doi.org/10.51891/rease.v10i11.16492

ANÁLISE DAS QUESTÕES ÉTICAS E LEGAIS EM TORNO DA PRIVACIDADE DIGITAL

João Marcos Amorim Medeiros[1]
Thiago de Almeida Feller[2]

RESUMO: A Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018, surge em um contexto onde os dados pessoais se tornaram a nova moeda de troca no mercado. A LGPD visa proteger os direitos dos titulares desses dados, abordando questões como a portabilidade, correção e eliminação de informações pessoais, garantindo transparência e segurança na coleta e uso desses dados. A aplicação da lei é ampla, abrangendo tanto entidades públicas quanto privadas, atingindo dados coletados no Brasil ou destinados a indivíduos brasileiros. No entanto, a LGPD não se aplica a tratamentos realizados para fins exclusivamente pessoais, jornalísticos, artísticos ou de segurança pública. A implementação da LGPD enfrenta desafios, especialmente considerando a globalização e o fluxo intenso de dados internacionais, o que ressalta a necessidade de uma abordagem colaborativa e de regulamentos similares em nível global. A legislação busca alinhar-se com o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, embora a versão brasileira seja mais flexível em alguns aspectos. A LGPD estabelece princípios fundamentais, como finalidade, necessidade e segurança, que orientam a proteção de dados pessoais e visam reduzir práticas prejudiciais. A lei também prevê penalidades para infratores, incluindo multas significativas, destacando a importância de uma governança corporativa adequada para garantir conformidade. Em suma, a LGPD representa um avanço significativo na proteção de dados, exigindo uma rápida adaptação por parte das organizações e promovendo a discussão sobre a privacidade e a ética no tratamento de informações pessoais.

Palavras-chave: LGPD. Proteção de dados. Privacidade. Penalidades. Conformidade.

ABSTRACT: The General Data Protection Law (LGPD), established by Law No. 13,709/2018, appears in a context where personal data has become the new currency in the market. The LGPD aims to protect the rights of data holders, addressing issues such as portability, correction and deletion of personal information, and ensuring transparency and security in the collection and use of this data. The application of the law is broad, covering both public and private entities and affecting data collected in Brazil or intended for Brazilian individuals. However, the LGPD does not apply to treatments carried out for exclusively personal, journalistic, artistic or public security purposes. The implementation of the LGPD faces challenges, especially considering globalization and the intense flow of international data, which highlights the need for a collaborative approach and similar regulations at a global level. The legislation seeks to align with the European Union's General Data Protection Regulation (GDPR), although the Brazilian version is more flexible in some aspects. The LGPD establishes fundamental principles, such as purpose, necessity and security, that guide the protection of personal data and aim to reduce harmful practices. The law also provides penalties for violators, including significant fines, and highlights the importance of adequate corporate governance to ensure compliance. In short, the LGPD represents a significant advance in data protection, requiring rapid adaptation by organizations and promoting discussion about privacy and ethics in the treatment of personal information.

Keywords: LGPD. Data Protection. Privacy. Penalties. Compliance.

[1]Acadêmico da universidade UNIRG.
[2]Docente da universidade, Perito Papiloscopista e Mestre em Gestão de Políticas Públicas.

INTRODUÇÃO

Esta pesquisa visa relacionar a disposição de dados pessoais, a manipulação e a predição comportamental com a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), por meio de uma análise aprofundada das obras de especialistas nas áreas de direito, economia e ciência da computação. O objetivo é ilustrar os desafios a serem enfrentados em um contexto social complexo e dinâmico.

O tema é parte do direito civil e está em rápida evolução devido às novas tecnologias e mudanças sociais. No entanto, essas mudanças exigem uma reflexão correspondente sobre as questões éticas e jurídicas envolvidas. A importância da proteção de dados pessoais no Brasil é evidenciada pelas seguintes estatísticas:

Em 2016, a Internet estava presente em 69,3% dos domicílios permanentes do país, e esse percentual aumentou para 74,9% em 2017. A adoção da Internet nas áreas rurais cresceu mais rapidamente do que nas áreas urbanas, diminuindo a grande disparidade entre essas regiões. Nas áreas urbanas, a porcentagem de domicílios com Internet foi de 75,0% em 2016 e subiu para 80,1% em 2017, enquanto nas áreas rurais, aumentou de 33,6% para 41,0%. Esse padrão de crescimento foi observado em todas as Grandes Regiões (IBGE, 2017).

O trabalho é estruturado em cinco capítulos. O primeiro capítulo analisa a transformação social moderna em uma sociedade informacional, onde a conectividade e a inovação tecnológica revolucionaram os negócios, as relações interpessoais, os valores éticos e até o conceito de privacidade. Esta transformação é explicada através do panoptismo desenvolvido por Foucault e Bentham, aplicando-o ao contexto atual.

O segundo capítulo define termos essenciais para entender como a personalidade do indivíduo se estende ao ambiente virtual, justificando a proteção jurídica dos direitos fundamentais desde a Carta Magna até a Lei Geral de Proteção de Dados (LGPD).

No terceiro capítulo, é detalhado o paradoxo da coleta de informações pelos usuários da rede como moeda de troca por bens ou serviços, introduzindo o aspecto monetário dos dados pessoais. Inclui também um subtópico dedicado à compreensão do funcionamento do mercado de dados.

O quarto capítulo constitui o núcleo do trabalho, abordando o viés jurídico das tensões discutidas anteriormente. Examina a evolução normativa dos direitos fundamentais relacionados à proteção de dados pessoais, os princípios que regem essa proteção, as legislações

anteriores que ofereceram amparo jurídico e a regulação europeia que impulsionou o debate nacional e levou à criação da LGPD.

Por fim, o quinto capítulo realiza uma análise crítica da Lei Geral de Proteção de Dados, apontando as possíveis adversidades e limitações que a norma enfrentará para alcançar sua plena eficácia. O tema será tratado metodologicamente para demonstrar que, além do rigor normativo necessário, há uma carência de ética e justiça no tratamento dos dados como simples estatísticas. Isso pode definir padrões de consumo e controle, influenciar consciências, restringir a liberdade de escolha do indivíduo e estabelecer padrões discriminatórios, ameaçando e violando direitos fundamentais como privacidade, intimidade e liberdade.

1 SOCIEDADE INFORMACIONAL

O ser humano, como um ser altamente adaptável e em constante evolução, passou por diversas revoluções em busca do aprimoramento do seu eu-consciente. Momentos cruciais resultaram em mudanças de comportamento, destino e crenças da humanidade, culminando no atual marco extraordinário em que os indivíduos são vistos como "chips" compartilhadores de informações inseridos em uma vasta rede (HARARI, 2000).

Sinais dessa transformação já eram visíveis na sociedade pré-industrial: a documentação das relações pessoais era limitada a uma pequena parte da vida das pessoas, restrita a uma elite dominante. A rotina diária das pessoas comuns não era registrada de forma escrita. Coletar todos os tipos de dados sobre esses cidadãos era extremamente fácil, considerando que a maioria das relações pessoais ocorria de maneira presencial. As relações negociais eram seladas por aperto de mão e testemunhadas por outros (SCAAR, 2011).

Com o tempo, as relações complexas e confusas substituíram as interações “boca a boca”. A perda de confiança nas relações pessoais levou à diminuição dessas interações e ao estabelecimento de relações racionais, marcando o início do armazenamento documentado de informações. O modelo de produção industrial impulsionou a consolidação do registro de fatos e eventos diários como forma de coleta de evidências. Esse processo inicial de armazenamento, documentação e uso de informações pessoais foi o que deu origem à sociedade informacional como a conhecemos atualmente.

Houve uma época em que um computador era visto como uma máquina enorme e difícil de entender e manusear. Com a chegada dos “computadores pessoais” no mercado, entre as décadas de 80 e 90, a internet se expandiu até se tornar essencial. Essa evolução tecnológica e

sua acessibilidade impactaram tanto a sociedade que, atualmente, um smartphone possui mais de 100.000 vezes o poder de processamento do computador usado na missão Apollo 11, que levou o homem à Lua há 50 anos (GNIPPER, 2019).

A integração do computador como um objeto pessoal desencadeou o processo de armazenamento e análise de dados relacionados à vida pessoal de terceiros. Quando setores econômicos e o próprio Estado reconheceram a utilidade da coleta e armazenamento de informações pessoais, começou o processo de panoptização social.

1.1 Panoptização Social

O Panoptismo de Foucault (2014), inspirado por Jeremy Bentham, foi desenvolvido na década de 1970 e descreve o padrão da sociedade contemporânea por meio das novas técnicas de vigilância. Para Foucault, o Panóptico representa como a tecnologia de vigilância e controle opera, permitindo uma visão privilegiada das ações e comportamentos daqueles que são monitorados. Nesse modelo de monitoramento, chamado "panoptismo", o espetáculo se inverte: "em vez de a multidão observar o que acontece com alguns poucos, são poucos que observam o que acontece com a multidão" (VEIGA, 2019).

A consequência mais previsível dessa concentração de poder é a capacidade de influenciar o comportamento das pessoas; o domínio onde esse poder é exercido (FOUCAULT, 2005, p. 169). Foucault sugere que o principal objetivo desse monitoramento é econômico, pois o controle de um grande número de pessoas é exercido por poucos observadores. Portanto, "o panoptismo representa a base do poder-saber, que regula a vida dos indivíduos e serve como protótipo dos sistemas sociais de controle e vigilância (total) presentes atualmente" (OLIVEIRA; CARNEIRO, 2016).

No contexto do panoptismo social criado pelas tecnologias e plataformas, há um fator distintivo: o indivíduo se permite ser persuadido não mais pelos argumentos, mas pelo contexto de submissão em que é praticamente conduzido à aceitação (OLIVEIRA; CARNEIRO, 2016). No cenário contemporâneo, essa busca por controle se manifesta na constante procura por uma sensação de segurança, vigilância permanente e maior visibilidade. No entanto, isso apresenta uma contradição interna, refletida na exposição pública do indivíduo nas comunicações digitais e nas redes sociais, onde há um escambo de "privacidades" no espaço público, promovendo a publicidade das intimidades. As redes sociais representam o modelo panóptico mais recente, enquanto o panoptismo se manifesta na proliferação de dispositivos digitais que, em nome da

conectividade e da formação de 'networks', replicam informações pessoais nos ambientes virtuais (OLIVEIRA; CARNEIRO, 2016, p. 215).

O panoptismo exercido pela internet alcança dimensões que vão além da compreensão dos que dela se utilizam. Foucault alertou para a capacidade dos modelos de vigilância se adaptarem a diferentes contextos, apresentando uma aparência inocente, mas suspeita; as tecnologias obedecem às economias de mercado com seus próprios interesses (FOUCAULT, 2005, p. 120). Segundo Oliveira e Carneiro (2018):

Enquanto no "panoptismo tradicional", a pessoa é monitorada contra sua vontade, embora sua integridade seja teoricamente garantida pelo agente monitorador, no contexto das tecnologias da informação, as pessoas agem de forma deliberada, oferecendo voluntariamente suas informações pessoais, o que vulnerabiliza sua integridade e a torna passível de manipulação pelos responsáveis pelo monitoramento.

Assim, a privacidade é sacrificada em prol de uma sensação de segurança, possibilitando novas formas de dominação, disfarçadas sob valores supostamente universais. Com o advento da 4ª Revolução Industrial (SCHWAB, 2019), a inteligência artificial (IA), a robótica e a internet das coisas (IoT) intensificaram a cultura do monitoramento, mesmo que essa intenção seja negada e até desacreditada por muitos. Além disso, a sociedade passou a compartilhar uma quantidade sem precedentes de informações em uma conexão global.

Nessa sociedade informacional (ou sociedade em rede), descrita por Manuel Castells (2002), vivemos em uma realidade cada vez mais permeada pela tecnologia, conectada e interligada, com uma produção de dados e informações em volumes imensos.

Em termos práticos, a evolução mercadológica e tecnológica não permite uma vida austera em isolamento. Portanto, é crucial ressaltar que este trabalho não se dedica a combater esses setores, mas a apontar a falta de transparência e de informações das instituições públicas e privadas em relação aos titulares dos dados. Não parece razoável exigir tanto dos indivíduos e tão pouco das organizações que ocultam a finalidade e o modo de uso das informações que possuem. O resultado é a coleta e uso de dados pessoais como matéria-prima para manipulação de comportamentos, criação de um falso sentimento de liberdade e invasão da privacidade.

Portanto, entende-se que, até certo ponto histórico, a proteção jurídica dos direitos à privacidade, liberdade e igualdade foi suficiente. Hoje, dadas as situações descritas, é evidente a necessidade de estabelecer novos limites, adequados à realidade de uma sociedade

informacional. Nesse contexto prospectivo, torna-se essencial o estudo da proteção dos dados pessoais.

2 DADOS PESSOAIS E DADOS SENSÍVEIS

Com base nas premissas apresentadas no Capítulo 1, é crucial definir os conceitos básicos para entender como a identidade do indivíduo se estende ao ambiente virtual por meio de seus dados pessoais.

Nesse contexto, a nova Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018) define os seguintes termos (BRASIL, 2018):

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a uma pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, crença religiosa, opinião política, afiliação a sindicato ou a organização de caráter religioso, filosófico ou político, dado relacionado à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III - dado anonimizado: dado relativo a um titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis no momento de seu tratamento;
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou vários locais, em suporte eletrônico ou físico;
>
> V - titular: pessoa natural a quem se referem os dados pessoais que estão sendo tratados;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

De acordo com Maria Luciana Pereira de Souza em sua dissertação de mestrado (SOUZA, 2018, p. 76), dado pessoal é informação de qualquer natureza, registrada em qualquer modalidade de suporte, relacionada a uma pessoa identificada ou identificável.

Com isso, a ampla gama de informações que cada usuário da rede gera pode ser dividida em duas categorias: dados pessoais e dados pessoais sensíveis, sendo os últimos protegidos por normas especiais e confidencialidade.

A LGPD define dados sensíveis como todo dado pessoal relacionado a origem racial ou étnica, crença religiosa, opinião política, afiliação a sindicato ou a organização de caráter religioso, filosófico ou político, informação sobre saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

O caráter sigiloso e confidencial dos dados sensíveis levanta preocupações sobre aspectos legais e éticos relacionados ao seu vazamento, armazenamento e segurança. A Comissão Europeia (2018, p. 2) ressalta que tais dados só podem ser coletados e utilizados sob condições específicas, como consentimento explícito ou quando permitido pela legislação nacional, como será detalhado no Capítulo 6.

Além disso, é importante distinguir que a presença de dados sensíveis dentro dos dados pessoais não implica que todos os dados sensíveis sejam pessoais, e que até mesmo pessoas jurídicas e o governo possuem proteção em relação a esses dados sensíveis, conforme explica Vignoli, Richele e Vechiato (2019):

Há a possibilidade de Dados Sensíveis dentro dos Dados Pessoais. No entanto, nem todo Dado Pessoal é sensível, e nem todo Dado Sensível é pessoal. É necessário esclarecer que Dados Sensíveis podem ocorrer tanto em dados de pessoas naturais quanto jurídicas (VIGNOLI; VECHIATO, 2019).

Contrariando o que está previsto na Lei Geral de Proteção de Dados Pessoais (LGPD), os Dados Pessoais propriamente ditos são considerados sensíveis sempre que expõem seu titular a situações constrangedoras ou discriminatórias, como informações sobre remuneração, notas acadêmicas, faturas, dados médicos, acordos conjugais, declaração de imposto de renda. Assim, observa-se uma ampliação do caráter da lei desde antes de sua vigência.

2.1 *Big Data e Big Analytics*

Com a definição inicial de dados pessoais estabelecida, é importante considerar a possibilidade de transformá-los em matéria-prima para um produto comercial muito mais valioso: a informação.

Nesse contexto, informações são dados pessoais que foram devidamente processados, e quando essa informação é processada, transforma-se em conhecimento, como explica Ana Frazão (2018):

> Para entender a importância do *big data* na concorrência, é necessário distinguir entre dados, informação e conhecimento. Simplificadamente, dados são considerados como matérias-primas para a informação, e a informação é uma matéria-prima para o conhecimento, que resulta de uma análise mais profunda – e idealmente aplicável – sobre um determinado assunto.

O termo Big Data refere-se ao grande volume de dados brutos, não agregados e não organizados, gerados rapidamente e em grande variedade, que precisam ser processados para se tornarem valiosos, organizados e armazenados.

Big Analytics é o processo de análise e transformação do Big Data com o objetivo de identificar padrões e tirar conclusões a partir da informação. Esse tratamento é realizado por computadores, podendo incluir técnicas estatísticas, algorítmicas e computacionais, para possibilitar uma melhor compreensão e tomada de decisões e automação de processos.

A partir disso, surge um novo tipo de conhecimento denominado Data Insight, que é a análise do comportamento do usuário capaz de influenciar decisões importantes no mercado ou até mesmo criar Produtos Orientados por Dados (Data-Driven Product).

Sem esses instrumentos, ter uma grande quantidade de dados seria inútil sem a capacidade de transformá-los rapidamente e de maneira eficiente em informações que geram valor de mercado, conforme observa Frazão (2018):

Os dados precisam ser processados e trabalhados para gerar valor. Embora os dados isolados ou "crus" sejam importantes, é fundamental reconhecer que o simples acesso aos dados, sem a capacidade efetiva e eficiente de transformá-los em informação, pode ser insuficiente para obter benefícios econômicos.

Assim, a qualidade do tratamento dos dados se torna mais relevante do que a velocidade com que é realizado, pois determinará seu valor e importância.

De acordo com a LGPD, o tratamento é definido no art. 5º, inciso X, como “toda operação realizada com dados pessoais, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” realizada com o uso de ferramentas tecnológicas, identificando padrões de comportamento humano, catalogando, classificando ou etiquetando indivíduos.

Observa-se que a maioria das plataformas digitais utiliza Big Data e Big Analytics para seu funcionamento e até mesmo para sua existência, pois precisam acessar o maior número possível de dados dos usuários para convertê-los em informações e, a partir disso, usar essas informações em seus negócios, compartilhá-las com parceiros comerciais ou tomar decisões.

Nesse contexto, Renato Opice Blum destaca:

> Estamos vivendo uma verdadeira revolução nos métodos de organização, registro e uso de dados e informações pessoais. Imagine centralizar e cruzar informações de uma administradora de cartões de crédito com dados bancários, informações sobre patrimônio imobiliário, veículos, acesso à internet, contatos e dados coletados de diversas fontes, hábitos de compras, perfil em redes sociais, etc. Considerando os vários bancos de dados disponíveis na internet, ao reunir esses dados em um só lugar e cruzá-los, é possível conhecer muito bem uma pessoa. A novidade da sociedade

> contemporânea é que as informações pessoais estão se tornando cada vez mais acessíveis a quem quiser (e puder pagar). Isso permite conhecer profundamente qualquer pessoa, influenciar sua vida, seu cotidiano e suas oportunidades (BLUM; ELIAS, 2011).

A realidade descrita pelo autor levanta preocupações éticas e jurídicas significativas. A tecnologia atual, que rapidamente se torna obsoleta diante das novas inovações, permite a análise de grandes conjuntos de dados, possibilitando resultados analíticos precisos sobre o ser humano.

Nesse sentido, Souza (2018) complementa:

> De maneira geral, um like, um compartilhamento, uma interação, um check-in com geolocalização, um download, um login, uma busca, enfim, qualquer ação realizada na rede mundial de computadores permite o armazenamento e a análise da informação. As técnicas de tratamento de dados deram origem a tecnologias como Big Data, Data Analytics, Business Intelligence, além de Machine Learning e Inteligência Artificial (HOWARD; TONY, 2017, p. 45).

Este novo cenário evidencia a capacidade de transformação da internet e da tecnologia na sociedade, levantando questões nunca antes imaginadas. É devido a esse paradoxo entre a ficção e a realidade iminente, bem como o risco de violação de princípios fundamentais, que este estudo e legisladores em todo o mundo estão focados na proteção de dados pessoais, buscando garantir a dignidade humana, especialmente em relação à liberdade, igualdade, privacidade e autodeterminação informacional.

3 A MONETIZAÇÃO DOS DADOS PESSOAIS

Na economia capitalista moderna, a informação ocupa um papel comparável ao do petróleo no início do século XX. Sendo o novo "petróleo" do século XXI, suas reservas estão localizadas em bancos de dados públicos. No entanto, essa mudança não visa substituir os recursos antigos, mas sim transformar a maneira de gerar riqueza. Assim, a produção de valor torna-se mais econômica e simplificada.

Observa-se que, entre as diversas atividades realizadas por usuários da internet, apenas uma pequena parte das ferramentas (programas e aplicativos) é efetivamente remunerada pelos seus usuários. Por isso, os desenvolvedores criaram alternativas para financiar seus negócios, como a cobrança por funcionalidades avançadas, a venda de marketing direcionado e a monetização de dados pessoais.

Nesse contexto, Guimarães (2018) explica:

> A monetização ocorre no âmbito do 'Big Data' — um conceito que abrange a coleta, armazenamento, processamento e capitalização de dados e informações. Com o tratamento desses dados, é possível, por exemplo, aprimorar a publicidade direcionada

> com base em padrões de acesso e consumo e até influenciar o comportamento do usuário da internet, decidindo o que mostrar ou não mostrar, e também influenciar resultados de processos políticos, conforme sugerem alguns estudiosos.

Nesse processo, são gerados insights automatizados, que consistem no mapeamento de dados para definir o perfil do usuário (suas preferências de consumo, gostos pessoais, entre outros). A partir desses insights, pode-se aumentar a retenção de clientes e obter vantagens competitivas.

Com a mudança no comportamento dos consumidores, que buscam ser vistos como indivíduos e não apenas números, as ofertas personalizadas têm atraído atenção. Muitas empresas estão se especializando na coleta de dados, desenvolvendo expertise para descrever seus usuários com precisão em termos de preferências, opiniões, hábitos de consumo, entre outras características.

Inicialmente, a regulamentação era feita apenas por políticas de privacidade e termos de uso das plataformas. No entanto, a falta de transparência das empresas e a negligência dos usuários em relação aos termos de uso levaram à necessidade de criar normas legais que garantam a proteção dos direitos dos usuários.

Têmis Limberger posiciona-se sobre isso:

> A necessidade de proteger juridicamente o cidadão surge porque os dados têm valor econômico, devido à possibilidade de comercialização. Com as novas técnicas informáticas, a intimidade ganha um novo significado, pois se busca proteger o cidadão em relação aos dados informatizados. O indivíduo que confia seus dados deve ter proteção jurídica para garantir que esses dados sejam utilizados corretamente, tanto por entidades públicas quanto privadas. Os dados refletem aspectos da personalidade e revelam comportamentos e preferências, permitindo até mesmo traçar um perfil psicológico dos indivíduos. Isso pode destacar hábitos de consumo importantes para a publicidade e o comércio eletrônico. É possível criar uma imagem detalhada da pessoa, que pode incluir aspectos íntimos. O cidadão torna-se, então, um 'homem de cristal'.

As novas tecnologias transformam a informação em um recurso fundamental para a sociedade. Os programas interativos criam uma nova forma de mercadoria. O indivíduo fornece dados de maneira espontânea e, uma vez armazenados, esquece-se de sua origem. Portanto, é necessário estabelecer uma proteção eficaz para o consumidor. Os meios de comunicação interativos alteram a capacidade de coleta de dados, permitindo uma comunicação contínua e direta entre os gestores dos serviços e os usuários. Isso possibilita não apenas o controle do comportamento dos usuários, mas também um conhecimento mais detalhado sobre seus costumes, preferências e interesses. A partir disso, surge uma série de usos secundários dos dados coletados. A função da privacidade no âmbito digital não é apenas proteger a esfera pessoal da pessoa, evitando que ela seja incomodada pelo uso indevido de seus dados. Também

busca evitar que o cidadão seja tratado como uma mercadoria, sem considerar seus aspectos subjetivos e sua intimidade (LIMBERGER, 2008, p. 219).

Atualmente, é difícil para um indivíduo manter o controle total sobre suas informações e características pessoais após inseri-las na internet, o que confirma as palavras de Chiara Teffé (2017, p. 122): "A velocidade da circulação da informação é inversamente proporcional à capacidade de seu controle, correção e eliminação."

Por outro lado, a conscientização dos usuários de redes sociais sobre a entrega excessiva e voluntária de seus dados pessoais aumentou, especialmente após escândalos recentes envolvendo o uso inadequado dessas informações por agentes autorizados e não autorizados.

O escândalo da Cambridge Analytics e do Facebook levantou questões sobre a solidez e integridade dos processos eleitorais democráticos das eleições nos EUA e do Brexit, após a descoberta de que dados pessoais foram mal utilizados para manipular a opinião pública.

Assim, o grande desafio relacionado à coleta de uma quantidade imensa de dados pessoais é como essas informações serão protegidas e utilizadas. Alguns sites afirmam ter políticas de privacidade e proteção de dados, mas muitas vezes de forma vaga e superficial, sem detalhes sobre o processamento, armazenamento ou tempo de retenção dos dados. Outra falha significativa é a falta de treinamento dos funcionários, o que pode resultar em perdas e compartilhamento não autorizado das informações pessoais.

O uso econômico de dados, especialmente nas redes sociais, gera preocupações sobre a privacidade dos usuários da internet e de seus serviços. Muitas vezes, esses dados são coletados sem o devido consentimento dos usuários, que também ignoram o destino e a finalidade das informações.

É importante notar que os dados pessoais de um indivíduo podem ser amplamente utilizados. O Facebook, por exemplo, desenvolveu um aplicativo em teste chamado Study, que converte a disposição de dados pessoais (como aplicativos instalados, tempo gasto em cada aplicativo, país, modelo do dispositivo e tipo de conexão) em remuneração, tentando combinar a necessidade de insumos para a plataforma com o desejo de ganhar dinheiro dos participantes.

A empresa compromete-se, por meio de termos de uso e privacidade, a não divulgar ou revender os dados coletados, nem a coletar informações de logins ou senhas, mas apenas o necessário para melhorar o próprio Facebook de forma transparente.

Esse exemplo ilustra que a Lei Geral de Proteção de Dados busca garantir a liberdade do indivíduo para decidir sobre sua privacidade, desde que essa decisão seja livre, voluntária e consentida. Todos têm a liberdade de dispor de seus dados pessoais.

Enquanto o setor privado enfrenta os dilemas éticos e jurídicos descritos, o setor público enfrenta o desafio de se adaptar às mudanças sociais e inovações tecnológicas que ocorrem constantemente em um espaço virtual. Isso revela o caráter desterritorializante do ciberespaço e o consequente enfraquecimento da soberania dos Estados, como expõe Pierre Lévy:

> O ciberespaço é, por natureza, desterritorializante, enquanto o Estado moderno se baseia na noção de território. Na rede, bens informacionais (programas, dados, informações, obras de todos os tipos) podem transitar instantaneamente de um ponto a outro do planeta digital sem passar por qualquer tipo de fiscalização. Serviços financeiros, médicos, jurídicos, de educação a distância, aconselhamento, pesquisa e desenvolvimento, e processamento de dados também podem ser oferecidos de forma instantânea e quase invisível por empresas ou instituições estrangeiras. O Estado perde o controle sobre uma parte cada vez mais significativa dos fluxos econômicos e informacionais transfronteiriços. Além disso, as legislações nacionais só podem ser aplicadas dentro das fronteiras dos Estados. O ciberespaço permite que leis relacionadas à informação e comunicação (censura, direitos autorais, associações proibidas etc.) sejam facilmente contornadas. Um servidor que distribua ou organize comunicação proibida instalado em qualquer 'paraíso de dados', em qualquer lugar do mundo, fica fora da jurisdição nacional. Como os indivíduos podem se conectar a qualquer servidor globalmente, as leis nacionais sobre informação e comunicação se tornam inaplicáveis (LEVY, 1999, p. 312).

Na corrida pela modernização do setor público, o governo brasileiro investe pesadamente em tecnologias para reduzir a insatisfação com um sistema rígido e burocrático, reduzir custos, aumentar a transparência dos atos e gastos públicos, melhorar a qualidade dos serviços e estabelecer um diálogo direto entre cidadãos e administração pública.

Essas modernizações incluem o uso de blockchains para autenticação e emissão de certidões online, criação de portais com informações relevantes, ensino a distância, consulta online ao imposto de renda, entre outras. No entanto, a ampla utilização de tecnologias na gestão e controle de estruturas essenciais implica em vulnerabilidades, com possíveis fragilidades nos sistemas públicos que, se descobertas e exploradas por agentes mal-intencionados, podem causar incidentes de segurança irreparáveis.

Atualmente, um ataque cibernético pode interromper o fornecimento de água ou energia em cidades inteiras, e a rede de transporte aéreo, que depende totalmente de computadores, está sujeita a ataques e falhas. Quanto mais o governo e seus cidadãos dependem da tecnologia, maior é a exposição a ataques de crackers, hackers e organizações criminosas, e aos chamados crimes cibernéticos.

No cenário nacional, os dados indicam que 32% dos serviços do governo federal brasileiro são totalmente digitalizados, 39% parcialmente e 29% não estão disponíveis online, conforme levantamento parcial do Ministério do Planejamento (BRASIL, 2017). Esse aumento na utilização de tecnologias para serviços públicos levanta questões sobre a capacidade dos órgãos governamentais de garantir a privacidade dos cidadãos, dada a lenta evolução da segurança da informação nos setores privado e público.

3.1 A Economia de Atenção e o Capitalismo de Vigilância

Com a expansão global da Internet, economias, valores e sociedades inteiras passaram por profundas transformações. A noção de privacidade, anteriormente entendida como "o direito de ser deixado em paz", mudou radicalmente com o surgimento do ambiente virtual, sendo redefinida como a capacidade de cada pessoa controlar o uso das informações que dizem respeito a ela.

Dessa forma, é fundamental considerar o controle exercido por grupos econômicos que baseiam suas operações na disponibilização de informações. Essa discussão sobre a redefinição da privacidade exige que busquemos equilíbrios sócio-políticos que estejam mais alinhados com os objetivos e valores de um Estado Democrático de Direito.

Os conceitos de “capitalismo de vigilância” e “economia de atenção” destacam a necessidade de criar fronteiras que se ajustem à realidade digital.

De uma perspectiva mais ampla, o Estado deve reconhecer que indivíduos e a sociedade demandam uma convivência democrática, transparente e organizada de maneira muito diferente do pensamento antiquado de três décadas atrás, o que inclui a proteção adequada contra registros, manipulações e distorções.

A economia de atenção refere-se à “alocação do tempo e da atenção das pessoas diante de uma infinidade de atividades, negócios e relacionamentos possíveis”, segundo Ana Frazão (2018). A preocupação com esse novo modelo econômico surge da transformação das necessidades tradicionais para a indução de avaliações e escolhas, influenciando o que fazer, adquirir e com quem, limitando as opções disponíveis para o usuário. Como Tim Wu explica:

> A atenção dos usuários tornou-se um dos maiores bens disputados pelos agentes da economia digital. Quanto mais tempo as pessoas passam em determinadas plataformas, mais intensamente são expostas à publicidade e à coleta de seus dados, além de serem mais suscetíveis a estratégias que visam influenciar e alterar suas preferências e visões de mundo (FRAZÃO, 2018).

Nesse cenário, as plataformas digitais concentram um grande poder na economia digital, intermediando de maneira eficiente e rápida uma variedade de relações. Essas circunstâncias podem ameaçar a própria democracia, ao prejudicar o debate público e criar uma "bolha social", onde os filtros fornecem aos usuários apenas o que eles querem ver. Esse tipo de seleção pode polarizar opiniões, tornando os usuários vulneráveis a manipulações e comprometendo a legitimidade das instituições democráticas.

Além disso, como já foi mencionado, para utilizar essas plataformas, é necessário fornecer dados pessoais suficientes para revelar detalhadamente a identidade de uma pessoa. É justamente a capacidade reveladora desses dados que os torna valiosos e perigosos, exigindo proteção e controle rigorosos.

Uma das características mais importantes das plataformas digitais é sua vasta capacidade de conectar usuários, agentes econômicos e governos. Atualmente, os maiores detentores de poder econômico são aqueles que exploram plataformas, utilizando seu poder de conexão para atrair relacionamentos e negócios. Exemplos incluem o Facebook conectando pessoas, bens e serviços; a Amazon conectando fornecedores e consumidores; e o Airbnb conectando propriedades e pessoas (FRAZÃO, 2018).

Como conhecer um público-alvo é uma tarefa complexa e cara, plataformas sofisticadas como Google e Facebook oferecem uma solução importante através dos dados pessoais que possuem. Ana Frazão (2018, p. 78) observa que:

> São inúmeros os benefícios e eficiências advindos, pois as plataformas digitais reduzem significativos custos de transação e agregam valor para seus usuários, superando obstáculos que podem dificultar as transações e oferecendo recursos valiosos para melhorar as combinações. Esses recursos vão desde informações sobre a qualidade das ofertas e a reputação dos agentes (como as diversas formas de rating) até recomendações de produtos que correspondam aos gostos e preferências dos consumidores.

Sob essa perspectiva, a tecnologia pode estar sendo usada contra nossa própria individualidade, uma vez que existem máquinas capazes de conhecer melhor as pessoas do que elas mesmas, prever suas ações e interações e até explorar vulnerabilidades para manipular sentimentos, crenças e ideias para diversos fins, inclusive políticos, como demonstrado nas eleições de Donald Trump e no Brexit.

O poder, nesse novo modelo econômico, é visto como a capacidade de influenciar pessoas, o que amplia as ameaças para além da privacidade, liberdade e identidade pessoal, afetando a cidadania e a democracia. Os agentes que controlam grandes bancos de dados se

posicionam não apenas como concorrentes, mas como o próprio mercado, dominando informações sobre milhares de usuários.

A autora destaca que o "imperativo de extração" de dados criou uma economia de escala cuja vantagem singular é a capacidade de prever comportamentos individuais, que se torna um ativo comercializável. O trecho abaixo ilustra essa realidade:

> A primeira onda de produtos preditivos foi impulsionada pelo excedente extraído em larga escala na internet para produzir anúncios online 'relevantes'. A etapa seguinte focou na qualidade das previsões. Para alcançar a maior certeza, as melhores previsões devem estar o mais próximas possível da observação. Ao imperativo da extração somou-se o imperativo da previsão, manifestando-se inicialmente por economias de escopo. Em uma fase ainda mais ousada, a coleta de dados para aprofundamento visa obter previsões comportamentais mais precisas e lucrativas, investigando aspectos mais íntimos da personalidade, humor, emoções, mentiras e fragilidades dos usuários. Todos os níveis da vida pessoal seriam capturados e compactados em um fluxo de dados destinados a criar certeza. Sob a aparência de 'personalização', grande parte desse trabalho envolve uma extração intrusiva dos aspectos mais íntimos do cotidiano. Com o aumento da corrida pelos lucros gerados pela vigilância, os capitalistas percebem que economias de escopo não são suficientes. O excedente comportamental deve ser abundante e variado, mas a maneira mais segura de prever o comportamento é moldar a própria fonte. Chamo de 'economias de ação' os processos criados para isso: softwares configurados para intervir diretamente nas situações da vida real sobre pessoas e coisas reais (ZUBOFF, 2019, p. 57).

A autora descreve claramente a evolução e as novas ambições na gestão de dados pessoais por grupos que buscam mais do que lucro econômico, entrando na esfera do controle social e da exploração de predições sobre indivíduos. Para ela, as grandes plataformas utilizam os dados pessoais recebidos para monetização em larga e arbitrária escala.

Essas práticas, em um contexto neoliberal que desconsidera os direitos sociais e o bem-estar dos cidadãos, levam à obtenção desmedida de dados pessoais em escala coletiva, ignorando características íntimas, remodelando comportamentos conforme interesses próprios e comprometendo direitos que deveriam ser protegidos.

4 A PROTEÇÃO DE DADOS PESSOAIS: ORIGEM E DESENVOLVIMENTO

Certamente, invenções tão revolucionárias quanto as redes sociais não poderiam ficar sem uma resposta jurídica apropriada. A regulação deste tema sempre foi uma preocupação e uma questão sensível no âmbito legislativo. Atualmente, com o surgimento de conflitos cada vez mais complexos, como os anteriormente discutidos, a Internet, que começou sem regulamentação legal e continuou assim por um tempo, agora começa a ser influenciada por normas estatais. Michael Kloepfle explica (SARLET, 2017):

> Ela foi amplamente moldada com base nos princípios técnicos das redes de telecomunicações, que inicialmente eram estatais e depois privatizadas, assim como aquelas que sempre foram privadas. A organização e o formato da rede são essencialmente questões privadas, embora haja influências estatais que podem ser intensificadas devido à tendência de censura estatal na Internet.

Até agora, o princípio internacional de autorregulação social (ICANN) tem predominado, mas apresenta deficiências democráticas. Com os avanços em técnicas de filtragem e barreiras de acesso, é esperado um fortalecimento da influência estatal.

O princípio internacional de autorregulação social (ICANN) refere-se às regras estabelecidas pelos próprios organismos da Internet, que se regulam sem interferência externa. No entanto, esse liberalismo virtual possui deficiências democráticas, como evidenciado no capítulo anterior.

Assim, Estados Democráticos de Direito ao redor do mundo estabeleceram diretrizes para cumprir seu dever de proteger os direitos fundamentais, entendendo que os dados pessoais representam uma projeção da personalidade do indivíduo e precisam de proteção constitucional. O principal desafio é definir um nível adequado de proteção, levando em consideração que as ações de terceiros (como o direito à livre concorrência e à iniciativa) também devem ser protegidas com base nos direitos fundamentais que lhes são inerentes. O Estado, portanto, enfrenta expectativas conflitantes de diferentes titulares de direitos fundamentais. Como resultado, a influência estatal se concretizou com a criação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).

Para abordar a norma brasileira de proteção de dados, é essencial revisitar a definição e importância dos bens jurídicos protegidos, reconhecidos e salvaguardados desde a Constituição Federal Brasileira de 1988.

4.1 Constituição Federal de 1988: Direitos Fundamentais e a Dignidade da Pessoa Humana

A Constituição Federal de 1988 impacta diretamente o tratamento de dados pessoais, especialmente no que diz respeito aos direitos fundamentais à privacidade, liberdade, igualdade, autodeterminação informativa, e aos princípios que garantem uma ordem econômica justa e equilibrada e a dignidade da pessoa humana, como destaca Laura Schertel (2008, p. 119):

> A Constituição é o ordenamento jurídico fundamental do Estado e da sociedade, que constitui e limita os processos de poder. A partir de suas características procedimentais, ela configura um sistema de direitos fundamentais que institucionaliza os pressupostos de comunicação necessários à autodeterminação democrática dos cidadãos. Segundo uma visão dinâmica da Constituição, ela é um projeto inacabado, sempre sujeito a alterações interpretativas, refletindo um processo de aprendizado falível.

Para uma compreensão completa da Lei Geral de Proteção de Dados, o presente trabalho dedicará os próximos subtítulos a uma breve explicação desses direitos e princípios.

4.1.1 Privacidade

Os debates doutrinários sobre o direito à privacidade surgiram em resposta à criação de novas técnicas e ferramentas tecnológicas que possibilitaram o acesso e divulgação de informações sobre a vida privada do indivíduo de maneiras antes inimagináveis, reformulando o significado desse direito fundamental. Laura Schertel afirma (2008, p. 14):

> A origem do direito à privacidade ocorreu em um momento diferente de outros direitos liberais, uma vez que não foi reconhecido nas Constituições nem nos Códigos Civis do século XIX. Sua origem se deu inicialmente no contexto doutrinário, sendo reconhecido no âmbito legislativo apenas no século XX.

Essa mudança ocorreu com a substituição do antigo conceito de proteção da vida privada como um aspecto da propriedade pelo novo conceito de proteção da inviolabilidade da personalidade. Warren e Brandeis afirmam: "O princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na verdade o princípio da inviolabilidade da personalidade" (WARREN; BRANDEIS, 2011).

Dessa forma, o caráter individualista da proteção à privacidade em seus primórdios estava associado ao direito de ser deixado em paz (right to be let alone) (WARREN; BRANDEIS, 2011). Isso faz com que o direito à privacidade seja visto como um direito negativo, anteriormente acompanhado pela necessidade de abstenção estatal na esfera privada para sua concretização.

No século XX, a privacidade foi reinstituída com o Estado, impulsionado pela revolução tecnológica e pela rápida coleta e disseminação de informações, passando a ser considerada uma garantia de controle do indivíduo sobre suas próprias informações e um pressuposto para qualquer regime democrático. A autora descreve esse período da seguinte maneira:

> Após a II Guerra Mundial, a proteção à privacidade ganhou reconhecimento internacional. A Declaração Universal dos Direitos Humanos, de 1948, prevê, em seu art. XII, além do direito à privacidade, também o direito à honra e ao sigilo de correspondência, nos seguintes termos: '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 Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, o Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos, no Pacto de São José da Costa Rica,

> também preveram a proteção da vida privada em termos semelhantes (SCHERTEL, 2017, p. 215).

No contexto constitucional brasileiro, o direito à privacidade é considerado uma forma de direito à personalidade do indivíduo, possuindo tanto um caráter negativo (direito de defesa) quanto um caráter positivo (direito à prestação). A autora explica:

> Negativo, por delimitar uma esfera de proteção que não pode ser invadida pelo poder estatal ou privado, exigindo a abstenção do Estado nesse âmbito. Positivo, por exigir também uma ação do Estado para garantir essa proteção. Assim, por exemplo, exige-se a intervenção estatal para obrigar os órgãos que realizam o tratamento dos dados pessoais a prestar informações (SCHERTEL, 2017, p. 199).

Na prática, o caráter negativo implica que nenhuma lei pode ser promulgada para anular ou eliminar esse direito fundamental, sob pena de ser considerada inconstitucional e declarada nula. Quanto ao caráter positivo, o direito à proteção de dados pessoais, reconhecido indiretamente pela Constituição, impõe ao Estado o dever de agir para proteger a personalidade do indivíduo, incluindo a edição de leis específicas que regulamentem o assunto.

A Constituição Federal contém várias disposições relacionadas à proteção da privacidade e dos dados pessoais, como a inviolabilidade da vida privada e da intimidade (art. 5º, X), a proibição da interceptação de comunicações telefônicas, telegráficas ou de dados (art. 5º, XII), a proibição da invasão de domicílio (art. 5º, XI) e de correspondência (art. 5º, XII), e a materialização do direito à privacidade: o habeas data (art. 5º, LXXII), um direito fundamental processual para o conhecimento e correção de dados pessoais. No entanto, este último se tornou ineficaz na proteção de dados pessoais devido à dificuldade do impetrante em obter informações precisas sobre quem detém os dados pessoais, suas finalidades, quais dados são utilizados, de que forma e para quais propósitos.

Hoje, a privacidade enfrenta ofensas que vão além da invasão e captura indevida de dados pessoais, exigindo que o paradigma da privacidade lide com antigos ilícitos e métodos atuais lícitos.

Nesse contexto, a teoria dos mosaicos, desenvolvida por Conessa (1984), oferece uma abordagem útil para entender a privacidade em relação aos dados pessoais. A teoria sugere que informações aparentemente inofensivas, quando combinadas, podem se tornar perigosas ao criar um perfil íntimo e detalhado de um indivíduo, mesmo que não seja completamente verdadeiro.

Portanto, o potencial ofensivo de alguns dados pessoais só se revela quando eles são relacionados com outras informações. A teoria ajuda a esclarecer as diversas facetas da

privacidade e destaca a importância de considerar o aspecto macro na coleta de informações pessoais.

4.1.2 Liberdade e Igualdade

A existência do Estado está profundamente ligada à regulação dos comportamentos e ações dos indivíduos, o que justifica a classificação de atos como lícitos ou ilícitos. Contudo, a liberdade de decisão é assegurada por diversas formas criadas pelo sistema jurídico para protegê-la.

Em uma análise breve, a perspectiva histórico-evolutiva de Mayer-Schonberger (apud. SCHERTEL, 2017, p. 36) identifica três gerações de normas de proteção de dados pessoais, sendo a segunda geração a mais relevante para nós. Ela aborda o paradigma da liberdade:

> A segunda geração de normas de proteção de dados pessoais levanta uma questão interessante sobre a eficácia do consentimento do cidadão e o real exercício de sua liberdade de escolha, em um cenário onde a não disponibilização dos dados pode resultar em exclusão social. Por um lado, no contexto do Estado Social, é bastante desafiador garantir a liberdade informacional sem comprometer as funções da burocracia complexa que necessita dos dados dos cidadãos para planejamento. Por outro lado, também na relação entre particulares, é difícil verificar o exercício do direito à privacidade informacional, pois tal exercício pode impedir o acesso do indivíduo a certos serviços no mercado de consumo, que os fornecedores estão dispostos a oferecer somente em troca do fornecimento de informações pessoais.

Nesse contexto, Mayer-Schönberger critica o verdadeiro dilema social enfrentado pelos indivíduos para exercer seu direito à privacidade e à proteção de dados:

> A proteção de dados pessoais como liberdade individual pode realmente proteger a liberdade do indivíduo. Ela pode oferecer ao indivíduo a possibilidade de não fornecer informações solicitadas sobre si mesmo. Mas qual é o custo disso? É aceitável que a proteção de dados pessoais seja exercida apenas por reclusos? Teremos atingido o estágio ideal de proteção de dados se garantirmos direitos à privacidade que, ao serem exercidos, levarão à exclusão do indivíduo da sociedade?

A violação da autodeterminação e liberdade do indivíduo ocorre quando suas informações pessoais, que também formam sua personalidade, são divulgadas indevidamente ou usadas sem permissão, resultando na perda de controle sobre seus próprios dados pessoais.

A LGPD é uma medida legislativa que proporciona ao cidadão os mecanismos necessários para controlar suas próprias informações. Ela também representa a concretização desse direito fundamental, permitindo ao indivíduo definir o alcance da própria privacidade e evitando a imposição de uma única visão de mundo (SCHERTEL, 2017).

A autora também esclarece que a liberdade no contexto dos dados pessoais não é um princípio absoluto, afirmando que "ela (a liberdade) está constantemente articulada com o

princípio da igualdade e ambos compõem o preceito da dignidade humana". Assim, o pleno exercício da liberdade de controle dos dados pessoais baseia-se no consentimento consciente e informado do titular.

A LGPD (Lei Geral de Proteção de Dados Pessoais) visa dotar o indivíduo do controle livre sobre a divulgação e o uso de seus dados pessoais pelos agentes de tratamento, preservando, assim, sua capacidade de autodeterminação e o livre desenvolvimento de sua personalidade.

5. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018)

A Lei nº 13.709/2018 (LGPD) traz como principal receio dos afetados a garantia dos direitos dos titulares, alguns dos quais inovadores para o ordenamento jurídico e para os setores públicos e privados, como o direito à portabilidade dos dados pessoais e outros direitos descritos a seguir:

> (i) confirmação da existência de tratamento;
>
> (ii) acesso aos dados;
>
> (iii) correção de dados incompletos, inexatos ou desatualizados;
>
> (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desacordo com a Lei;
>
> (v) portabilidade dos dados para outro fornecedor de serviço ou produto;
>
> (vi) eliminação dos dados pessoais tratados com o consentimento do titular;
>
> (vii) informação sobre a possibilidade de não fornecer consentimento e as consequências da recusa;
>
> (viii) revogação do consentimento.

Denota-se, portanto, que o objetivo da lei não é proteger os dados em si, mas sim proteger a pessoa que é titular dessas informações. Assim, observa-se uma certa vulnerabilidade do usuário que fornece seus dados em troca de bens ou serviços, semelhante ao previsto no Código de Defesa do Consumidor. A diferença crucial é que a proteção prevista na LGPD abrange todos os tipos de dados pessoais, tanto físicos quanto virtuais, reconhecendo as limitações técnicas, econômicas e jurídicas que um indivíduo enfrenta ao lidar com um sistema complexo de coleta e processamento de dados, muitas vezes encontrando dificuldades intransponíveis para acessar seus dados.

Em relação à aplicabilidade e territorialidade, o art. 3º da LGPD esclarece que a lei se aplica a todos que realizam qualquer operação de tratamento de dados pessoais, sejam entidades públicas ou privadas, pessoas físicas ou jurídicas, independentemente do meio utilizado ou do país de origem ou localização dos dados, desde que (BRASIL, 2018):

> I - a operação de tratamento ocorra no território nacional;
>
> II - a atividade de tratamento tenha como objetivo a oferta ou o fornecimento de bens ou serviços, ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Dessa forma, a LGPD também se aplica a dados tratados fora do Brasil, desde que a coleta tenha ocorrido no território nacional, ou se houver oferta de produto ou serviço para indivíduos no Brasil ou que estejam no Brasil, conforme explica Patrícia Pinheiro (2020). Ela exemplifica que "dados pessoais tratados por uma empresa de serviço de cloud computing que armazena os dados fora do país terão que cumprir as exigências da LGPD."

Por outro lado, a lei não se aplica quando o tratamento dos dados é realizado por pessoa física para fins exclusivamente pessoais e não econômicos, para fins exclusivamente jornalísticos e artísticos, ou para tratamentos realizados com a finalidade de segurança pública e defesa nacional, conforme estabelecido no art. 4º, I, II, III e IV.

A autora sugere que "o tema da proteção dos dados pessoais teria sido mais bem abordado em um tratado internacional, considerando que a natureza atual dos fluxos de dados nos negócios é transfronteiriça" (PINHEIRO, 2020).

Essa crítica é pertinente devido à crescente globalização e ao intenso fluxo internacional de dados, o que facilitaria a comunicação em casos de violação dos direitos protegidos. Além disso, na visão da autora, a União Europeia conseguiu consolidar as diretrizes de 28 Estados-Membros em um único regulamento geral, o GDPR, criando um precedente para que outras regiões do mundo adotem uma abordagem similar.

No entanto, a LGPD apresenta semelhanças com o GDPR, visando minimizar as diferenças técnicas, jurídicas e econômicas entre usuários e empresas, sejam elas públicas ou privadas, internas ou externas ao território brasileiro. Nesse sentido, Patrícia (2020) observa:

> A versão nacional é mais compacta e, em alguns aspectos, permite uma interpretação mais ampla, o que pode gerar certa insegurança jurídica ao permitir margem para subjetividade onde deveria ter sido mais assertiva. Um exemplo disso é a definição de prazos: enquanto o GDPR estabelece prazos exatos, como 72 horas, a LGPD prevê 'prazo razoável (PINHEIRO, 2020, p. 231).

Essa flexibilidade pode ser explicada pelos desafios que a lei representa para todos os setores regulados por ela, como será detalhado ao longo do capítulo.

O artigo 6º define os princípios que regem a norma e que são responsáveis pela harmonização da legislação brasileira com a internacional. Embora não tenham força

normativa, esses princípios guiarão e limitarão o tratamento de dados pessoais nos setores públicos e privados para garantir o exercício da autodeterminação informativa:

> Art. 6º As atividades de tratamento de dados pessoais devem observar a boa-fé e os seguintes princípios:
>
> I - Finalidade: tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior incompatível com essas finalidades;
>
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, conforme o contexto do tratamento;
>
> III - Necessidade: limitação do tratamento ao mínimo necessário para a realização das finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento;
>
> IV - Livre acesso: garantia ao titular de consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - Qualidade dos dados: garantia ao titular de exatidão, clareza, relevância e atualização dos dados, conforme a necessidade e para o cumprimento da finalidade do tratamento;
>
> VI - Transparência: garantia ao titular de informações claras, precisas e facilmente acessíveis sobre o tratamento e os respectivos agentes, respeitados os segredos comercial e industrial;
>
> VII - Segurança: uso de medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em decorrência do tratamento de dados pessoais;
>
> IX - Não discriminação: impossibilidade de tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e cumprimento das normas de proteção de dados pessoais, bem como da eficácia dessas medidas.

Embora ainda não esteja em vigor, espera-se que a LGPD seja capaz de enfrentar o desafio da tecnologia e da modernidade, tratando a proteção dos dados com o devido respeito e seriedade, reconhecendo a titularidade dos dados como propriedade dos indivíduos, e não das organizações, como ocorre em países sem legislação específica, orientando o tratamento de dados durante sua coleta, armazenamento, processamento, uso e exclusão.

No que se refere às penalidades, previstas no art. 52, devem observar critérios como a proporcionalidade. As sanções incluem: advertência, publicização da infração, suspensão parcial, sanções administrativas e até a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

Entre as penalidades, destaca-se o inciso II, que prevê "multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no

Brasil no último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração."

Inicialmente, é importante que sejam preferidas as sanções administrativas em vez de multas severas, pois a lei visa promover uma mudança cultural nas organizações para que os princípios mencionados se tornem pilares internos. Nesse sentido, o art. 2º esclarece que a lei foi criada não apenas para proteger os titulares dos dados, mas também para fomentar o desenvolvimento econômico dos agentes de tratamento de dados.

Entre os aspectos que podem ser considerados na redução de uma sanção pela Autoridade fiscalizadora estão a gravidade e a natureza das infrações, a categoria dos direitos pessoais afetados, a boa-fé, a reincidência, entre outros previstos no art. 52, §2º e incisos.

Portanto, um sistema de gestão de dados pessoais bem implementado pode ser relevante na redução das penalidades em caso de infrações. É necessário que os setores afetados pela lei reestruturem sua governança corporativa para focar nos princípios previstos pela LGPD, garantindo a sustentabilidade do negócio.

6 CONCLUSÃO

O mercado contemporâneo tem se transformado, com os dados pessoais emergindo como a nova moeda de troca. Nesse cenário, o direito à privacidade enfrenta riscos e desafios inéditos, impulsionados pelo uso massivo de algoritmos. Esses algoritmos, desenvolvidos a partir do *big data* e big analytics, criaram uma nova economia e uma nova forma de tomada de decisões baseadas em análises preditivas e marketing direcionado. No contexto do capitalismo de vigilância e da economia da atenção, as entidades que controlam vastos bancos de dados se tornam não apenas concorrentes, mas o próprio mercado, dominando informações sobre milhares de usuários.

A predição comportamental e o marketing direcionado emergem como métodos que vão além da simples oferta de bens e serviços. Eles visam definir padrões de consumo, controlar comportamentos, influenciar consciências, restringir a liberdade de escolha dos indivíduos e estabelecer padrões discriminatórios, ameaçando e violando direitos fundamentais como a privacidade, a igualdade e a liberdade, tanto antes quanto após a coleta de informações.

Além disso, há uma ausência de ética e justiça no tratamento de dados como meras estatísticas, e a tecnologia tem sido usada contra a individualidade dos usuários, com máquinas

capazes de conhecer o homem melhor do que ele mesmo. O caso do metrô de São Paulo ilustra a coleta indiscriminada de dados e evidencia a necessidade urgente de regulação e fiscalização.

Apesar da proteção constitucional e da existência de legislações dispersas, práticas violadoras continuam a crescer. A LGPD surge como uma resposta a essa realidade, buscando trazer transparência às práticas das instituições públicas e privadas em relação aos titulares dos dados. A legislação demonstra que o Direito não deve servir apenas à sociedade, mas deve também se adaptar às suas constantes transformações. As fronteiras legais são expandidas a cada momento, e a lei de proteção de dados introduz novas práticas, muitas das quais agora são ilegais. A adequação à LGPD exige rapidez, visto que as penalidades podem ser severas.

É importante reconhecer que a LGPD e a ANPD, por si só, não resolverão todos os conflitos relacionados à proteção de dados pessoais. A solução para esses conflitos dependerá da cooperação entre a autoridade reguladora e outros órgãos, bem como do diálogo entre diferentes fontes legais. O Estado também enfrentará desafios para se adequar à LGPD, o que exigirá maior segurança e rigor na coleta e proteção de informações pessoais. Além disso, o tema carece de maior inclusão e debate nas instituições de ensino de Direito, para preparar melhor os futuros profissionais para lidar com esses desafios.

REFERÊNCIAS

BEZERRA, André Luís Martins. **A Lei 13.709/18 e os novos desafios da proteção de dados pessoais e identidade**. 2019.

BLUM, Renato Opice; ELIAS, Paulo Sá. O consumidor do século XXI. **Revista do Advogado.** Ano XXXI. n.114.São Paulo: Associação dos Advogados de São Paulo, dez. 2011.

BRAGHIT, Ronaldo. **Business Intelligence:** Implementar do jeito certo e a custo zero. São Paulo: Casa Código, 2017.

BRASIL. **Decreto-Lei nº 13.709, de 14 de agosto de 2018**. Regulamenta o tratamento de dados pessoais no Brasil, tanto pelo poder público quanto pela iniciativa privada. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 abr. 2024.

BRASIL. Ministério da Economia. **Economia com implantação de serviços digitais pode gerar economia de 97% aos cofres públicos.** 2017. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/planejamento/economia-com-implantacao-de-servicos-digitais-pode-gerar-economia-de-97-aos-cofres-publicos. Acesso em: 10 jul. 2024.

BRASIL. **Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD Contínua, Ano 2017.** Disponível em:

https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 25 maio 2024.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1168547/RJ.** (Quarta Turma). Relator: Ministro Luis Felipe Salomão. Brasília, de 11 de maio de 2010. Disponível em: https://scon.stj.jus.br/SCON/. Acesso em: 10 jul. 2024.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1348532/SP.** (Quarta Turma). Relator: Ministro Luis Felipe Salomão. Brasília, de 10 de outubro de 2017. Disponível em: https://scon.stj.jus.br/SCON/. Acesso em: 10 jul. 2024.

BRASIL. Supremo Tribunal Federal. **Plenário retoma nesta quinta-feira (28) julgamento de ações sobre bloqueio de aplicativos de mensagens.** Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=444283. Acessado 5 jun. 2024.

CASTELLS, Manuel. **A sociedade em rede.** São Paulo: Paz e Terra, 2002.

COMISSÃO EUROPEIA. **Assuma o controle de seus dados: um guia do cidadão para a proteção de dados na UE.** Luxemburgo: Serviço das Publicações da União Europeia. 2018.

CONESA, F. **Derecho à la intimidad, informática y Estado de Derecho**. Valencia: Universidad, 1984.

DANTAS, Haendel. **Um mosaico de pessoas:** Barack Obama. 2008. Disponível em: https://comunicadores.info/2008/03/26/barack-obama-um-mosaico-de-pessoas/. Acesso em: 30 maio 2024.

DOMINGOS, Pedro. **O Algoritmo Mestre:** Como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. São Paulo: Novatec Editora Edição, 2019.

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

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet.** São Paulo: Lumen Juris, 2016.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Petrópolis: Vozes, 2014.

FRAZÃO, Ana. **Plataformas digitais e os desafios para a regulação jurídica**. v.1. Belo Horizonte: Editora D'Plácido, 2018.

GNIPPER, Patrícia. **Seu smartphone seria poderoso o suficiente para te levar até a Lua?** 2019. Disponível em: https://canaltech.com.br/espaco/seu-smartphone-seria-poderoso-o-suficiente-para-te-levar-ate-a-lua-144515/. Acesso em: 20 abr. 2024.

GUIMARÃES, Patrícia Borba Vilar. Monetização De Dados Pessoais Na Internet: Competência Regulatória A Partir Do Decreto Nº 8.771/2016. v. 4, nº1. Artigo. **Revista de Estudos Constitucionais UFRN.** 2018.

HARARI, Yuval Noa. **Homo Deus:** uma breve história do amanhã. Disponível em: http://lelivros.love/book/baixar-livro-homo-deus-yuval-noah-harari-em-pdf-epub-e-mobi-ou-ler-online/. Acesso em: 20 maio 2024.

HELTON, Simões Gomes; LAPORTA, Taís. **Entenda o que é blockchain, a tecnologia por trás do bitcoin**. 2018. Disponível em: https://g1.globo.com/economia/noticia/entenda-o-que-e-blockchain-a-tecnologia-por-tras-do-bitcoin.ghtml. Acesso em: 20 abr. 2024.

HOWARD, Dresner; TONI, Ronaldo. **Business Intelligence**: Implementar do jeito certo e a custo zero. São Paulo: Casa Código, 2017.

IBGE. Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD Contínua" Ano 2017. **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: 25 maio 2024.

JOTA. **O valor positivo da LGPD.** 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-valor-positivo-da-lgpd-25112019. Acesso em: 10 jul. 2024.

JOTA. **Sorria? Seus dados estão sendo compartilhados**. 2018. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/sorria-dados-compartilhados-29032018. Acesso em: 20 abr. 2024.

LÈVY, Pierre. **Cybercultura.** Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIMBERGER, Têmis. **Proteção de dados Pessoais e comércio eletrônico:** os desafios do século XXI, São Paulo: Vozes, 2008.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** Linhas gerais de um novo direito fundamental. São Paulo: Saraiva Educação, 2017.

MENDES, Laura Schertel. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. São Paulo: Saraiva, 2008.

MIGUEL, Fernando Gomes. **Os desafios do Brasil na nova era da proteção de dados pessoais e da privacidade**. 2019. Disponível em: https://www.migalhas.com.br/depeso/298736/os-desafios-do-brasil-na-nova-era-da-protecao-de-dados-pessoais-e-da-privacidade. Acesso em: 10 jul. 2024.

OLIVEIRA, Eduardo Chagas; CARNEIRO, Ivana Libertadoira Borges. Sobre o caráter persuasivo da estrutura panóptica: Bentham, Foucalt e as novas tecnologias. **Revista Ideação**. n. 33. 2016.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018-LGPD. São Paulo: Saraiva Educação, 2020.

RENASCENÇA. Dados pessoais e dados pessoais sensíveis, 2018. Disponível em: https://rr.sapo.pt/privacidade-online/cap1.aspx. Acesso em: 20 abr. 2024.

RIBEIRO, Jose Antonio. **Big Data para Executivos e Profissionais de Mercado**. Rio de Janeiro: Método, 2018.

RUARO, Regina Linden, RODRIGUEZ, Daniel Piñeiro, FINGER, Brunize. O Direito à Proteção de Dados Pessoais e a privacidade. **Revista da Faculdade de Direito da Universidade Federal do Paraná**. Curitiba. n. 53. 2011.

SARLET, INGO WOLFGANG. **Série Direito Inovação e Tecnologia-Direito, Inovação e Tecnologia:** volume 1. São Paulo: Saraiva Educação, 2017.

SCHAAR, Peter. Das Ende der Privatsphäre: der Weg in die Uberwachungsgesellschaft. Munchen, C. Bertelsmann apud RUARO, Regina Linden. O Direito à Proteção de Dados Pessoais e a Privacidade. 2011. **Revista da Faculdade de Direito UFPR.** Disponível em: https://revistas.ufpr.br/direito/article/view/30768. Acesso em: 20 maio 2024.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** Rio de Janeiro: EDIPRO, 2019.

SOUZA, Maria Luciana Pereira de. **Proteção de dados pessoais na internet:** a mais recente instrumentalização do princípio da dignidade humana na sociedade da informação. Rio de Janeiro: Vozes, 2018.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet.** v. 22. Fortaleza: Pensar, 2017.

VEIGA, Alfredo Neto. **Foucault & a Educação.** São Paulo: Autêntica Editora, 2019.

VELOSO, Thássius. **WhatsApp em números: 120 milhões de brasileiros e 100% de criptografia.** 2017. Disponível em: https://www.techtudo.com.br/noticias/2017/05/whatsapp-em-numeros-120-milhoes-de-brasileiros-e-100-de-criptografia.ghtml. Acesso em: 05 de junho de 2024

VIGNOLI, Richele; VECHIATO, Fernando. **Dados sensíveis no contexto dos dados de pesquisa: um olhar na perspectiva da Ciência da Informação.** 2019. Disponível em: 10.31229/osf.io/dkn8z. Acesso em: 20 abr. 2024.

WHATSAPP. **FAQ do WhatsApp - Criptografia de ponta a ponta.** https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption. Acessado 5 jun. 2024

WIFI METRO SP. **Termos e Condições. Termos de Privacidade**. 2017. Disponível em: http://freewifimetrosp.com.br/. Acesso em: 20 abr. 2024.

WU, Tim. **The atention merchants: the epic scramble to get inside our heads**. New York: Knopf, 2016.

ZUBOFF, Shoshana. **Um capitalismo de vigilância:** Le Monde Diplomatique. 2019. Disponível em: https://diplomatique.org.br/um-capitalismo-de-vigilancia/. Acesso em: 20 abr. 2024.