios possibilitam o exercício da jurisdição de um Estado para onde um ato é iniciado ou consumado (subjetivo e territorialidade objetiva); a nacionalidade do indivíduo; a proteção dos interesses vitais de um Estado; os efeitos do ato; e crimes contra tudo o que possa envolver normas de *jus cogens ou jure gentium* e criar obrigações erga omnes. Aparentemente apenas a última categoria de jurisdição universal poderia, em tese, admitir o exercício da jurisdição totalmente extraterritorial sem qualquer conexão territorial entre a situação e sua regulamentação.

Nem é preciso lembrar que a Internet desconhece fronteiras, aparentemente nenhuma legislação existente a nível nacional, internacional, nem mesmo os instrumentos firmados entre blocos de Estados, se mostra adequada para resolver as demandas desse mundo digital transfronteiriço. A Internet criou fenômenos

inteiramente novos que precisam se tornar objeto de regras jurídicas claras, sem considerar o fenômeno da territorialidade (JOHNSON; POST, 1996, p. 1376).

Danilo Doneda (2019) menciona a necessidade de uma regulamentação internacional uniforme, coesa e segura frente à facilidade de circulação da informação no ambiente digital. Assim, um dos principais debates entre os estudiosos dos temas relacionados à proteção do direito à privacidade e de dados é "se o direito terá condições de sair do território estatal", passando para um nível global.

Quando se considera o ambiente da tecnologia, não é mais possível olhar apenas para um espaço geográfico fisicamente demarcado, é necessário olhar para o mundo sob a perspectiva de um ambiente sem fronteiras. Sendo assim, é preciso repensar o modelo de jurisdição baseado em territorialidade quando se trata de questões concebidas em ambiente virtual. Jhonson e Post apontam a possibilidade de separar fronteiras físicas de fronteiras digitais.

> Muitos dos dilemas processuais e materiais criados em razão da natureza transfronteiriça das comunicações eletrônicas poderiam ser resolvidos por um simples princípio: conceber o ciberespaço como um 'lugar' distinto para fins de análise jurídica, reconhecendo uma fronteira legalmente significativa entre o ciberespaço e o 'mundo real' (JOHNSON; POST, 1996, p. 1378).

Como exemplo é possível citar a cooperação formulada entre EUA e a União Europeia que encontraram, em certa medida, um meio termo entre seus diferentes sistemas regulatórios[93].

Carvalho (2018, p. 219), traz uma possibilidade para a solução de demandas relacionadas a conflitos em meios digitais, o reconhecimento de uma "fronteira virtual", no sentido de que o acesso à Internet significaria ultrapassar essa fronteira, onde a jurisdição seria regida por uma lei digital comum.

> Portanto, de acordo com a concepção liberal, a lei do ciberespaço seria mais legítima (visto que fundada no consentimento dos usuários e na liberdade individual) e mais eficaz (já que as suas normas seriam mais apropriadas para a resolução de conflitos virtuais) do que a jurisdição estatal. Por essa razão, os Estados deveriam adotar um princípio de autolimitação em qualquer processo de exercício da soberania ou de aplicação de leis locais no ambiente digital. (CARVALHO, 2018, p. 219).

[93] Privacy Shield UE-EUA.

Tecnologias criadas em um determinado local são disponibilizadas a nível mundial, a transferências de dados não conhece fronteiras, isso tudo já ocorre com ou sem a existência de uma regulamentação. Quando se trata de litígios originados em ambiente digital, definir a jurisdição e a lei aplicável para a solução do problema pode se revelar uma questão complexa, por exemplo, uma empresa tem sede nos Estados Unidos e presta serviços no Brasil, um usuário que mora na Espanha moveu uma ação face à empresa. Qual seria a jurisdição aplicável a este caso? A sede da empresa, o local de prestação do serviço ou o endereço do consumidor? Do mesmo modo, como a sentença será executada? A resposta não parece simples, tampouco de fácil aplicação, qualquer jurisdição, pensando nos modelos atuais, parece morosa e pouco efetiva, na medida em que todos os atos processuais, desde a citação até a execução de sentença, dependeriam da expedição de cartas rogatórias entre países.

Vale mencionar que diante das diversas legislações nacionais, a depender do modelo de tratamento de dados, mais de um país poderia atrair a jurisdição do caso[94].

Debater uma regulamentação e jurisdição para proteção de dados a nível internacional é necessário. Se o mundo todo usa produtos e tecnologias semelhantes, porque não fazer uso de uma regulamentação única criada a partir de um único órgão regulamentador, com poder de jurisdição para casos relacionados a dados e privacidade que envolvam mais de um país.

[94] No Brasil, o art. 3º da LGPD determina que a referida Lei “aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional e os dados pessoais objeto do tratamento tenham sido coletados no território nacional”.

## CONSIDERAÇÕES FINAIS

O debate sobre o direito à privacidade não perde seu status de contemporaneidade, assim como a sociedade evoluiu, a ideia sobre o que é privacidade também mudou. Nossa realidade é absurdamente diversa das primeiras comunidades humanas, seja pelo número de habitantes, seja pela organização social, pela comunicação, mas principalmente pelo modo como nos comportamos como indivíduos nesse meio.

O uso de algoritmos, seja para mineração de dados, aprimorar sistemas, balizar modelos de consumo ou identificar infratores e maus pagadores é uma realidade tecnológica e econômica impossível de ser impedida. Essas ferramentas desenvolveram verdadeiras bolhas sociais, somos diariamente classificados a partir de nossos hábitos, consumo, comportamentos e emoções por sistemas com as mais diversas naturezas, no entanto, não podemos normalizar a perda da nossa privacidade, como se inevitável fosse ou como se não houvesse escolha.

Ao entrar em um portal eletrônico e permitir a utilização de *cookies*, aceitamos de maneira inadmissivelmente passiva que nossos dados sejam captados, nos tornando meros produtos. É possível dizer que a privacidade se tornou uma moeda de troca, gasta para receber conveniências e facilidades, mas, é preciso lembrar que ela é um direito inalienável.

Não podemos normalizar a ausência de privacidade, somos pessoas repletas de vulnerabilidades, erramos, acertamos, o senso de discrição que cada indivíduo carrega dentro de si é um aspecto da própria personalidade e como tal, deve ser legalmente protegido.

É necessário lembrar que o mero aceite em termos de uso não nos faz efetivamente conhecedores e cientes sobre o uso dos nossos dados. Do mesmo modo, todas as informações que compartilhamos, ainda que de modo público, não podem ser usadas sem nossa ciência e concordância. A publicidade não é aval ou carta branca para a monetização e vigilância da nossa vida pessoal.

Não somos meros objetos, razão pela qual não podemos permitir que nossas emoções, escolhas ou mesmo nosso futuro sejam ditados por máquinas.

A ideia deste trabalho não foi apontar algoritmos como vilões, os benefícios de tecnologias baseadas em algoritmos são inegáveis. O objetivo maior é chamar

atenção para um debate necessário; o uso de tecnologias sem uma regulamentação prévia e sem sistemas de controle e supervisão é uma ameaça ao direito de privacidade, constitucionalmente reconhecido.

O direito tem a obrigação de viabilizar mecanismos de autonomia e bem-estar, isso inclui o exercício da privacidade caracterizada pelo controle sobre o que queremos ou não compartilhar, como queremos, sob quais circunstâncias queremos, para a finalidade que escolhermos.

A maior parte da tecnologia existente atualmente é desenvolvida em sua essência por homens, brancos, para corporações privadas, as chamadas *Big Techs*, que, por sua vez, compartilham dados com seus governos. No entanto, essas empresas captam dados de pessoas a nível mundial, sem restrições, transparência e na maior parte do tempo sem nosso conhecimento.

Se em sistemas democráticos o uso de dados de forma indevida é um risco para a estabilidade democrática, como no exemplo das eleições americanas, a ameaça para países que vivem sob sistemas ditatoriais, ou democracias enfraquecidas é ainda maior. Algoritmos são capazes de induzir consumo e igualmente capazes de induzir ideologias, remodelando a realidade da sociedade.

Embora as violações à privacidade decorrentes do uso indevido de dados, seja um assunto amplamente debatido, no Brasil, há pouco trabalho na área que relaciona essas violações ao uso de algoritmos. Pesquisadores norte-americanos têm promovido debates importantes a respeito do uso desses sistemas, culminando inclusive na suspensão do projeto de compartilhamento de dados entre a gigante corporativa *Amazon* e o governo norte americano.

As preocupações em relação à privacidade dos usuários da Internet são legítimas, à medida que novos problemas sociais surgem, novas soluções devem ser criadas.

Há muito trabalho a ser feito em relação à privacidade do ponto de vista de dados pessoais. Conforme os escândalos continuam a surgir, abundam as questões sobre como interpretar e fazer cumprir a regulamentação, como projetar novas e melhores leis, como complementar a regulamentação com melhor ética e como encontrar soluções técnicas para os problemas tecnológicos relacionados à dados pessoais.

O contexto do Código do Consumidor pode servir de paradigma no debate sobre proteção de dados. O CDC foi criado a partir da vulnerabilidade dos

consumidores perante a indústria. Era comum que as embalagens de alimentos sequer trouxessem a data de validade para consumo, o que parece inimaginável hoje.

A normativa de defesa do consumidor trouxe consigo não apenas regras, mas um verdadeiro empoderamento do cidadão, resultando em significativas melhorias por parte dos fornecedores em termos de produtos e serviços.

A chegada do CDC trouxe efetividade a diversos direitos fundamentais do consumidor, mas não impediu que novos produtos fossem criados, pelo contrário, trouxe oportunidades de melhoria para aqueles existentes no mercado. Do mesmo modo novos produtos foram pensados a partir da legislação consumerista, como exemplo, para garantir a segurança dos usuários, os rótulos das embalagens passaram a ser claros, descrevendo componentes, alertando para riscos, definido prazo de validade.

O mesmo pode acontecer com a privacidade e a tecnologia, algoritmos podem ser desenvolvidos a partir de regras de privacidade bem definidas, esse é o papel do direito, definir os parâmetros.

A monetização da privacidade e estado de vigilância não são compatíveis com o Estado Democrático de direito. O universo material deve ser pensado em prol do ser humano, como mecanismo de melhoria da vida, não em detrimento de liberdades e direitos fundamentais.

## REFERÊNCIAS


ABREU, Fabiano. *Uso acrítico das redes sociais pode levar a manipulação de consumo e massificação de gostos*. EcoDebate, 2020. Disponível em: <https://www.ecodebate.com.br/2020/01/15/uso-acritico-das-redes-sociais-pode-levar-a-manipulacao-de-consumo-e-massificacao-de-gostos/>. Acesso em: 21 fev. 2021.

AGUIAR, Emerson Barros de. *Ética: Instrumento de Paz e justiça*. 2ª ed. Natal: Tessitura, 2003.

ALLÉRÈS, Danielle. *Luxo: estratégias, marketing*. Rio de Janeiro: FGV, 2000.

AGOSTINI, Leonardo Cesar de. *A intimidade e a vida privada como expressões da liberdade humana*. Porto Alegre: Núria Fabris, 2011.

ALEMANHA. *BVerfGE 65, 1 – Volkszählung.* 1983. Disponível em:<https://www.servat.unibe.ch/dfr/bv065001.html>. Acesso em: 20 nov. 2020.

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgilio Afonso da Silva. São Paulo: Malheiros, 2008, p. 83.

AMARAL, Thiago Bottino do. *Estudo Comparativo dos Regimes Excepcionais no Brasil e na França. Estados de Defesa, Urgência e Sítio*. In: Jus Navigandi, Teresina, ano 10, n. 803, 14/09/2005. Disponível em http://jus.com.br/artigos/7292. Acesso em 25 ago. 2020.

ARENDT, Hannah. *A condição humana*. Trad. Roberto Raposo. 10ª ed. Rio de Janeiro: Forense Universitária, 2007, p. 38-41.

ASENSIO, Pedro Alberto de Miguel. *Derecho privado de Internet*. Madrid: Civitas, 2001, p. 27.

BABO, Gustavo Schainberg S. *Discriminação Algorítmica: Origens, Conceitos e Perspectivas Regulatórias (Parte 1)*. 2020. Disponível em: < https://www.dtibr.com/post/discrimina%C3%A7%C3%A3o-algor%C3%ADtmica-origens-conceitos-e-perspectivas-regulat%C3%B3rias-parte-1#:~:text=S%C3%A3o%20v%C3%A1rios%20os%20exemplos%20de,o%20g%C3%AAnero%20masculino%20para%20uma>. Acesso em: 21 fev. 2021.

BAUMAN, Zygmunt. *Vida para consumo: a transformação das pessoas em mercadorias*. Rio de Janeiro: Jorge Zahar, 2008, p. 20,41 e 82.

BAUMAN, Zygmunt. *Danos Colaterais: desigualdades sociais numa era global*. Rio de Janeiro: Jorge Zahar, 2013, p.107.

BAROCAS, Solon. SELBEST, Andrew D. *Big Data's Disparate Impact*. California: Law Review. vol. 10. 2016, p. 671-732.

BARROSO, Luís Roberto e BARCELLOS, Ana Paula. *Colisão entre liberdade de expressão e direitos da personalidade*. *Critérios de ponderação.* Interpretação constitucionalmente adequada do Código Civil e da Lei de Imprensa. Rio de Janeiro: Revista de Direito Administrativo, jan/mar 2004, p. 1-36.

BELL, Emily. *Facebook is eating the world*. Columbia Journalism Review, mar. 2016. Disponível em: <http://www.cjr.org/analysis/Facebook_and_media.php?page=all>. Acesso em: 21 jan. 2021.

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

BITTAR, Carlos Alberto. *Os direitos da personalidade*. Rio de Janeiro: Forense Universitária, 2015, p. 107.

BLUM, Renato; VAINZOF, Rony. *O Marco Civil da Internet e a Legislação*. OAB São Paulo, 2016. Disponível em: <https://www.oabsp.org.br/comissoes2010/gestoes-anteriores/direito-eletronico-crimes-alta-tecnologia/artigos/2013/O%20MARCO%20CIVIL%20DA%20INTERNET.pdf>. Acesso em: 3 mar. 2021.

BOFF, Salete Oro.; FORTES, Vinicius. Borges.; FREITAS, Cinthia Obladen de Almeida. *Proteção de Dados e Privacidade: do direito às novas tecnologias na sociedade da informação*. 1ª ed. Rio de Janeiro: Lumen Juris, 2018.

BOYD, Danah.; HERR, Jeffrey. *Profiles as Conversation: Networked Identity Performance on Friendster*. In: Proceedings of the Hawaii International Conference on System Sciences Computer Society. Jan, 2007.

BRASIL, Superior Tribunal de Justiça. *Recurso Especial nº 1.117.633*. Relator Ministro Herman Benjamin. DJ: 03/03/10.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6.387*. Relatora Ministra Rosa Weber. Plenário. Dje. 02/06/2020.

BRASIL. Supremo Tribunal Federal. *Agravo Regimental na Reclamação nº 25.872/SP*. Relatora Ministra Rosa Weber. Plenário. Dje. 23/05/2019.

BRITO, Rodrigo Toscano de Brito. ARAÚJO, Fábio José de Oliveira. *Contratos, Superendividamento e a Proteção de Consumidores na Atividade Econômica*. Revista Direito e Desenvolvimento, João Pessoa, v. 5, nº 9, jan/jun. 2014, p. 165-204.

BRUNO, Fernanda. *Máquinas de Ver. Modos de Ser. Vigilância, Tecnologia e Subjetividade*. Porto Alegre: Sulina, 2013.

BURK, Dan L. *Algorithmic Fair Use. University of Chicago Law Review*. 2018. Disponível em: <https://lawreview.uchicago.edu/publication/algorithmic-fair-use>. Acesso em: 01 abr. 2020.

CACHAPUZ, Maria Cláudia. *Intimidade e vida privada no novo Código Civil brasileiro: uma leitura orientada no Discurso Jurídico*. Porto Alegre: Sergio Antonio Fabris, 2006.

CANCELIER, Mikhail Vieira de Lorenzi. *Propriedade intelectual e sensoriamento remoto: a proteção jurídica das imagens geradas por satélites*. Florianópolis: Empório do Direito, 2016.

CARDOSO, Fernando Galves. *Retornando a lista de usuários de uma aplicação vulnerável usando o SQL Injection*. Viva o Linux. 2018. Disponível em: <https://www.vivaolinux.com.br/dica/Retornando-a-lista-de-usuarios-de-uma-aplicacao-vulneravel-usando-o-SQL-Injection>. Acesso em: 15 mar. 2021.

CARPENA, Heloisa; CAVALLAZZI, Rosangela Lunardelli. *Superendividamento: propostas para um estudo empírico e perspectiva de regulação*. In: MARQUES, Cláudia Lima; CAVALLAZZI, Rosângela Lunardelli (Coord.) Direitos do consumidor endividado: Superendividamento e crédito. São Paulo: RT, 2006.

CARVALHO, Lucas Borges de. *Soberania digital: legitimidade e eficácia da aplicação da lei na internet*. Revista Brasileira de Direito, Passo Fundo, v. 14, nº 2, p. 213-235, mai/ago, 2018. Disponível em: <https://seer.imed.edu.br/index.php/revistadedireito/article/view/2183/1839>. Acesso em: 3 jan. 2021.

CASTELLS, Manuel. *A Sociedade em Rede*. Trad. Roneide Venancio Majer. 17ª ed., São Paulo: Paz & Terra, 2016.

CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade*. Trad. Maria Luiza X. de Borges. Rio de Janeiro: Zahar, 2003.

CATALA, Pierre. *Ebauche d' une théorie juridique de l'information*. Informatica e Dirito, ano 9, jan/abr 1983, p. 20.

CAVOUKIAN, Ann. *Privacy by Design The 7 Foundational Principles*. 2009. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Aceso em: 22 mar. 2021.

COHEN, Julie. What Privacy is For. Harvard Law Review, maio, 2013.

CLARKE, Roger. *Internet privacy concerns confirm the case for intervention*. Communications of the Association for Computing Machinery, v. 42, nº 2, 1999, p. 60-67.

COSTA JÚNIOR, Paulo José da. *O Direito de Estar Só: Tutela Penal da Intimidade*. São Paulo: Revista dos Tribunais, 1970.

COSTA, Larissa et al. *Redes: uma introdução às dinâmicas da conectividade e da auto-organização*. Brasília: WWF-Brasil, 2003.

CORMEN, Thomas H. et al. *Algoritmos*. Rio de Janeiro: Campus/Elsevier, 2012.

CORVALÁN, Juan Gustavo. *Inteligência Artificial y Derechos Humanos (parte I).* 2017. Disponível em: <http://dpicuantico.com/area_diario/doctrina-en-dos-paginas-diario-constitucional-y-derechos-humanos-nro-156-03-07-2017/>. Acesso em: 29 mar. 2020.

CORVALÁN, Juan Gustavo. *Inteligência Artificial y Derechos Humanos (parte II).* 2017. Disponível em: <https://dpicuantico.com/sitio/wp-content/uploads/2017/07/Juan-Gustavo-Corvalan-Constitucional-10.07.2017.pdf>. Acesso em: 29 mar. 2020.

DOMINGOS, Pedro. O Algoritmo Mestre. São Paulo. Novatec, 2015. Versão Ebook.

DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental.* Espaço Jurídico Journal of Law, Joaçaba-SC, v. 12, nº 2, p. 91-108, jul./dez. 2011. Disponível em: < https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 29 mar. 2020.

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo. *Problemas de Direito Constitucional*. Rio de Janeiro: Renovar, 2000, p. 111-136.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2020. Versão Ebook.

DONEDA, Danilo. *Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro: da emergência de uma revisão conceitual e da tutela de dados pessoais*. Âmbito Jurídico, 2008. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460>. Acesso em: 15 mar. 2021.

DONEDA, Danilo; BARRETO, Maurício Lima; ALMEIDA, Bethânia. *Uso e proteção de dados pessoais na pesquisa científica*. Direito Público, v. 16, nº 90, 2019.

DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação*. São Paulo: Revista dos Tribunais, 1980.

EFFING, Antônio Carlos. *Bancos de dados e cadastro de consumidores*. São Paulo: Revista dos Tribunais, 2002.

ELIAS, Paulo Sá. *Algoritmos, Inteligência Artificial e o Direito*. 2017. Disponível em: <http://www.direitodainformatica.com.br/?p=1969>. Acesso em: 20 nov. 2020.

ELKIN-KOREN, Niva. GAL, MICHAL S. *The Chilling Effect of Governance-by-Data on Data Markets*. University of Chicago Law Review, 2018. Disponível em: <https://lawreview.uchicago.edu/publication/chilling-effect-governance-data-data-markets>. Acesso em: 29 mar. 2020.

ERL, Thomas; KHATTAK, Wajid; BUHLER, Paul. Big Data Fundamentals: Concepts, Drivers & Techniques. Boston: Prentice Hall, 2016.

ESPANHA. *Constituição Espanhola de 1978*. Disponível em: <https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf>. Acesso em: 05 nov. 2020.

FANJUL, Sergio C. *Na verdade, o que [...] é exatamente um algoritmo*? El País. Madri, 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/03/30/tecnologia/1522424604_741609.html>. Acesso em 15 abr. 2021.

FARIAS, Edilson Pereira de. *Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação*. 2ª ed. Porto Alegre: Sérgio Antonio Fabris Editor, 2000.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. *Curso de direito civil: parte geral e LINDB*. 10ª ed. vol. 1. rev. amp. e atual. Salvador, BA: JusPODIVM, 2012, p. 47;110.

FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. São Paulo: Revista da Faculdade de Direito de São Paulo, 1993, p. 439-459.

FERNANDES, Milton. *Proteção civil da intimidade*. São Paulo: Saraiva, 1977, p. 99.

FEIGELSON, Bruno; e SIQUEIRA, Antonio Henrique Albani. *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Revista dos Tribunais, 2019.

FIORILLO, Celso Antonio Pacheco *O Marco Civil da Internet e o meio ambiente digital na sociedade da informação: Comentários à Lei n. 12.965/2014*. São Paulo: Saraiva, 2015. Edição do Kindle.

FINN, Ed. *What Algorithms Want.* Imagination in the Age of Computing. MIT Press. England, 2017.

FONTES, Edison. *Segurança da Informação: o usuário faz a diferença*. São Paulo: Saraiva, 2006, p. 38.

FORTES, Vinícius Borges. *Os direitos de privacidade e a proteção de dados pessoais na Internet*. Rio de Janeiro: Lumen Juris, 2016, p. 103.

GASSER, URS. Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy. Harvard Law Review, vol. 130, nº 2, dez. 2016. Disponível em: <https://harvardlawreview.org/2016/12/recoding-privacy-law-reflections-on-the-future-relationship-among-law-technology-and-privacy/ discrimination>. Acesso em: 29 jan. 2021.

GELMANN, Barton. BLAKE, Aaron. MILLER, Greg. *Edward Snowden comes forward as source of NSA leaks.* 2013. Disponível em: <www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html>. Acesso em: 29 nov. 2020.

GLANCY, Dorothy J. *Invention of the Right to Privacy*. Arizona Law Review, v. 21, 1979.

GLOBALSEG. *Segurança compartilhada nas Olimpíadas conta com o apoio da segurança privada*. Disponível em: <https://www.globalsegmg.com.br/seguranca-compartilhada-nas-olimpiadas/>. Acesso em: 15 abr. 2021.

GOETTENAUER, Carlos Eduardo. Algoritmos, Inteligência Artificial, Mercados. Desafios ao arcabouço jurídico. In: FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de. *Empresa, Mercado e Tecnologia*. Belo Horizonte: Fórum, 2019, p. 277.

GONÇALVES, Diego Marques; RODRIGUES, Bruno Aloy. *Os Desafios À Preservação Da Intimidade E Da Privacidade No Ambiente Virtual*: Um Debate à Luz Das Teorias dos Círculos Concêntricos e do Mosaico. Seminário Internacional Demandas Sociais e Políticas Públicas na Sociedade Contemporânea, 2018.

GOOGLE AI BLOG. *Equality of Opportunity in Machine Learning*. 2016. Disponível em: <https://ai.googleblog.com/2016/10/equality-of-opportunity-in-machine.html>. Acesso em: 15 jan. 2021.

GOOGLE. *Cookie: definição*. Disponível em: <https://support.google.com/google-ads/answer/2407785?hl=pt-BR>. Acesso em: 20 abr. 2021.

GONZÁLEZ, Paloma Llaneza. *Internet y comunicaciones digitales: régimen legal de las tecnologías de la información y la comunicación*. Barcelona: Bosch, 2000.

GUERRA, Sidney. *A internet e os desafios para o direito internacion*al. Revista eletrônica da Faculdade de Direito de Campos, Campos dos Goytacazes, RJ, v. 1, n. 1, nov. 2006. Disponível em: <http://bdjur.stj.jus.br//dspace/handle/2011/18803>. Acesso em 15 jan. 2021.

HAAS, Guilherme. *O caso Edward Snowden e a vigilância de dados no Brasil*. 2013. Disponível em: <http://www.tecmundo.com.br/seguranca/41721-o-caso-edward-snowden-e-a-vigilancia-de-dados-no-brasil.htm>. Acesso em 15 jan. 2021.

HABERMAS, Jürgen. *Mudança estrutural da esfera pública: investigações sobre uma categoria da sociedade burguesa*. São Paulo: Editora Unesp, 2014.

HAIKAL, Victor Auilio. Enfim, o marco civil da internet. In: PINHEIRO, Patrícia Peck (coord.). *Direito digital aplicado 2.0.* 2ª ed. São Paulo: Thomson Reuters, 2016.

HAN, Byung-Chul. *Sociedade do cansaço*. Rio de Janeiro: Vozes, 2019. Edição do Kindle.

HARTZOG, Woodrow. *Privacy's Blueprint – The Battle to Control the Design of New Technologies Harvard University Press*, 2018. Versão Ebook.

HEAVEN, Douglas Heaven. *Not Like Us: Artificial Minds We Can't Understand*. New Scientist, nº 2929, ago. 2013, p. 35.

HESSE, Konrad. Temas Fundamentais do Direito Constitucional. São Paulo: Saraiva, 2009, p. 52.

HOEPMAN, Jaap-Henk. *Privacy Design Strategies*. Radboud University Nijmegen. 2014, p. 446-459.

IBGE, instituto Brasileiro de Geografia e Estatística. *Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD*. Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal. 2017. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf>. Acesso em: 30 jan. 2021.

INTERNET WORLD STATS. *Usage and population statistics*. 2020. Disponível em: <https://www.internetworldstats.com/stats.htm. Acesso em: 10 jan. 2021.

INTRONA, Lucas D. *Algorithm, Governance, and Governmentality: On governing academic writing.* Science, Technology, & Human Values, v. 41, nº 1, p. 17-49, jun. 2015.

JOHNSON, David; POST; David. Law and borders: the rise of law in cyberspace. Stanford Law Review, vol. 48, nº 5, 1996, p. 1367-1402.

LEMOS, Ronaldo. *Direito, tecnologia e cultura*. Rio de Janeiro: FGV, 2005, p. 28.

LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. São Paulo: Juarez de Oliveira, 2005.

LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2011.

LERMA, Esther Morón. *Internet y Derecho Penal: "hacking y otras conductas ilícitas en la red*, Revista de Derecho y Processo Penal. 1/79, Pamplona, Aranzadi, 1999.

LESSIG, Lawrence. *Code: version 2.0*. New York: Basic Books, 2006.

LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 1999.

LÉVY, Pierre. *O que é virtual*. São Paulo: Editora 34, 2011.

LEWICKI, Bruno. *A privacidade da pessoa humana no ambiente de trabalho*. Rio de Janeiro: Renovar, 2003. p. 83-85.

LIMA, Diana Nogueira de Oliveira. *Consumo: uma perspectiva antropológica*. Rio de Janeiro: Vozes, 2010.

LINDOSO, Maria Cristine Branco. *Discriminação de gênero em processos decisórios automatizados*. 2019. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2019.

LOSANO, Mario. *A informática jurídica 20 anos depois*. Revista dos Tribunais, nº 715, maio, 1995, p. 350-367.

LÓSCIO, Bernadete Farias; OLIVEIRA, Hélio Rodrigues; e PONTES, Jonas César de Souza. *NoSQL no desenvolvimento de aplicações Web colaborativas,* 2011. Disponível em: <https://www.addlabs.uff.br/sbsc_site/SBSC2011_NoSQL.pdf>. Acesso em: 29 mar. 2020.

MACHADO, Joana de Moraes Souza. *Caminhos para a tutela da Privacidade a Sociedade da informação: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil*. 2014. Tese (Doutorado) – Universidade de Fortaleza. Disponível em: http://uolp.unifor.br/oul/ObraSiteLivroTrazer.do?method=trazerLivro Acesso em: 29 mar. 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. *LGPD: Lei Geral De Proteção de Dados*. São Paulo: Revista dos Tribunais, 2019.

MANZANO, José Augusto NG; OLIVEIRA, Jayr Figueiredo. *Algoritmos: lógica para desenvolvimento de programação de computadores*. São Paulo: Saraiva Educação SA, 2000.

MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor: um estudo dos negócios jurídicos do consumo no comércio eletrônico*. São Paulo: Revista dos Tribunais, 2004.

MARTELETO, Regina Maria. *Análise de redes sociais: aplicação nos estudos de transferência da in formação*. Ciência da Informação, Brasília, v. 30, nº 1, p. 71-81, jan./abr. 2001.

MARTINEZ, Bruno. *Facebook supera Google como site mais visitado em 2010***.** 2010. Disponível em: <http://showmetech.com.br/facebook-supera-google-como-site-mais-visitado-em-2010>. Acesso em: 20 mar. 2021.

MANYIKA, James; CHUI, Michael; e BROWN, Brad; et al. *Big data: The next frontier for innovation, competition, and productivity.* McKinsey Global Institute, 2011. Disponível em: <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx>. Acesso em: 29 mar. 2020.

MCT, Ministério da Ciência e Tecnologia; Ministério das Comunicações. *Internet no Brasil. Nota Conjunta*. 1996. Disponível em: <https://homepages.dcc.ufmg.br/~mlbc/cursos/internet/provedores_pol/intro.htm> Acesso em: 20 mar. 2020.

MENDEL, Toby. *The Public's Right to Know***.** Principles on Freedom of Information Legislation. London: ARTICLE 19, 1999. Disponível em: <http://bit.ly/1lYHR4n>. Acesso em: 13 fev. 2021.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014, p. 29.

MENDES, Laura Schertel. MIRAGEM, Bruno. O novo direito privado e a proteção dos vulneráveis. São Paulo: Revista dos Tribunais, 2012.

MENDES, Laura Schertel. *Autodeterminação informativa: a história de um conceito*. Pensar, Fortaleza, v. 25, nº 4, p. 1-18, 2020.

MENDONÇA, Fernanda Graebin. O direito à autodeterminação informativa: a (des) necessidade de criação de um novo direito fundamental para a proteção de dados pessoais no Brasil. Seminário Internacional Demandas Sociais e Políticas Públicas na Sociedade Contemporânea, n. 11, 2014.

MILLER, Alex. P. *Want less-biased decisions? Use algorithms*. Business Review. 2018. Disponível em: <https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms>. Acesso em: 12 fev. 2021.

MINAS GERAIS. AgRg no REsp 1309891/MG, Rel. Ministro Sidnei Beneti, Terceira Turma, julgado em 26/06/2012, DJe 29/06/2012. 2012. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/21877390/agravo-regimental-no-recurso-especial-agrg-no-resp-1309891-mg-2012-0035031-2-stj/inteiro-teor-21877392>. Acesso em: 15 mar. 2021.

MORAES, Alexandre de. Direito Constitucional. 6 ed. São Paulo: Atlas. 1999, p. 80.

MORAES, Giseli Diniz de Almeida; TERENCE, Ana Cláudia Fernandes; ESCRIVÃO FILHO, Edmundo. A tecnologia da informação como suporte à gestão estratégica da informação na pequena empresa. JISTEM-Journal of Information Systems and Technology Management, v. 1, nº 1, p. 27-43, 2004.

MORAES, Maria Celina Bodin de. *Ampliando os direitos da personalidade. Na medida da pessoa humana: Estudo de direito civil-constitucional*. Rio de Janeiro: Renovar, 2010.

MOURA Raissa, CABELLA Daniela e FERRAZ Lara. *Descomplicando Privacy by Design*. Revista in loco, São Paulo, 2020.

MULHOLLAND, Caitlin. *O Direito de não saber como decorrência do direito à intimidade – Comentários aos REsp 1.195.995*. Civilistica.com. Rio de Janeiro, a. 1, jul-set/2012. Disponível em: <http://civilistica.com/wp-content/uploads/2012/09/Direito-de-nao-saber-civilistica.com-1.-2012.pdf.> Acesso em: 29 mar. 2020.

MULLER, Léo. *Tay: Twitter conseguiu corromper a IA da Microsoft em menos de 24 horas*. 2016. Disponível em: https://www.tecmundo.com.br/inteligencia-artificial/102782-tay-twitter-conseguiu-corromper-ia-microsoft-24-horas.htm >. Acesso em: 29 fev. 2021.

NAZARENO, Claudio. PINHEIRO, Guilherme. (org). *Legislação sobre acesso à informação, proteção de dados pessoais e internet*. 1ª ed. Brasília: Câmara, 2020. Versão e-book.

NETO, Elias Jacob de Menezes; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. *O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos*. Rev. Bras. Polít. Públicas, v. 7, nº 3 Brasília; 2017. p. 184-198.

NIGER, Sergio. *Le Nuove Dimensioni Della Privacy: Dal Diritto Alla Riservatezza Alla Protezione Dei Dati Personali*. Padova: Cedam, 2006.

NISSENBAUM, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press: Stanford, California. 2010. Versão Ebook.

NOBLE, Safiya Umoja. *Algorithms of oppression: how search engines reinforce racism*. New York, United States: New York University Press, 2018.

OLIVEIRA, Djalma de Pinho Rebouças de. Estratégia empresarial. Uma abordagem empreendedora. São Paulo: Atlas, 2014.

O'NEIL, C. Weapons of math destruction: How big data increases inequality and threatens democracy. New York: Crown, 2016.

ONU, Organização das Nações Unidas. Assembly General. Resolution adopted by the General Assembly on 19 December 2014. Training, v. 23, p. 1, 2011.

O'SHAUGHNESSY, Brian. Consciousness. Midwest Studies in Philosophy. nº X, setembro 1987.

ORACLE. *O Que é IoT?.* Disponível em: <https://www.oracle.com/br/internet-of-things/what-is-iot/>. Acesso em: 12 mar. 2021.

PARISER, E. O Filtro invisível: o que a Internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

PASQUALE, Frank. The blackbox society: The secret algorithms that control money and information. Cambridge: Harvard University Press, 2016. Versão e-book.

PEREIRA, Alexandre Dias. Direitos autorais e acesso à internet: uma relação tensa. Anais do IV Congresso de Direito de Autor e Interesse Público. Florianópolis: UFSC, Fundação Boiteux, 2010.

PETERSEN, Julie K. et al. Understanding surveillance technologies: Spy devices, privacy, history & applications. CRC Press, 2007.

PINHEIRO, Patricia Peck. *Direito digital*. 4ª ed. São Paulo: Saraiva, 2010.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais*: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2018. Edição do Kindle.

PINTO, Paulo Mota. *O Direito à Reserva sobre a Intimidade da Vida Privada*. Boletim da Faculdade de Direito. Coimbra, v. 69, 1993, p. 479-585.

PORTO, Antônio José Maristrello. *O Direito e a economia do cadastro positivo*. Conjuntura Jurídica, nº 77, p. 77-80. 2019. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rce/article/viewFile/24693/23466>. Acesso em: 12 mar. 2021.

POWLES, Julia; HODSON, Hal. *Google DeepMind and healthcare in an age of algorithms*. Health and technology, v. 7, nº 4, p. 351-367, 2017.

REASON WHY, 2018

RODOTÀ, Stefano. *Tecnopolitica: La democrazia e le nuove tecnologie dellacomunicazione*. Roma, Itália: Laterza, 1997.

RODOTÀ, Stefano. *Tecnologie e Diritti*. Bologna: Il Mulino, 1995.

REIS, Paulo Victor Alfeo. *Algoritmos e o Direito*. São Paulo: Almedina, 2020. Versão Kindle.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

SAMPAIO, José Adércio. *Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte*. Belo Horizonte: Del Rey, 1998, p. 55-60.

SANTOS, Cláudio Sinoé Ardenghy. *Superendividamento: a fragilidade do consumidor.* Boletim Jurídico, 2005. Disponível em: <https://www.boletimjuridico.com.br/artigos/direito-do-consumidor/899/superendividamento-fragilidade-consumidor>. Acesso em: 21 fev. 2021.

SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company, 2015.

SCHOEMAN, Ferdinand David. *Philosofical Dimensions os Privacy: Na Anthology*. Cambridge University Press, 1984. Edição do Kindle, p. 21.

SCHWARTZ, Barry. *Psychology of learning and behavior*. WW Norton & Co, 1989.

SECRETARIA DE COMUNICAÇÃO SOCIAL DA PRESIDÊNCIA DA REPÚBLICA. Pesquisa Brasileira de Mídia 2016: hábitos de consumo de mídia pela população brasileira. Brasília: Secom, 2016.

SETZER, Valdemar. Dado, Informação, Conhecimento e Competência. Universidade de São Paulo, 2015. Disponível em: https://www.ime.usp.br/~vwsetzer/dado-info.html Acesso em: 18 mar. 2021.

SIEBECKER, Michael R. *Cookies and The Common Law: Are Internet Advertisers Trespassing On Our Computers?* Southern California Law Review, vol. 76, nº. 4, maio

2003. Disponível em: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=601921>. Acesso em: 18 mar. 2021.

SILBERG, Jake. MANYIKA, James. *Como lidar com vieses na inteligência artificial e nos seres humanos*. McKinsey Global Institute, 2019. Disponível em: < https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans/pt-br>. Acesso em: 18 mar. 2021.

SILVA, Selena; KENNEY, Martin. *Algorithms, Platforms and Ethnic Bias: An Integrative Essay*. Clark Atlanta University: Phylon, v. 55, 2018, p. 55.

SILVA, Tarcízio. *Linha do Tempo do Racismo Algorítmico*. Blog do Tarcízio Silva, 2020. Disponível em: <http://https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo>. Acesso em: 18 mar. 2021.

SILVEIRA, Sergio Amadeu. *Governo dos Algoritmos*. Revista de Políticas Públicas, vol. 21, nº 1, São Luís. 2017, p. 267-281.

SILVEIRA, Sergio Amadeu. *Democracia e os códigos invisíveis*. Edições Sesc. São Paulo, 2019. Edição do Kindle.

SOLOVE, Daniel J. A *taxonomy of privacy*. University of Pennsylvania Law Review, 2006. p. 477–564.

SOLOVE, Daniel J. *Understanding Privacy*. New York: Harvard University Press, 2008. Edição do Kindle.

SOLOVE, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. New York: Harvard University Press, 2004. Versão Ebook.

SPANIOL, Bruna Paiani Nasser**.** *A vigilância na internet: a circulação midiática brasileira do vazamento de dados da NSA por Edward Snowden*. 2015. Dissertação de Mestrado, Universidade Federal do Rio Grande do Norte, Natal, 2015.

TAYLOR, Mistale. *Permissions and Prohibitions in Data Protection Jurisdiction*. Brussels Privacy Hub, vol.2, nº 6, 2016.

TARTUCE, Flávio. *Manual de direito civil: volume único*. 4ª ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: Método, 2014, p. 166-167.

THE GUARDIAN. *Edward Snowden: the whistleblower behind the NSA surveillance revelations*. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance >. Acesso em: 14 nov. 2020.

THE GUARDIAN. *NSA collecting phone records of millions of Verizon customers daily*. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order >. Acesso em: 14 nov. 2020.

THIBES, Mariana Medeiros. Conflitos socioambientais e áreas de preservação permanente em meio urbano: o caso da Vila do Arvoredo, município de Florianópolis, SC. 2014. 261f. 2014. Tese de Doutorado. Universidade Federal de Santa Catarina, Florianópolis, p. 87-91.

TUNES, Suzel. *Algoritmos parciais.* Como a inteligência artificial absorve padrões discriminatórios e o que a ciência pode fazer para evitar essas distorções. 2019. Disponível em: <https://revistapesquisa.fapesp.br/algoritmos-parciais/>. Acesso em: 15 abr. 2021.

UNESCO. *Devemos instruir os algoritmos*. 2020. Disponível em: <https://pt.unesco.org/courier/suplemento-online/devemos-instruir-os-algoritmos>. Acesso em: 15 abr. 2021.

UNIÃO EUROPEIA. *Diretiva 95/46/CE da União Europeia*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>. Acesso em 20. mar. 2020.

VÉLIZ, Carissa. *Privacy is Power: Why and how You Should Take Back Control of Your Data*. Random House, 2020. Edição do Kindle.

VENTURA, Miriam; COELI, Cláudia Medina. *Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança*. Cadernos de Saúde Pública, v. 34, 2018.

VIANNA, William Barbosa; DUTRA, Moisés Lima; e FRAZZON, Enzo Morosini. *Big data e gestão da informação: modelagem do contexto decisional apoiado pela sistemografia*. Informação & Informação, v. 21, n. 1, 2016, p. 185. Disponível em: <http://www.uel.br/revistas/uel/index.php/informacao/article/view/23327/18993>. Acesso em: 29 mar. 2021.

VIERA, Tatiana Malta. *O direito à Privacidade na Sociedade informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Dissertação (Mestrado) – Universidade de Brasília, Programa de Pós-Graduação em Direito, Estado e Sociedade, 2007.

VILICIC, Filipe. *AVISO: Nenhum algoritmo é "neutro". Nem o do Facebook, nem o de ninguém*. 2020. Disponível em: < https://veja.abril.com.br/blog/a-origem-dos-bytes/aviso-nenhum-algoritmo-e-neutro-nem-o-do-facebook-nem-o-de-ninguem/>. Acesso em: 29 mar. 2021.

ZARSKY, Tal. *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making*. Science, Technology, & Human Values, v. 41, nº 1, p. 118-132, 2016.

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância. A luta por um futuro humano na nova fronteira do poder*. Trad. George Schlesinger. Rio de Janeiro: Intrínseca, 2021. Edição do Kindle.

WARREN, Samuel; BRANDEIS, Louis D. *The right to privacy*. Harvard Law Review. Cambridge: Harvard Law Review Association, nº 193, 1890.

WESTIN, Alan. *Privacy and Freedom*. Wash. & Lee Law Review, 1968. Disponível em: <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20>. Acesso em: 15 ago. 2020.