UNIVERSIDADE DE PASSO FUNDO
FACULDADE DE DIREITO

Sérgio Miguel De Moraes Barros Corrêa

# ANÁLISE DA REGULAMENTAÇÃO E RESPONSABILIZAÇÃO DAS *BIG TECHS*

Passo Fundo, RS
2024

Sérgio Miguel de Moraes Barros Corrêa

# ANÁLISE DA REGULAMENTAÇÃO E RESPONSABILIZAÇÃO DAS *BIG TECHS*

Monografia apresentada ao Curso de Direito da Universidade de Passo Fundo (UPF), como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientadora: Profa. Dra. Micheli Piucco

_____
Micheli Piucco, Dra. (UPF)
(Presidente/Orientadora)

_____
XXXXXXX (UPF)
(Avaliadora)

_____
XXXXXXXX. (UPF)
(Avaliador)

**RESUMO**

A presente monografia analisa o funcionamento das Big Techs, destacando como os dados pessoais se tornaram a principal matéria-prima e fonte de monetização dessas empresas. O estudo aborda a evolução da regulamentação do tratamento de dados pessoais no Brasil e no exterior, com destaque para a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (RGPD). A pesquisa parte do problema da assimetria de poder entre grandes empresas de tecnologia e usuários, que resulta em violações frequentes da privacidade e direitos fundamentais. Além disso, considerando a prematuridade das normas, busca-se examinar como vem ocorrendo a responsabilização dessas empresas nos casos de violação à proteção de dados no ambiente digital e refletir sobre os mecanismos legislativos que possibilitam atenuar o desequilíbrio entre as empresas e os usuários.

**Palavras-chave**: *Big Techs;* dados pessoais; LGPD; responsabilidade civil; RGPD.

**ABSTRACT**

This monograph analyzes the operations of Big Tech companies, highlighting how personal data has become their primary raw material and source of monetization. The study examines the evolution of data protection regulations in Brazil and abroad, focusing on the General Data Protection Law (LGPD) and the General Data Protection Regulation (GDPR). It addresses the problem of power asymmetry between major technology companies and users, which leads to frequent violations of privacy and fundamental rights. Furthermore, considering the nascent stage of these regulations, the research explores how accountability is being enforced in cases of data protection breaches in the digital environment, and reflects on legislative mechanisms that could mitigate the imbalance between companies and users.

**Keywords**: *Big Techs*; civil liability; GDPR; LGPD; personal data.

## AGRADECIMENTOS

Em primeiro lugar, agradeço aos desafios superados na jornada, porquanto esses nos retiram do estado de inércia e promovem o movimento necessário para evolução. Segundamente, à família, que é base e estrutura principal do indivíduo, sem o qual não seria possível ultrapassar as adversidades da jornada acadêmica. Por fim, aos professores, amigos e colegas, que participaram, de algum modo, dessa bela empreitada.

*Sancte Michael Archangele, defende nos in praelio, contra nequitiam et insidias diaboli esto praesidium. Imperet illi Deus, supplices deprecamur: tuque, Princeps militiae caelestis, Satanam aliosque spiritus malignos, qui ad perditionem animarum pervagantur in mundo, divina virtute in infernum detrude.* (Papa Leão XII,1884)

**SUMÁRIO**

# INTRODUÇÃO

Nas últimas décadas, o avanço tecnológico consolidou um cenário em que os dados pessoais se tornaram o principal recurso explorado pelas grandes empresas de tecnologia, conhecidas como *big techs*. O uso intensivo de dados para moldar serviços, aprimorar algoritmos e otimizar produtos não apenas revolucionou o mercado digital, mas também trouxe à tona questões fundamentais relacionadas à privacidade, à autonomia individual e aos direitos da personalidade. Nesse contexto, os dados passaram a ser vistos não apenas como um bem econômico, mas como um elemento essencial da dignidade humana.

A Lei Geral de Proteção de Dados (LGPD), inspirada no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, surge como resposta a essas novas demandas sociais e econômicas. Mais do que uma ferramenta de conformidade regulatória, a LGPD representa um marco no direito brasileiro, definindo princípios e diretrizes que assegurem transparência, segurança e responsabilidade no tratamento de dados. A legislação objetiva equilibrar os interesses comerciais das empresas e os direitos fundamentais dos indivíduos, promovendo um ambiente digital mais ético e seguro.

Este estudo também discute como o sistema jurídico brasileiro, influenciado por legislações internacionais, busca alinhar suas práticas às referências globais. Destacando, em particular, o  efeito Bruxelas do RGPD, que tem sido fator crucial para uniformizar políticas em diversas jurisdições, incluindo Brasil e os Estados Unidos, com o California Consumer Privacy Act (CCPA). A comparação dessas normativas permite uma análise sobre a aplicabilidade e os desafios enfrentados pelo Brasil na implementação de um sistema de proteção de dados eficiente.

Por fim, este trabalho reafirma a importância de responsabilizar as *Big Techs* pela violação à proteção de dados, considerando o desequilíbrio de poder entre essas os atores envolvidos, desse modo, para entender o contexto tecnológico que permitiu a ascensão das *Big Techs*, é necessário revisitar a história da internet e como suas estruturas evoluíram.

## 1.1. CONTEXTUALIZAÇÃO DA ORIGEM DA INTERNET

As grandes empresas de tecnologia se valem da conectividade de seus serviços para gerar monetização por meio da obtenção de dados. Entretanto, o funcionamento vital das estruturas digitais de hoje em dia são apenas adaptações da tecnologia e meios de comunicação antecessores, como o rádio, o telefone e a telegrafia sem fios, uma vez que todos compartilham características em comum com os atuais meios. A ideia de criar uma rede conectada para transmissão facilitada de informações é perceptível na finalidade do rádio e telefone, bem como a percepção que o tamanho da estrutura interligada de agentes às suas redes se traduz em valor ou atratividade de rede (Rosa, 2012, p. 90).

De modo que torna-se essencial uma breve introdução do meio digital utilizado pelas *big techs* para o desenvolvimento de seus negócios e, também, investigando o modelo de negócio e a fórmula da rentabilidade destas empresas.

## 1.2. O surgimento da *internet*

As grandes empresas, em especial, as objeto de estudo do presente trabalho, sempre tiveram necessidade de mecanismos capazes de propagar e difundir informações, com intuito de maximizar suas ofertas e o consumo de seus produtos. Assim, cabe realizar breve estudo do meio de comunicação que foi capaz de intensificar a globalização em larga escala, a *Internet*.

A *internet* teve como origem ideais perpassados pelos meios de comunicação antecessores, quais são a formação de uma rede conectada entre si, que permitia o fluxo de troca de informação, diferenciando-se no aspecto privado da rede, uma vez que a *Internet* "[...] resultou de um trabalho conjunto de académicos financiados por governos e guiados por princípios teóricos[...]*"* (Rosa, 2012, p. 106), ao contrário dos seus antecessores, que surgiram e foram mantidas pela propriedade privada.

Em meados dos anos de 1960, após a Segunda Guerra *Mundial* e início da chamada "Guerra Fria", mais especificamente após o lançamento do foguete *Sputnik*, o presidente americano, Dwight Eisenhower, anunciou a criação da *Advanced Research Projects Agency* (ARPA – Agência de Pesquisa e Projetos Avançados), que integrava o Departamento Nacional de Defesa norte-americano e teve como líder, o cientista Joseph Carl Robnett Licklider (Filho; Rocha, 2016).

Com a necessidade que a troca de informações entre as bases de pesquisa fossem mais rápidas e facilitadas, a ARPA desenvolveu um meio de comunicação entre as bases de pesquisas, de modo que a velocidade de troca de informações entre as bases fossem rápidas e, em caso de comprometimento de uma das bases, não haveria perda das informações desenvolvidas no local. Motivo pelo qual a "[...] montagem da ARPAnet foi justificada como uma maneira de permitir aos vários centros de computadores e grupos de pesquisa, que trabalhavam para a agência, compartilhar online tempo de computação [...]" (Castells, 2003, p. 14).

A rede desenvolvida pela agência do governo ficou conhecida como ARPANET, que, basicamente, consistia em uma rede de computadores interligados entre si, que recebiam, emitiam e armazenavam informações dos usuários conectados a essa rede. A ideia principal era ter uma *backup* dos dados contidos em cada base, além da comunicação on-line (António Rosa, 2012).

Segundo Glauco Rocha e Veridiano Filho (2016), com o sucesso da utilidade dessa forma de troca de informações, o interesse do governo americano cresceu, ante as diversas possibilidades de uso dessa rede, o que resultou na ajuda de Universidades no desenvolvimento do projeto de melhoria desse modelo de rede e os vários testes com a rede ensejaram o aperfeiçoamento das conexões com outras redes conectadas e independentes, dando luz a novas formas de conexão.

O sociólogo Manuel Castells[1] retrata a tecnologia de transmissão de telecomunicações como revolucionária:

> Para montar uma rede interativa de computadores, o IPTO valeu-se de uma tecnologia revolucionária de transmissão de telecomunicações, a comutação por pacote, desenvolvida independentemente por Paul Baran na Rand Corporation (um centro de pesquisas californiano que frequentemente trabalha para o Pentágono) e por Donald Davies no British National Physical Laboratory. O projeto de Baran de uma rede de comunicação descentralizada, flexível, foi uma proposta que a Rand Corporation fez ao Departamento de Defesa para a construção de um sistema militar de comunicações capaz de sobreviver a um ataque nuclear, embora esse nunca tenha sido o objetivo por trás do desenvolvimento da Arpanet (CASTELLS, 2003, p. 14).

O sistema mencionado por Manuel Castells é o TCP/IP, proposto em 1974 por Robert Kahn e Vinton Cerf, criado para ser um protocolo aberto, uma vez que é indiferente quanto ao conteúdo que transporta e não se limitava às redes locais, mas sim, crescia conforme as

[1]**Manuel Castells**, nascido na Espanha em 1942, lecionou durante 12 anos na Universidade de Paris, ingressando, em 1979, na Universidade da Califórnia em Berkeley, onde é professor de Sociologia e Planejamento Regional.

conexões realizadas por protocolos comuns, sem obedecer a qualquer plano central prévio, à exemplo, as condições especiais de propriedade privada, como a marca do computador utilizado para fazer a conexão na rede (Rosa, 2012, p. 107).

A obra "O passado e o futuro da história da *internet",* escrito em 1997, descreve a evolução da idealização da interconexão de redes:

> A ARPANET original evoluiu para a Internet baseada na ideia de que haveria múltiplas redes independentes de design bastante arbitrário. Começando com a ARPANET como a rede pioneira de comutação de pacotes, ela logo cresceu para incluir redes de satélite de pacotes, redes de rádio de pacotes terrestres e outras redes. A Internet de hoje incorpora uma ideia técnica fundamental subjacente: redes de arquitetura aberta. Nesta abordagem, a escolha de qualquer tecnologia de rede individual não é ditada por uma arquitetura de rede específica, mas pode ser selecionada livremente por um provedor e feita para interoperar com outras redes por meio de uma "arquitetura de interconexão" de meta-nível. Cada rede pode ser projetada para se adequar a um ambiente específico e requisitos do usuário. (Leiner et al., 1997, p. 103) (Tradução livre).[2]

De acordo com Araya e Vidotti (2010, p. 23), em 1983, a ARPANET foi dividida entre a rede pública para uso da comunidade científica e civil e a MILNET, que era a rede militar. Dessa forma, a *Internet* deu passos largos em direção à revolução dos atuais meios de comunicação, considerando que se trata de uma rede de estruturas aberta, que permite ao usuário desenvolver *softwares* para a *internet* (Carvalho, 2006, p. 550).

Assim, ante a carência de conteúdo na rede, em 1989, o inventor Tim Bernes Lee apresentou o WWW - *World Wide We*b (Rede de Abrangência Mundial), que é, nas palavras do próprio inventor (1996), *"*[...]o universo da informação acessível na rede global. Ela é um espaço abstrato povoado, principalmente, por páginas interconectadas de texto, imagens e animações, com ocasionais sons, mundos tridimensionais e vídeos[…]"

Essa ferramenta possibilitou a criação de conteúdo multimídia na *internet*, que são acessíveis mediante uso de navegador de WWW (ou WEB) - atualmente temos o *Microsoft Edge, Google Chrome, Mozilla Firefox, Opera*, entre outros- , logo, na metade dos anos 90, a *internet* surge como "[...]um sistema de comunicação flexível descentralizado. A arquitetura

[2]The original ARPANET grew into the Internet based on the idea that there would be multiple independent networks of rather arbitrary design. Beginning with the ARPANET as the pioneering packet-switching network, it soon grew to include packet satellite networks, ground-based packet radio networks, and other networks. Today's Internet embodies a key underlying technical idea: open-architecture networking. In this approach, the choice of any individual network technology is not dictated by a particular network architecture but can be selected freely by a provider and made to interwork with the other networks through a meta-level "internetworking architecture." Each network can be designed to fit a specific environment and user requirements (Leiner et al., 1997, p. 103).

aberta proporcionava a cooperação dos usuários. Assim, a flexibilidade e a liberdade foram valores importantes para o desenvolvimento da Internet[...]"(Carvalho, 2006, p. 550).

Dessa forma, se valendo das redes do *World Wide Web,* foi possível criar páginas de *internet* com conteúdo interativo para os usuários conectados na rede, dando luz aos modelos iniciais de interação humana por meio do uso da rede de *internet*.

### 1.3. Origem das redes sociais

Conforme exposto no tópico anterior, com o advento da *World Wide Web* foi possível a criação de páginas com multimídia, o que ensejou a criação de páginas da Web interativas, podendo o usuário criar conteúdos para compartilhar com seus amigos ou com qualquer interessado nos assuntos debatidos.

Deve-se salientar que, para não recair em imprecisão terminológica, o termo "rede social" não se refere unicamente às empresas de tecnologias, porque tal palavra, conforme Queila Souza e Carlos Quandt (2008, p. 32), representa "estruturas dinâmicas e complexas formadas por pessoas com valores e/ou objetivos em comum, interligadas de forma horizontal e predominantemente descentralizada". Assim, "rede social" é o conjunto de interações humanas, que formam uma rede, ligada por nós, capaz de promover o fluxo informacional.

Segundo Queila Souza e Carlos Quandt (2008, p. 32), as atuais tecnologias da informação são estruturadas pelo modelo de "rede social informais", porque são baseadas no alto fluxo de comunicação e na inexistência de contratos formais reguladores do resultado de interações.

Popularmente se utiliza da expressão "rede social" para se referir às modernas provedoras de conteúdo na *internet*, mas os primeiros modelos de interação humana intermediado pelas redes de computadores, surgiram antes da criação de Tim Bernes Lee[3], que somente foi proposta em 1989. À exemplo, a *Usernet*, que utiliza seu próprio protocolo de transmissão, a *Net News Transfer Protocol (NNTP),* criada em 1976, tinha como função atuar como um fórum, onde é possível publicar artigos e aos leitores, comentar. Também, anterior a criação da *World Wide Web*, em 1980, a rede acadêmica de Yale, que possibilitou aos

[3]**Timothy John Berners-Lee** é o diretor do *World Wide Web* e um cientista pesquisador principal no Laboratório de Ciência da Computação, Instituto de Tecnologia de Massachusetts, 545 Technology Square, Cambridge (WWW.W3.org) (Tradução-livre).

acadêmicos utilizarem a rede conectada como correio eletrônico, semelhante aos atuais emails. (Kirkpatrick, 2010, p. 90).

Dessa forma, se entende que a conexão por redes sempre teve o objetivo de ser meio facilitador para a sociabilização dos usuários, haja vista que o alcance das informações rompiam as barreiras da distância. Howard Rheingold, um dos primeiros autores do conceito de comunidade virtual, descreve como "um grupo de pessoas que podem ou não se encontrar pessoalmente" (Kirkpatrick, 2010, p. 78).

As provedoras de conteúdo digital facilitaram as interações denominadas como "redes sociais", que são as próprias teias de interações dos indivíduos. No início de 1997, surgiu o *sixdegrees.com,* uma das plataformas precursoras das redes sociais da era moderna, que funcionava por meio de uma cadeia amplificada de relacionamentos de amigos (Kirkpatrick, 2010, p. 78/79).

Kirkpatrick (2010, p 100) aponta que em 2001 a plataforma Ryze foi lançada, tendo por caraterística ser "uma rede de negócios, não de namoro". O site não se firmou, mas inspirou a outros, como o Friendster, que objetivava conectar pessoas de modo social, de maneira semelhante ao *sixdegrees.com*. Seu criador, Jonathan Abrams, viu a oportunidade de explorar o lado pessoal e social das pessoas. Essa estrutura de interações moldou o funcionamento das atuais plataformas de conteúdo digital, Sean Parker[4] diz que "[...]Jonathan decifrou o código. Ele definiu a estrutura básica do que hoje chamamos de rede socia[…]*".* Com o esqueleto do funcionamento de uma "rede social", a partir de 2003, surgiram diversas outras plataformas com funções e destinações específicas, como o LinkedIn e Tribe, que tinham viés voltado às atividades profissionais, e o *MySpace*, que utilizava-se da mesma finalidade do *Friendster*, porém, se diferenciava na medida que permitia os denominados *fakesters*[5] e mesclava outras funcionalidades, como jogos, horóscopo e blogs.

Posteriormente, surgiram as mídias voltadas especificamente para relacionamentos sociais, tais como o *Orkut*, *Facebook*, *Twitter* e *Youtube*, plataformas que revolucionaram, tanto a forma de se socializar e informar, como economicamente, através do crescimento exponencial das empresas que administram referidos produtos. Os poderes de influenciar economicamente e socialmente destes entes privados ganharam proporções globais, despertando sentimentos de

[4]**Sean Parker** é um empreendedor norte americano. Co-fundou o Napster, Plaxo e Causes, e participou do Facebook. (Wikipédia)

[5]**Fakesters** são usuários que deliberadamente criavam perfis usando nomes e identidades falsas, incluindo personagens de desenhos animados e cães (Kirkpatrick, 2011, p. 100).

cautela por muitos países e entidades internacionais. Assim sendo, é de fundamental importância compreender o funcionamento do modelo de negócio dessas entidades globais denominadas por *big techs*.

### 1.4. O que são *Big techs*?

A partir da criação da *Internet* e da *World Wide Web*, que possibilitaram o aperfeiçoamento da comunicação em massa e, principalmente, à distância, foi possível a exploração econômica, por parte de agentes privados, através desses meios. O que resultou na formação de potências globais

As plataformas de conteúdo da internet tomaram tamanha proporção, que as empresas às quais pertencem alcançaram patamar ímpar em relação às outras companhias, haja vista esse grupo de empresas ter uma forte tendência à oligopolização[6] (Giovanna Bortolotto, 2020, p. 11).

O fato da empresa ter uma rede social como produto, não necessariamente torna ela uma *big techs*[7], porque essas, segundo Júlia Figueiredo (2022, p. 26) "[...]são grandes empresas, que possuem relativa vantagem no uso da tecnologia digital. Geralmente, são fornecedores de web serviços para consumidores finais ou são capazes de desenvolver e manter uma infraestrutura, onde outras empresas fornecem serviços e produtos[...]".

Dessa forma, podem ser definidas como empresas de tecnologia da informação e comunicação (TIC), configuradas como grandes conglomerados econômicos que executam e prestam serviços digitais a diversos segmentos da economia de um país, incluindo comunicação social, além de conectar produção a consumidores. Na Europa, as *big techs* recebem nomes como *Very Large Online Platforms* (VLOPs) ou *Search Engines* (VLOSEs), respectivamente, Plataformas Online Muito Grandes e Motores de Busca Online Muito Grandes (Montenegro, 2023, p. 11).

Atualmente, temos 5 *big techs* que controlam o mercado de tratamento de dados, sendo elas: o *Twitter* (X), *Amazon* Inc, *Google* Inc, *Microsoft* e *META* (Nunes, 2023, p. 07).

---

[6]**Oligopolização**: relativo ao processo de fazer oligopólios, ou seja, de concentrar o controle de algo para um grupo de poucas pessoas (Dício.com).

[7]**BigTecs** is a generic name that is used for large technology companies active worldwide, having a relative advantage in using digital technology. BigTech companies are usually providers of web services (search engines (SEO), social networks, e-commerce etc.) for end-users on the internet and/or IT platforms or develop and maintain an infrastructure (storage and processing capabilities data) for which other regular companies provide products or services (Mărăcine; Scarlat; Voican 2020, p. 02**)**.

Em suma, são as empresas que, pela sua dimensão e influência, atuam em regime de oligopólio e todas, por mais que sua atividade-fim não seja apenas o tratamento de dados, atuam por meio dos serviços de tecnologia. (Bortolotto, 2020, p. 17) E, pela tradução literal da palavra, é definido como "Gigantes da tecnologia", não restando outro entendimento, senão o de que são grandes empresas do ramo da tecnologia ou dela desfrutam para maximizar seus ganhos e lucros.

As *bigs techs* são empresas de tecnologia que, geralmente, oferecem três tipos de serviço: serviços principais, serviços financeiros e serviços de tecnologia. As atividades principais das grandes empresas de tecnologia permitem que elas coletem dados em uma ampla rede de usuários. Essas informações são essenciais para personalizar suas atividades principais e desenvolver ainda mais a gama de produtos e serviços oferecidos (Crisanto; Ehrentraud; Fabian, 2022, p. 06).

Esse elemento é o que diferencia as *big techs* em comparação às empresas convencionais. A vantagem proveniente da análise de dados inerentes dos serviços digitais impacta substancialmente na assertividade do serviço a ser oferecido e, quanto mais usuários conectados nos servidores das plataformas, mais informações sobre aquele cliente é gerado, o que possibilita exercer influência no mercado, considerando que as empresas controlam quem recebe determinados dados. Assim, as *big techs* são capazes de penetrar em diferentes mercados conectados (Figueiredo, 2022, p. 27).

Os serviços digitais fornecidos por grandes empresas de plataforma digital se tornaram onipresentes em todo o mundo. As *big techs*, agora atendem a inúmeros clientes que regularmente pedem produtos online, enviam mensagens via aplicativos em telefones celulares ou checam seus e-mails ou contas de redes sociais. Ao expandir seus serviços, as *big techs* cresceram muito, e várias delas agora têm capitalizações de mercado que excedem as das maiores instituições financeiras (Crisanto; Ehrentraud; Fabian, 2022, p. 3).

Assim, se entende que as *big techs* são grandes empresas de tecnologia que atuam globalmente, por meio da rede de *internet*, e possuem uma vasta coleta de informações acerca de seus usuários, a fim de providenciar serviços direcionados e personalizados ao cliente, transformando a informação em monetização, destacando que devido ao extenso número de usuários ao redor do mundo, permite uma ampla análise do comportamento desses em nível global.

## 1.5. Modelo de negócio (*business model*)

As *big techs* atuam em plano de ecossistema, no qual há vários atores e personagens, como usuários e empresas, cada um com seu objetivo específico. Esse ecossistema é baseado na interdependência dos multi-atores que orbitam os serviços das *big techs* e, todos, produzem algum tipo de informação ou geram dados específicos passíveis a de serem analisados e transformados em matéria-prima para esse conglomerado econômico.

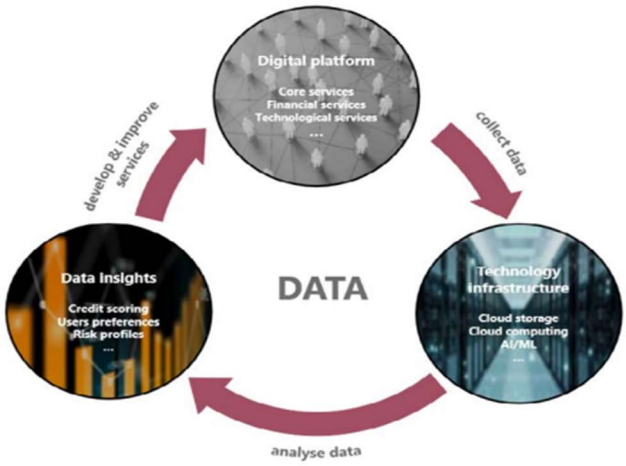
Os autores Juan Carlos Crisanto, Johannes Ehrentraud, Marcos Fabian e Amélie Monteil (2022) apontam que as grandes companhias podem ser divididas em *regionais* e *globais,* dependendo da sua atividade principal, a empresa pode ter um ramo de atuação preponderante em determinada região do globo. À título de ilustração, se pode citar o *Mercado Libre.com,* que tem seus maiores índices de atuação na América Latina, e a *Amazon.com,* que tem atuação em um mercado global, consequentemente, uma base de consumidores mais extensa.

Em seus modelos de negócio, há o serviço principal, que é a própria razão de existir da plataforma, que são complementados por uma ampla gama de serviços, como os financeiros e tecnológicos. Essa complementação, cria um ecossistema complexo, porque essas plataformas são alimentadas por vários atores que participam do ecossistema das big techs. Esses atores compartilham dados e fornecem serviços uns aos outros, ou seja, criando uma relação de dependência entre eles (Crisanto; Ehrentraud; Fabian, 2022, pág. 3).

Os serviços tecnológicos mencionados, podem ser definidos como as infraestruturas tecnológicas, que são as estruturas físicas (servidores, computadores, instalações, discos rígidos, entre outros) e não físicas (software, aplicações, estruturas de nuvem, lagos de dados, entre outros) que suportam o armazenamento e a transmissão de dados, e outras operações destas empresas. Uma das vantagens das *big techs* globais, é que elas desenvolvem internamente essas infraestruturas ou por meio de filiais subsidiárias, parcerias e aquisições, enquanto as *big techs regionais* dependem da infraestrutura de terceiro para operar, muitas das vezes se utilizam dos serviços da *big techs globais*, dessa forma nasce uma relação de interdependência entre as companhias (Crisanto; Ehrentraud; Fabian, 2022, p. 12).

Essa parceria resulta em mais dados a serem analisados, permitindo uma leitura especializada dos comportamentos do consumidor. Basicamente, o uso de dados é um componente-chave nos modelos de negócios dessas empresas, por que a informação criada é monetizada através do processamento desses dados pelas *big techs* (Bruncko; Jacobides; Langen, 2020, p. 18).

O ecossistema criado por esse grupo de empresas e o processamento de dados realizado a partir do banco de informações de seus usuários resultam na promoção de serviços cada vez mais atrativos aos seus consumidores, formando uma relação em *looping* (Crisanto; Ehrentraud; Fabian, 2022, p. 9), conforme o gráfico abaixo:




Fonte: Crisanto; Ehrentraud; Fabian, 2022, p. 09.

O gráfico acima ilustra o ciclo da coleta de dados, sendo que (i) as plataformas digitais coletam os dados através de seus três serviços característicos (típicos, financeiros e tecnológicos), e (ii) por meio de infraestruturas tecnológicas, que podem ser estruturas próprias das *big techs* ou de terceiros parceiros dessas empresas, ocorre a análise de dados, o refinamento das informações e, por fim, (iii) as ideias oriundas da análise de dados, resultam em novos projetos e inovações dentro dos serviços típicos ou fora deles, como o uso do refinamento na atividade de publicidade direcionada. Esses passos levam a fidelização dos consumidores, bem como ao ingresso de novos usuários aos produtos das *big techs* e todo esse ciclo, consequentemente, levam a obtenção de mais dados a serem refinados, analisados e transformados em produtos para os mais variados fins (Crisanto; Ehrentraud; Fabian, 2022, pág. 12).

A forma como essas companhias analisam os dados e obtém, como produto dessa refinaria informacional, as preferências e tendências de comportamento dos usuários é:

> Uma faca de dois-gumes. Por um lado, permite que as Big Techs ofereçam serviços altamente personalizados e convenientes. Por outro lado, pode restringir suas escolhas, pois existe uma linha tênue entre conveniência no ofertado e induzimento,

> por meio de uma rede fechada tendenciosa" (Bruncko; Jacobides; Langen, 2020, pág. 5) (Tradução livre).[8]

Cada big tech utiliza estratégias singulares a fim de cativar os usuários a usarem seu serviço típico e levar seus dados para serem processados em suas redes. À exemplo, a Apple tem o foco em manter seus clientes engajados em passar o tempo em seu próprio ecossistema, que é uma "carteira fechada", somente acessível mediante autorização da empresa. Portanto, a empresa procura engajar os usuários em seus próprios produtos, tais como Apple Music, App Store, entre outros (Bruncko; Jacobides; Langen, 2020, pág. 16).

Todas essas atividades também coletam dados dos usuários, mas o diferencial da Apple, que o torna menos depende da coleta direta de dados é "que o Google paga para ser o mecanismo de pesquisa padrão em dispositivos Apple, deixando o Google fazer o 'trabalho sujo' de usar os dados e aprender com eles" (Bruncko; Jacobides; Langen, 2020, pág. 5)(Tradução livre)[9].

Esse acordo entre as gigantes da tecnologia permite que o Google seja o pesquisador padrão dos usuários da *Apple*, ensejando em um poderoso artifício de obtenção de dados para a *Google*, uma vez que há mais de 2 bilhões de aparelhos da Apple ativos no mundo.

O Facebook e o Google não dependem de hardware para monetizar, seu modelo de negócio é embasado no comportamento de seus usuários, a fim de resultar em receitas baseadas na publicidade. O *Google* coleta informações de seus serviços típicos (pesquisa) e do terceiro setor (aparelhos Android, por exemplo) para refinar e traçar perfis comportamentais e suas possíveis tendências, resultando na assertividade da publicidade proposta (anúncio), bem como no consumo de mais produtos dentro de uma empresa parceira (no caso do Google, a recomendação de vídeos no *YouTube*). (Bruncko; Jacobides; Langen, 2020, pág. 17).

O *Facebook,* por sua vez, analisa e combina os dados de todas as suas propriedades digitais, incluindo *Instagram* e *WhatsApp*, gerando informações precisas acerca das tendências comportamentais dos usuários, com fins para melhorias e criação de seus produtos, bem como para venda à terceiros com fins de publicidade direcionada. (Crisanto; Ehrentraud; Fabian, 2020, pág. 13).

---

[8]For consumers, having their preferences and habits known is a double-edged sword. On the one hand, it allows Big Tech to bring them highly customised and convenient services. But on the other, it may restrict their choices, as there is a fine line between convenience and lock in

[9]Google pays to be the default search engine on Apple devices- leaving Google to do the "dirty work" of using the data and learning from it (Bruncko; Jacobides; Langen, 2020, pág. 5).

Segundo os autores Martin Bruncko, Michael G. Jacobides e Rene Langen (2020), cada uma dessas três *Big Techs* adota uma abordagem ligeiramente diferente para aproveitar os benefícios que os dados geram – embora, para *Google* e *Facebook*, seja a própria informação que cria os fluxos de caixa. Os dados valiosos sobre os clientes e seus interesses de navegação são analisados pelo negócio de *Ad Tech*[10], que é feito internamente por algumas das *Big Techs* e por empresas externas. Como vimos, a Apple prefere monetizar as informações em seu ecossistema, dando a si mesma uma vantagem competitiva para o desenvolvimento de produtos e permitindo que o Google seja o mecanismo de busca padrão, capturando dados de seus usuários. Ao fazer isso, a Apple afasta sua responsabilidade acerca do mau uso dos dados, enquanto gera em torno de um quarto de suas receitas a partir da análise de dados coletados pelo Google (Bruncko; Jacobides; Langen, 2020, pág. 18).

Assim, se demonstra que o modelo de negócio das *big techs* envolvem a captação e o refinamento das informações dos usuários, com o fim de monetizar esses dados através da assertividade das preferências do usuário no consumo de certos produtos e comportamentos propostos.

As controvérsias e as emergentes preocupações, repousam na questão do consentimento da obtenção dos dados pessoais, que são usados no processo de análise da informação que resulta na publicidade direcionada, e na efetividade dessa análise, que pelas altas taxas de conversão da plataforma sugere uma predominância na assertividade do público selecionado, havendo uma linha tênue entre a conveniência e o induzimento tendencioso àquele resultado. Dessa forma, surge o risco dessas plataformas promoverem escolhas aos usuários, a partir da precisão da leitura dos hábitos do usuário e suas propensões comportamentais. (Bruncko; Jacobides; Langen, 2020, pág. 20).

Com as diversas notícias de vazamento de dados relativo às operações das *bigs techs* e de influência comportamental através do refinamento de informações, como foi utilizado nas campanhas presidenciais do Estados Unidos (Costa, F. V., Bastos, F. K. F., & dos Santos, J. M. M. G, 2022, p. 4), nasce as constantes preocupações com a proteção dos direitos dos cidadãos, em especial no meio digital, porque até advir regulamentação acerca da utilização de dados, esses eram tidos pelas *big techs* como "terra de ninguém", ensejando brechas para o

[10]**Ad Tech** é uma abreviação de "Advertising Technology", refere-se ao conjunto de softwares e ferramentas que os anunciantes usam para planejar, entregar e analisar campanhas de publicidade digital. (Bruno Luciano. AdTech: o que é? Para que serve? Por que usar essa tecnologia?, 2023).

acometimento de vários abusos (Costa, F. V., Bastos, F. K. F., & dos Santos, J. M. M. G, 2022, p. 5).

Com o advento da Lei nº.13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), o cenário da proteção de dados expressou significativo avanço, na medida que reconheceu a importância da tutela do tratamento de dados e, posteriormente, positivado no rol de direitos fundamentais do art. 5, inciso LXXIX da Constituição Federal brasileira pela emenda à constituição nº 115/22.

As referidas inovações legislativas mudaram o viés interpretativo sobre a relevância do tratamento de dados, bem como a responsabilização no caso de falha na cadeia de custódia dos dados sensíveis ou pessoais. Assim sendo, a análise da legislação pátria regulamentadora dos direitos e deveres e dos casos de responsabilização dos tratadores de dados é imprescindível para compreensão do papel do usuário, da plataforma que coleta os dados e da tratadora de dados, bem como dos entes estatais, nas atribuições originárias de garantir a promoção dos direitos fundamentais dos cidadãos.

## II- DAS REGULAÇÕES SOBRE AS PRESTADORAS DE SERVIÇOS NO BRASIL E A RESPONSABILIDADE CIVIL

Da análise do método de operacionalização das *big techs,* se denota que sua atividade perpassa elementos que são objetos de tutela estatal, protegidos tanto em normas constitucionais e infraconstitucionais. Dessa forma, a averiguação das normas jurídicas incidentes e dos entendimentos dos juízes brasileiros é fundamental para compreensão de como a responsabilização das *bigs techs* será aplicada no Brasil.

### 2.1. Das normas jurídicas protetoras de dados pessoais

É incontroverso que as grandes empresas transformaram o processamento de informações em um ativo financeiro, através da sua metodologia de monetização da informação produzida pelo usuário a partir do uso dos produtos dessas empresas (Costa, F. V., Bastos, F. K. F., & dos Santos, J. M. M. G., 2022, p. 5).

Os dados coletados, muitas vezes, envolvem conteúdo sensível, dada a natureza pessoal e a circunstância da coleta. Conforme exposto no capítulo 1, item 1.3, da presente monografia, essas grandes empresas utilizam a informação produzida pelo usuário em seus serviços disponibilizados, tais como o *Instagram* e *WhatsApp Messenger,* e como se sabe, a sociedade em geral está conectada 24 horas por dia, se utilizando das redes sociais para todo tipo de fim, de natureza pública e privada (Jeff Orlowski, 2020).

Dessa forma, é razoável se compreender que a partir da coleta e do tratamento dos rastros digitais deixados pelos usuários se pode traçar perfis de consumo, estilos de vida, preferências pessoais e políticas, influenciando um grande mercado digital (Barros, 2021).

Os autores Fabrício Costa, Frederico Bastos, João Manoel Dos Santos, em publicação na Revista Brasileira de Direito Civil em Perspectiva, apontam que "a sociedade está sendo monitorada diuturnamente mediante os rastros digitais *(footprints)* que são coletados, dos quais muitos são dados pessoais de natureza sensível, utilizados sem o devido consentimento e, na maioria das vezes, sem que o usuário tenha ciência de que está involuntariamente participando de um *'big brother'* virtual com efeitos na vida real" (2022, p. 3).

Ao inserir a proteção de dados pessoais no rol dos direitos e garantias fundamentais[11], por meio da emenda constitucional 115/2022, foi conferido maior proteção jurídica aos direitos conexos à proteção de dados pessoais, como os direitos à privacidade e a proteção da honra e imagem (art.5, X também da CF/88) (Costa, F. V., Bastos, F. K. F., & dos Santos, J. M. M. G., 2022, p. 6).

Assim, denota-se que a defesa dos direitos conexos à proteção de dados, também são de suma importância, porque a "[...] privacidade, mais do que um direito, é uma necessidade humana para o desenvolvimento da sua personalidade[...]" (Costa, F. V., Bastos, F. K. F., & dos Santos, J. M. M. G., 2022, p. 4).

O professor Ingo Sarlet aponta que os principais pilares do nascimento a um direito à proteção de dados são alguns direitos da personalidade, como o direito à privacidade e ao livre desenvolvimento da personalidade:

> "[...] o conteúdo (no sentido do âmbito de proteção normativo) de um direito fundamental à proteção de dados pessoais, embora fortemente articulado com o princípio da dignidade da pessoa humana e de outros direitos fundamentais, em especial o direito ao livre desenvolvimento da personalidade e alguns direitos especiais de personalidade, como é o caso, entre outros, do direito à privacidade e do assim chamado direito à autodeterminação informativa, não se confunde com o do objeto da proteção de tais direitos[...]" (SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. Direitos Fundamentais & Justiça, 2020, p. 10).

Dessa forma, os direitos à privacidade e o livre desenvolvimento da personalidade estão diretamente ligados à necessidade de proteção dos dados pessoais sensíveis, embora tenha por âmbito de proteção objetos diversos em si. Diante da complexidade de elementos constitucionais que se relacionam com a proteção de dados, é necessário uma breve dissertação acerca dos elementos conexos à proteção de dados.

Primeiramente, cabe mencionar o direito à privacidade, que está positivado na Constituição Federal brasileira, mais especificamente, no artigo 5º, inciso X, e tem por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público (Branco, 2009, p. 420). Este direito é visto como um dos pilares da dignidade da pessoa humana, garantindo a inviolabilidade da vida privada e protegendo os indivíduos contra ingerências indevidas em sua intimidade.

[11]Art. 5º [...] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Para Tércio Sampaio Ferraz, o direito à privacidade consiste em:

> Um direito subjetivo fundamental, cujo titular é toda pessoa física ou jurídica, brasileira ou estrangeira, residente ou em trânsito no país; cujo conteúdo é a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por só a ele lhe dizerem respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão; e cujo objeto é a integridade moral do titular (Ferraz Júnior, 1993, p. 440).

Essa definição reforça a ideia de que a privacidade é um direito essencialmente vinculado à liberdade individual, permitindo que cada pessoa controle as informações sobre si mesma.

De modo geral, há consenso que se trata de um direito relativo ao indivíduo perante a sociedade, uma vez que se remonta ao direito de "ficar só" da pessoa. Entretanto, ao mesmo tempo, há uma dificuldade em se conceituar e pacificar o que é o direito à privacidade, considerando os avanços tecnológicos que dificultam a percepção do que é público ou privado (Costa, F. V., Bastos, F. K. F., & dos Santos, J. M. M. G., 2022, p. 12).

Em sentido mais estrito, se traduz na pretensão da pessoa não ser foco de observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiro ou ao público em geral (Branco, 2009, p. 423).

No Brasil, nas primeiras constituições, como a do Império de 1824, o direito à privacidade estava diretamente relacionado ao direito à propriedade, com uma abordagem que priorizava a proteção da esfera física e a inviolabilidade do domicílio, evitando que o indivíduo fosse perturbado em sua propriedade. Esse conceito se limitava a barreiras físicas e ao espaço privado. No entanto, com o avanço da tecnologia e o crescimento da mídia, sobretudo a partir do século XX, surgiu a necessidade de repensar o conceito de privacidade, adaptando-o às novas realidades sociais e tecnológicas, como a proteção de informações pessoais e dados sensíveis. Nesse contexto, a privacidade passou a abranger não apenas a proteção contra invasões físicas, mas também a defesa contra a intrusão na vida pessoal por meios tecnológicos e midiáticos (Soares, 2018, p. 23).

Em 1890, no contexto do sistema americano de justiça, o *Common Law* testemunhou debates profundos sobre a existência de um direito de "ser deixado em paz", promovidos por Warren e Brandeis, que defendiam o direito à privacidade como uma proteção contra os abusos da imprensa (Ehrhardt; Peixoto, 2020, p. 5). Essa concepção incorporava um teor psicológico no conceito de dano à personalidade, atribuindo à privacidade o papel de salvaguardar a

integridade emocional e o controle sobre as informações pessoais (Ehrhardt; Peixoto, 2020, p. 7).

Com base na evolução doutrinária do direito à privacidade, este passou a abranger outros aspectos dos direitos da personalidade na medida que novas turbações a esse direito iam ocorrendo devido às naturais evoluções da sociedade e da tecnologia. Dessa forma, a proteção de dados, em um contexto atual, é um elemento fundamental na preservação da privacidade dos indivíduos (Soares, 2018, p. 9**)**.

O processo de monetização conduzido pelas grandes empresas de tecnologia, as chamadas *big techs*, demonstra um grande potencial para violar o direito à privacidade dos usuários. A análise e o tratamento massivo de dados, muitas vezes sem consentimento adequado, permitem que essas empresas exerçam influência direta sobre aspectos íntimos da vida dos indivíduos, manipulando suas decisões e explorando seus dados como matéria-prima para a geração de receita (Carvalho, 2018, p. 28).

O uso de dados pessoais como insumo para essas atividades econômicas é uma prática que gera enormes fluxos de receita em detrimento das informações sensíveis dos usuários, infringindo diretamente os direitos da personalidade dos indivíduos e expondo-os a riscos de invasão de privacidade (Carvalho, 2018, p. 80).

Apesar da estreita relação entre a proteção de dados e a privacidade, o professor Ingo Sarlet aponta que "o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade[…]*"* (Sarlet, 2020, p. 7).

Nesse mesmo ritmo, com base nas breves considerações feitas acerca do direito à privacidade, também, se mostra necessário a análise do direito, igualmente constitucional, ao livre desenvolvimento da personalidade, uma vez que *"[...]* o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII)[...]" (Brasil, Supremo Tribunal Federal, ADI 6649/DF, 2023, p. 251).

Dessa forma, o legislador também considerou o direito ao livre desenvolvimento da personalidade como ponto a ser observado e resguardado no âmbito do tratamento de dados, especialmente no que se refere aos dados digitais, que, como visto no capítulo acima, é a matéria prima utilizada pelas *big techs* para o processo de monetização.

No que se refere ao *livre desenvolvimento da personalidade*, essa deve ser entendida como um direito de liberdade individual em relação à constituição da personalidade, a fim de garantir a autonomia de constituir uma personalidade livre, sem qualquer imposição de outrem, preconizando um direito à individualidade (Miranda, 2013).

Ademais, a Constituição Federal de 1988 não consagra positivamente o referido direito, mas em decorrência do *princípio da dignidade humana*, sendo um dos requisitos para sua efetivação, a promoção do livre desenvolvimento da personalidade. Esse também não se confunde com o *direito à personalidade*, que remonta a questão da identidade do indivíduo, bem como a forma que o indivíduo se mostra e é percebido pelos outros (Miranda, 2013), matéria que também deve ser tutelada pelo Estado.

O direito geral da personalidade pode ser de natureza subjetiva, tendo em vista estar relacionada com a defesa da pessoa humana em formar sua personalidade livre de influências externas, assegurando uma autodeterminação (Vieira, 2020).

No tocante ao livre desenvolvimento da personalidade objetiva, as relações sociais e ambientais em que a pessoa está inserida também afetam o pleno desenvolvimento do seu ser, por isso é preciso que exista a garantia da liberdade e ambiente adequado para o livre desenvolvimento da personalidade. Sendo função do Estado zelar pelas condições adequadas necessárias para a autoconstrução da pessoa, através de uma "juridificação", de atos que possibilitem aos indivíduos desenvolver sua personalidade (Miranda, 2013).

No Brasil, a novel legislação 13.709/2018, Lei Geral de Proteção de Dados (LGPD), reconheceu positivamente o referido direito nos artigos 1º[12] e 2º, inciso VII[13], representando significativo avanço na promoção da proteção dos dados pessoais, tendo em vista que até a promulgação da LGPD o direito fundamental ao livre desenvolvimento da personalidade estava apenas implicitamente positivado na Constituição Federal. (Sarlet, 2020, p. 6).

A lei referida foi fruto de várias contribuições da sociedade, ostentando disposições modernas e em consonância com diplomas legais de outros países, tendo por objetivo a proteção dos direitos fundamentais de liberdade, de privacidade e ao livre desenvolvimento da personalidade da pessoa natural. De forma que o direito fundamental à liberdade assume papel preponderante ao lado da privacidade, mas, ao mesmo tempo, o legislador destaca a proteção à

[12]Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
[13]Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...]VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

liberdade de desenvolvimento da personalidade da pessoa natural. É notável a complexidade e profundidade dos direitos fundamentais conexos que a Lei 13.709/2018 busca proteger e regular (Carvalho, 2018, p. 56/57).

Dessa forma, a privacidade passa a ser um valor fundamental para o livre desenvolvimento da personalidade, bem como da dignidade do usuário, valores que devem ser garantidos pelo Estado aos seus jurisdicionados. Com o atual cenário da monetização de dados pessoais e a premência de se resguardar o direito fundamental à privacidade e seus valores conexos, a LGPD se propõe a regular e oferecer maior proteção aos direitos fundamentais do usuário, conforme se verá no tópico abaixo.

Não obstante, considerando os avanços tecnológicos ocorridos após a década de 2000, em especial no tocante à evolução das redes sociais, que deu formato a um novo modelo de negócio, o qual tem por matéria-prima o dado do usuário, adveio a necessidade de regular a coleta e o tratamento de informações.

Para tanto, em 14 de agosto de 2018 foi promulgada a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709/2018, que entrou em vigor somente em setembro de 2020.

A referida lei representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais, como para instituições públicas e privadas. A proteção de dados pessoais também passou a constar no rol de direitos e garantias fundamentais (art. 5, LXXIX), a partir da promulgação da Emenda Constitucional n. 115/2022 (STJ, 2024).

A lei em comento é aplicável 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 no qual estejam localizados os dados, desde que a operação de tratamento de dados seja realizada no Brasil. Também, toda aquela atividade de tratamento que tenha por objetivo a oferta de bens ou serviços ou, ainda, o tratamento ou coleta de dados de indivíduos localizados no país (Brasil, 2018).[14]

[14]Art. 3º Esta 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: I - a operação de tratamento seja realizada no território nacional; II - 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; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.(Brasil, 2018)

Se exclui da aplicação da lei os dados tratados ou coletados para fins exclusivamente jornalísticos, artísticos e acadêmicos, além de informações relacionadas exclusivamente à segurança pública, defesa nacional, segurança do Estado e as atividades de investigação e repressão de infrações penais, conforme artigo 4 da Lei em estudo (Brasil, 2018)[15].

O artigo 2º da LGPD, expressa os fundamentos da disciplina, como sendo: I – o respeito à privacidade, II - a autodeterminação informativa, III – a liberdade de expressão, de informação, de comunicação e de opinião, IV – à inviolabilidade da intimidade, da honra e da imagem, V – o desenvolvimento econômico e tecnológico e a inovação, VI – da livre-iniciativa, a livre concorrência e a defesa do consumidor e VII – os direitos humanos, do livre desenvolvimento da personalidade, da dignidade e o exercício da cidadania pelas pessoas naturais. De modo a se extrair um extenso rol de diretrizes a serem consideradas pelo aplicador da lei, bem como a serem observadas pelos operadores e controladores de dados (Brasil, 2018).

Na dissertação acerca do direito fundamental à privacidade, ante monetização de dados pessoais na internet, o autor, Victor Miguel Barros de Carvalho, apontou que:

> São fundamentos que continuam em linha com as ideias expostas e defendidas pelos estudiosos do tema no país; atuando como delineações gerais, como balizas e limites, estes fundamentos conseguem englobar a complexidade que a contextualização da privacidade no âmbito da proteção de dados pessoais ostenta, tal qual demanda, também, a analogia com a metáfora de luz e sombra. Fundamentos que logram encaixar não apenas o respeito à privacidade, aos direitos humanos, à liberdade e valores conexos à dignidade da pessoa humana na regulamentação do tratamento de dados pessoais, mas também o desenvolvimento econômico, tecnológico, a inovação, a livre iniciativa e livre concorrência. (CARVALHO, 2018. p. 57).

De modo que a LGPD, concomitantemente a sua intenção de proteger a privacidade e os direitos fundamentais conexos, é capaz de não interferir no desenvolvimento econômico, tecnológico e, igualmente, nas vontades e interesses particulares envolvidos (Carvalho, 2018, p. 59).

Avançando no tema, o artigo 5° da legislação em estudo, define especificamente os objetos e os atores envolvidos no tratamento e na coleta de dados. À exemplo, o inciso II define como dado sensível aquele *"sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado*

[15]Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;II - realizado para fins exclusivamente:a) jornalístico e artísticos; ou III - realizado para fins exclusivos de:a) segurança pública;b) defesa nacional;c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; [...] (Brasil, 2018)

*referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural",* diferenciando substancialmente do que foi definido como o simples dado pessoal (Brasil, 2018).

Carvalho (2018), aponta que "a especificação de dados sensíveis é de suma importância na conformação da proteção à privacidade, já que são dados relacionados a questões que, em possível violação da privacidade, podem ter consequências nefastas […] ".

A norma também foi bem específica ao definir quem são os atores envolvidos no tratamento e coleta de dados, esses que foram denominados de controlador, operador e encarregado.

O controlador, nos termos do inciso VI do art. 5 da LGPD, é a *"pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais",* devendo se entender como o agente detentor do poder decisório da finalidade do tratamento de dados. No que se refere ao operador[16], é definido como aquele que realiza o tratamento de dados, ou seja, quem faz uso das informações e produz alguma utilidade/finalidade, em obediência às estipulações do controlador. Esses dois atores, o operador e o controlador são chamados de *agentes de tratamento*[17] pela norma. (Brasil, 2018)

A doutrinadora Patrícia Peck, ao analisar a LGPD, destacou a influência do GDPR (*General Data Protection Regulation*), que é a regulação europeia de proteção dados, na elaboração do documento brasileiro, por exemplo "a questão do controlador/processador do GDPR, que no LGPD ganharam o nome de controlador/operador, cujas ações, funções e responsabilidades são equivalentes, só se modificando a nomenclatura adotada... *"* (Peck, 2023).

O artigo 6 e seus dez incisos da LGPD, elenca os princípios a serem observados nas atividades envolvendo tratamento de dados. Além do princípio da *boa-fé*, previsto no caput, os incisos abordam elementos inovadores que decorrem do princípio amplo que é a boa-fé. o Mestre Victor M. Barros de Carvalho, faz breves apontamentos acerca dos incisos do artigo em estudo:

> [...] os princípios da finalidade (realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades), da adequação (compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento), da necessidade (limitação do tratamento ao mínimo

[16]Art. 5º Para os fins desta Lei, considera-se: [...] VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;(Brasil, 2018)

[17]Art. 5º Para os fins desta Lei, considera-se: [...] IX - agentes de tratamento: o controlador e o operador (Brasil, 2018)

> necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados), livre acesso (garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais), qualidade dos dados (garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento), transparência (garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial), segurança (utilização de medidas 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 difusão), prevenção (adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais), não discriminação (impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos) e responsabilização e prestação de contas (demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas), em seus incisos. (Carvalho, 2018. p. 60).

Em alusão ao artigo 6 da LGPD, Patrícia Peck destaca que "a garantia da proteção dos direitos dos titulares dos dados pessoais é pautada na indicação de princípios relativos ao tratamento de dados pessoais, cuja ação deve respeitar os limites dos direitos fundamentais" (Peck, 2023, p. 40).

A autora resume o artigo 6º da LGPD, narrando que "o tratamento de dados pessoais deve observar a boa-fé e possuir finalidade, limites, prestação de contas, garantir a segurança por meio de técnicas e medidas de segurança, assim como a transparência e a possibilidade de consulta aos titulares." (Peck, 2023, p. 40).

O artigo 7º[18] estipula um rol de hipóteses nas quais o tratamento de dados poderá ser realizado. Ressaltando-se as exigências expressas de consentimento do titular (inciso I) e demarcando as hipóteses que em se poderá excluir o requisito do consentimento do titular, presente nos incisos II até o X do referido artigo (Brasil, 2018).

[18]Art. 7° 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 n. 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 [...] (Brasil, 2018)

Novamente, valendo-se dos notáveis comentários à LGPD da Patrícia Peck, essa que frisa que *"*as hipóteses mencionadas referem-se tão somente ao tratamento de dados pessoais, excluindo-se o tratamento de dados pessoais sensíveis, que possui disposição própria no art. 11 da LGPD" (Peck, 2023. p. 41).

O requisito do artigo 7, inciso I (consentimento), é melhor abordado no artigo subsequente da LGPD.

O artigo 8º[19] desenvolve melhor o tema do consentimento, uma vez que reconhece a hipossuficiência do titular do consentimento ao atribuir, no §2º do artigo, o ônus da prova ao controlador acerca da comprovação que obteve o consentimento livre de quaisquer vícios (LGPD, 2018), prática semelhante ao da inversão do ônus da prova presente no Código de Defesa do Consumidor (Lei 8.078/90).

Nesse sentido, a questão do consentimento, em um contexto de constante evolução tecnológica, torna imprescindível a garantia da ciência inequívoca em relação à finalidade da coleta e limitar o acesso não autorizado dos dados sensíveis é fundamental para assegurar a liberdade e a privacidade (Peck, 2023. p. 41).

Ressalta-se a liberdade das empresas em utilizar os dados de maneira transparente e ética, propiciando equilíbrio entre a proteção de direitos fundamentais da personalidade e o livre desenvolvimento econômico a ser garantido a essas empresas, que também são detentoras de direitos, desde que observem os deveres implícitos no manejo de objetos tão sensíveis (Peck, 2023, p. 41).

O controlador do tratamento de dados deverá justificar seu legítimo interesse através da finalidade legítima, conforme apregoa o artigo 10 da LGPD[20]. No entendimento da doutrinadora:

---

[19]Art. 8° O consentimento previsto no inciso I do art. 7° desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.§ 1° Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.§ 2° Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.§ 3° É vedado o tratamento de dados pessoais mediante vício de consentimento.§ 4° O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.§ 5° O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.[...] (Brasil, 2018).

[20]Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:I – apoio e promoção de atividades do controlador; e II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.[...] (Brasil, 2018).

> A finalidade apontada pelo controlador para a realização do tratamento de dados deve ser pautada em fundamentações claras e legítimas, e somente os dados real e estritamente necessários devem ser coletados com vistas à garantia do direito a proteção à privacidade do titular.(Garrido, 2023, p. 42).

Também, vale transcrever o Enunciado 683 da IX Jornada de Direito Civil realizada pelo CJF, reconhecendo a forte influência do princípio da boa-fé no direito privado brasileiro e sua conexão com a vedação do abuso de direito, bem como guardando relação com uma legítima expectativa no dever de lealdade e de confiança com o titular de dados, se entendeu que "A legítima expectativa do titular quanto ao tratamento de seus dados pessoais se relaciona diretamente com o princípio da boa-fé objetiva e é um dos parâmetros de legalidade e juridicidade do legítimo interesse*"* (Brasil, CJF, 2022)

O artigo 11[21] aponta as hipóteses legais para o tratamento de dados pessoais sensíveis, acentuando que, nesses casos, o consentimento deve ser "específico e destacado", conforme inciso I do artigo referido, além de elencar as circunstâncias que possibilitam o manejo de tais espécies de dados sem o consentimento do titular, nos termos do inciso II e suas alíneas do artigo 11.

Se referindo ao artigo 11 da LGPD, Patrícia Peck aponta:

> A importância do consentimento para a realização do tratamento de dados sensíveis é intrínseca à validade dessa ação, todavia há algumas situações em que tal consentimento pode ser relativizado (excetuado), como pontua o art. 11.
> Essas situações são relacionadas ao cumprimento de obrigações legais por parte do controlador, à garantia da segurança do titular, à prevenção à fraude, à execução de políticas públicas, à proteção da vida/incolumidade física, assim como à tutela da saúde. Ainda que o tratamento de dados sensíveis seja realizado mediante a dispensa do consentimento, é obrigação do controlador publicizar essa situação.

[21]Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9° desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.§ 1° Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica. § 2° Nos casos de aplicação do disposto nas alíneas a e b do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei. [....](Brasil, 2018)

> Os dados sensíveis merecem tratamento especial porque em algumas situações a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa. (Garrido, 2023, p. 43).

Ante o exposto, buscando, em um primeiro momento, tecer considerações iniciais acerca de conceitos essenciais da Lei Geral de Proteção de Dados, os quais se relacionam, principalmente, à atividade desenvolvida pelas *big techs*, torna-se conveniente explorar a aplicação da responsabilidade quando a atividade de tratamento de dados estiver em descompasso com as normas regulamentares, de modo a ocasionar um dano ou violação aos direitos da personalidade.

Dessa forma, cabe investigar as disposições específicas na LGPD que tratam e auxiliam na fundamentação do assunto. Para tanto, se valerá dos ensinamentos dos autores Fabrício Veiga Costa, Frederico Kern Ferreira Bastos e João Manoel Miranda Gomes dos Santos, quando discorreram acerca da responsabilidade civil das grandes empresas de tecnologia *"big techs*"em casos de violação ao direito fundamental à proteção de dados, na Revista Brasileira de Direito Civil em Perspectiva, publicado em 2022.

Em um primeiro momento, os autores, remetem aos dispositivos legais que abordam a responsabilidade, tais como o artigo  37, parágrafo 6º da Constituição Federal e os artigos 927 e seguintes do Código Civil, e relembram que o fato social sempre anda a frente do direito, em busca de equivalência inalcançável entre o ser e o dever ser, de modo que a LGPD almeja garantir segurança ao titular dos dados (Bastos; Costa; Santos, 2022, p. 6).

Os casos de violação dos deveres de cuidado e segurança, tal como delineados no artigo 6, incisos VII e VIII da LGPD[22], demandam uma análise aprofundada acerca da natureza jurídica da responsabilização, conforme delineado no inciso X[23] do referido artigo (Bastos; Costa; Santos, 2022, p. 6).

Os autores demonstram uma dualidade na doutrina, porque parte dela, a teor da interpretação dos artigos 42 e 43 da LGPD,[24] entende que a criação de um extenso rol de deveres

[22]Art. 6º. [...] VII - segurança: utilização de medidas 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 difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (Brasil, 2018)

[23]Art. 6º. [...] X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil, 2018)

[24]Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados

de cuidado, reflete na intenção legislativa de analisar a culpa das operadoras de dados. Também, essa corrente doutrinária afirma que ao instituir princípios de responsabilização e de prestação de contas, acaba por se aproximar de elementos próprios da responsabilidade subjetiva, em que para sua configuração é necessário a presença de descumprimentos dos deveres de segurança (Bastos; Costa; Santos, 2022, p. 7).

A segunda corrente doutrinária defende a responsabilização de natureza objetiva, com base na teoria do risco, o qual seria intrínseco à atividade de armazenamento de dados pessoais de terceiros, haja vista o destaque dos deveres de segurança e prevenção *(compliance*) presentes no art. 6, inciso VII e VIII, e da obrigação de prestação de contas *(accountability)*, inseridos no inciso X do mesmo dispositivo da LGPD. (Bastos; Costa; Santos, 2022, p. 8).

Dessa forma, os deveres de mitigar os riscos no tratamento de dados são inerentes da atividade, tendo a prevenção como resultado do reconhecimento dos riscos no desenvolvimento do tratamento de dados, com o entendimento das suas "fraquezas" se pode evitar a violação dos dados e os danos aos direitos fundamentais (Bastos; Costa; Santos, 2022, p. 8).

Também, se deve destacar a similaridade de regime entre a LGPD e o Código de Defesa do Consumidor (Lei 8.078/1990), como a possibilidade de inversão do ônus da prova (art. 42, §2 LGPD), previsto em ambas as legislações. São pontos que favorecem o entendimento pela responsabilidade objetiva da violação de dados (Bastos; Costa; Santos, 2022, p. 9).

Diante de tais considerações, a responsabilização objetiva aparece atender melhor a dimensão dos direitos inerentes à personalidade, ante a violação dos dados pessoais sensíveis e a relevância dessa violação, considerando o contexto de direitos fundamentais conexos, nesse sentido:

> [...] que proteger os dados pessoais atualmente significa proteger a própria personalidade jurídica e digital do usuário, identidades que se misturam ao se relacionar vida pessoal e virtual. Ademais, considerando o grau de inserção de dados pessoais no meio digital a privacidade passa a ser um valor fundamental para desenvolvimento da autodeterminação informacional e da dignidade do usuário. Não

pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. [...] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (Brasil, 2018).

> sem razão, a proteção de dados foi elevada à condição de direito fundamental, status já reconhecido pelo Supremo Tribunal Federal antes mesmo da aprovação da referida emenda, ao analisar a Arguição de Descumprimento de Preceito Fundamental de nº.6387/ DF (2020), na qual havia sido reconhecido o caráter de direito fundamental implícito à proteção de dados (Costa, Bastos, Santos, 2022, p. 10).

O artigo 43 e os inciso I, II e III tratam das excludentes de responsabilidade das operadoras de dados, nessa senda, cabe analisar a aplicabilidade da excludente de ilicitude sobre o vazamento de dados por questões de força maior ou por fatos de terceiros, no contexto da Lei de Proteção de Dados.

Se depreende a inviabilidade da tese de aplicabilidade da excludente de ilicitude e qualquer discussão da isenção de responsabilidade, ao passo que, na realidade, a falta da possibilidade de escolher, monitorar, controlar os dados coletados pelas grandes empresas de tecnologia, pressupõe uma majorante na responsabilidade do operador dos dados em caso de vazamento de qualquer forma, seja com culpa ou sem culpa (Bastos; Costa; Santos, 2022, p. 13).

Nessa linha de raciocínio:

> [...] Assim, consequentemente, a forma como é coletado, comercializado os dados particulares, no comércio de informações, sem o expresso consentimento do uso das informações para os fins comerciais que são destinados, violam a orbita da privacidade, não se limitando, portanto, a excludente de ilicitude aos fatos e atos de hackeamento e violações de força maior. (Bastos; Costa; Santos, 2022, p. 13).

Portanto, haja vista a privacidade e a ampla relação com outros direitos fundamentais, aliado ao fato incontroverso da falta de liberdade do titular das informações em escolher quais dados sensíveis podem ser objeto de tratamento, não se pode admitir a excludente de ilicitude diante dos atos de terceiro, posto que *"a* ilegalidade dos monitoramentos da vida privada faz das plataformas de dados das grandes empresas de tecnologia responsáveis pelo conteúdo violado ilícito, ainda mais que tais dados são comercializados" (Bastos; Costa; Santos, 2022, p. 17).

Nesse sentido, a inaplicabilidade do caso fortuito ou ato de terceiro, é justificada, especialmente, na ausência de consentimento expresso e específico para a coleta de dados sensíveis, bem como na insuficiência de garantia da autodeterminação informacional. Não se faz necessário, portanto, a ocorrência de um dano efetivo relacionado aos dados coletados, pois a própria coleta de dados sensíveis, resultante de monitoramento ilegal, configura violação suficiente para ensejar dano aos direitos fundamentais à privacidade (Bastos; Costa; Santos, 2022, p. 18).

Desse modo, o dano decorrente de caso fortuito ou ato de terceiro envolvendo dados sensíveis não deve ensejar a exclusão da responsabilidade das operadoras, tratadoras e controladoras de dados.

Considerando ser uma inovação legislativa, as interpretações das normas pelos tribunais brasileiros são, também, recentíssimas. Cabendo ao presente trabalho percorrer os entendimentos da justiça brasileira acerca da responsabilidade das bigs techs no cenário contemporâneo.

Por fim, previamente à análise do posicionamento do judiciário brasileiro sobre a responsabilização das *big techs,* também cabe mencionar o Código de Defesa do Consumidor (CDC), instituído pela Lei nº 8.078/1990, que é um marco jurídico destinado a regulamentar as relações de consumo no Brasil.

Sua natureza é derivada de normas de ordem pública e interesse social, conforme disposto em seu artigo 1º[25], o que significa que suas normas são imperativas e não podem ser afastadas pelas partes envolvidas na relação consumerista. O CDC visa proteger a parte mais vulnerável nas relações de consumo, o qual é, por muitas vezes, o consumidor, que acaba sendo compelido a aceitar cláusulas desproporcionais para poder usufruir do serviço ou produto desejado, sem possibilidade de discussão ou pactuação em contrário, o que realça o desequilíbrio entre as fornecedor e consumidor.

Ademais, o CDC, ao tratar do uso de informações pessoais em bancos de dados e cadastros, estabelece uma série de direitos e garantias, como o acesso e a correção de dados pelos consumidores. Conforme observa Doneda (2011, p. 103), essa regulamentação adota elementos alinhados aos *Fair Information Principles,* promovendo maior transparência e controle sobre o tratamento de dados pessoais, especialmente em questões relacionadas à concessão de crédito.

Por meio de sua aplicabilidade abrangente e principiológica, o CDC constitui um pilar do ordenamento jurídico brasileiro, atuando como um mecanismo fundamental para assegurar justiça e equidade nas relações de consumo. Sua importância transcende o cenário tradicional, adaptando-se aos desafios do ambiente digital e reforçando os direitos dos consumidores em face das novas dinâmicas econômicas e tecnológicas (Zanatta, 2020, p. 13-14).

[25]Art. 1° O presente código estabelece normas de proteção e defesa do consumidor, de ordem pública e interesse social, nos termos dos arts. 5°, inciso XXXII, 170, inciso V, da Constituição Federal e art. 48 de suas Disposições Transitória (Brasil, 1990)

## 2.2. Posicionamento do judiciário brasileiro em matéria de responsabilização das *bigs techs*

Até o presente momento de publicação deste trabalho acadêmico, não houveram significativas decisões envolvendo a coalizão entre o tratamento de dados e as *big techs.*.

Assim, se valerá, para analisar os desafios e as tendências da justiça brasileira no confronto à violação e tratamento irregular de dados pessoais, das recentes e inovadoras decisões exaradas no primeiro grau do Tribunal de Justiça de Minas Gerais e do Maranhão.

### 2.2.1. Processos nº 5127283-45.2019.8.13.0024 e 5064103-55.2019.8.13.0024

Ambos os casos se tratam de ações civis públicas, ajuizadas pelo Instituto Defesa Coletiva, que tramitaram na 29º Vara Cível da Comarca de Belo Horizonte/MG, julgadas em 24/07/2023, pelo Juiz de Direito Jose Mauricio Cantarino Villela.

A ação 5064103-55.2019.8.13.0024 foi ajuizada em decorrência de um ataque cibernético, ocorrido em setembro de 2018, no qual a rede social do *Facebook* comprometeu cerca de 29 milhões de dados de usuários. Sendo que diversos usuários tiveram informações básicas como nome, e-mail e número de telefone expostos, enquanto os 14 milhões restantes tiveram dados mais sensíveis acessados, incluindo status de relacionamento, localidade, idioma, cidade natal, dispositivos utilizados, educação, histórico de localização e outros (TJ/MG, 2023, p. 3).

Posteriormente, em abril de 2019, um novo vazamento foi identificado, que expôs indevidamente 540 milhões de registros dos usuários, incluindo senhas de 22 mil contas. Os dados vazados, continham informações detalhadas das interações dos usuários na plataforma, como curtidas, comentários e imagens, foram encontrados armazenados irregularmente em servidores da *Amazon*. (TJ/MG, 2023, p. 4).

Além disso, em dezembro de 2018, foi divulgada nova falha nos sistemas de segurança, que permitiu que aplicativos de terceiros tivessem acesso indevido às fotos de aproximadamente 6,8 milhões de usuários, conforme relatado pelo próprio *Facebook* (TJ/MG, 2023).

No que se refere ao processo de nº 5127283-45.2019.8.13.002, essa ação se deu porque, em maio de 2019, ocorreu uma vulnerabilidade no aplicativo *WhatsApp* que permitiu a invasão por *hackers*, por meio de *softwares de spyware* nos dispositivos de usuários. O ataque era

executado por meio de uma ligação via *WhatsApp*, que, mesmo não atendida, instalava o software espião. O *softwares* concedia acesso a contatos, mensagens e fotos dos usuários, e, em muitos casos, a ligação desaparecia do histórico, tornando o ataque praticamente imperceptível (TJ/MG, 2023, p. 4).

O segundo incidente, divulgado em agosto de 2019 pela agência *Bloomberg*, revelou que o *Messenger* utilizou terceirizados para transcrever áudios de usuários, sem o devido consentimento. A prática foi confirmada pela ré, que informou ter suspendido o procedimento após notificações públicas (TJ/MG, 2023, p. 4).

Ressalta-se que o feito foi julgado conjuntamente em razão da conexão entre os feitos, nos termos do art. 55 da Lei nº 13.105/2015 (Código de Processo Civil).

Na fundamentação do *decisum* o magistrado, no mérito das questões, mencionou a incidência da legislação consumerista, em especial os artigos 6, incisos I e III[26], bem como os artigos 14[27] e 37[28] do Código de Defesa de Consumidor, de modo a reconhecer a natureza consumerista da relação entre o *Facebook* e o usuário, e reforçar os direitos basilares do consumidor e a responsabilização do fornecedor pelo serviço ou produto defeituoso (TJ/MG, 2023, p. 10).

Prosseguindo a argumentação, destacou que "[...]A evolução da sociedade e o desenvolvimento da tecnologia, deflagra uma nova era da sociedade, denominada era das informações e compartilhamento de dados[...]*"* (TJ/MG, 2023, p. 11), introduzindo a incidência da Lei Geral de Proteção de Dados aos casos em análises, destacando que:

> "[…].a Lei Geral de Proteção de Dados surge em um ambiente de evolução tecnológica e de manuseio de dados pessoais na condição de mercadoria, de forma que a observância aos direitos do titular de dados pessoais assume fundamental importância, exigindo o cumprimento do dever de protegê-lo e de informá-lo acerca de maneira (como), quando e em que condições serão utilizados, buscando possibilitar

[26]Art. 6º - São direitos básicos do consumidor: I – a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecido de produtos e serviços considerados perigos e nocivos; [...] III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;(Brasil, 1990)

[27]Art. 14. O fornecedor de serviços, responde independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação de serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos (Brasil, 1990)

[28]Art. 37. É proibida toda publicidade enganosa ou abusiva. § 1° É enganosa qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falsa, ou, por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço e quaisquer outros dados sobre produtos e serviços.[...] § 3° Para os efeitos deste código, a publicidade é enganosa por omissão quando deixar de informar sobre dado essencial do produto ou serviço.(Brasil, 1990)

> ao cidadão a segurança de que seus dados serão protegidos antes, durante e, após, o encerramento do tratamento[…]" (TJ/MG, 2023, p.11)

O julgador, realizando uma valoração constitucional dos objetos em discussão, sustentou que haveria base legal para responsabilização da ré, mesmo se não houvesse base legal específica, como a LGPD ou o CDC, em decorrência de garantias e direitos constitucionais, como as garantias à intimidade da vida privada, inviolabilidade do sigilo de correspondência e das comunicações e das comunicações telegráficas, de dados e telefônicas (TJ/MG, p. 11).

As condutas do *Facebook,* segundo o magistrado, recaíram em *"[...]violação desarrazoada da segurança do serviço fornecido, descumprindo o artigo 6º, incisos I e III, do CDC e artigo 6º, inciso VII e VIII, da Lei n.º 13.709/2018 [...]*" (TJ/MG, 2023), dessa forma, o ataque de *hackers* ou o compartilhamento indevido de dados dos usuários não configuram caso fortuito ou culpa de terceiro, sendo reconhecido o dever de segurança inerente do risco da atividade, *in verbis:*

> "[...]Neste sentido, entendo que as provas produzidas nos autos demonstram, de forma consistente, o defeito de prestação de serviço fornecido pelo réu, não havendo que se falar em imprevisibilidade/inevitabilidade, visto que o evento acima analisado configura fortuito interno inerente ao risco do empreendimento desenvolvido pela requerida.
>
> Cumpre registrar que a ocorrência de tal episódio era previsível em se tratando deste tipo de atividade e, mesmo diante da qualidade e de mecanismos de segurança que o réu deve oferecer, tal constatação não afasta a conclusão de que o sistema é vulnerável. E a falha desse sistema deve ser atribuída a quem dele usufrui como fonte de lucro. É o chamado risco da atividade, não havendo que se falar em culpa exclusiva de terceiro[…]"(TJ/MG, 2023)

Dessa forma ficou reconhecida a responsabilidade da empresa pelo tratamento de dados irregular, que ocasionaram ilícitos distintos e, em um contexto de ações civis públicas, o dano moral coletivo é presumido, uma vez que é "categoria autônoma de dano e se caracteriza por lesão grave, injusta e intolerável a valores e a interesses fundamentais da sociedade, independentemente da comprovação de prejuízos concretos ou de efetivo abalo moral*."* (TJ/MG, 2023, p. 13).

Por fim, diante da gravidade das infrações constatadas, o magistrado fixou a condenação do Facebook ao pagamento de indenizações por danos morais coletivos e individuais, utilizando critérios que refletem a extensão do impacto social e a função pedagógica da sanção. No processo nº 5064103-55.2019.8.13.0024, relacionado aos vazamentos de dados de milhões de

usuários entre 2018 e 2019, foi estipulada indenização coletiva no valor de R$ 10 milhões de reais.(TJ/MG, 2023, p. 15).

No que se refere ao caso envolvendo a vulnerabilidade do *WhatsApp* diante de ataque cibernético, o valor fixado para os danos coletivos foi de R$ 5 milhões de reais (TJ/MG, 2023, p. 19). No tocante aos danos morais individuais, o magistrado destacou que, para os usuários diretamente impactados, em ambos os casos, seriam devidos R$ 5 mil reais (TJ/MG, 2023, p. 20-21).

Por fim, frisou que os valores referentes aos danos morais coletivos serão destinados ao Fundo de Defesa de Direitos Difusos (FDD), conforme prevê o artigo 13 da Lei nº 7.347/1985[29], garantindo que esses recursos sejam aplicados em projetos voltados à proteção da privacidade e à segurança digital.

Cabe salientar que, atualmente, os efeitos da decisão foram suspensos em virtude da concessão do efeito suspensivo ao Recurso de Apelação do *Facebook,* o qual ainda pende de julgado pela 13ª Câmara Cível do Tribunal de Minas Gerais.

### 2.2.2. Do Processo nº 0816292-73.2020.8.10.0001

Trata-se de sentença exarada em Ação Civil Pública promovida pelo Instituto Brasileiro de Estudo e Defesa das Relações de Consumo em face da Bytedance Brasil Tecnologia LTDA, representante do *TIKTOK*, ajuizada na Comarca da Ilha de São Luís e julgada pelo juiz da Vara de Interesses Difusos e Coletivos, o Dr. Douglas de Melo Martins.

O Instituto alegou que a empresa violou a proteção legal dada aos consumidores quanto aos direitos fundamentais à privacidade, quando coletou indiscriminadamente dados pessoais (biometria facial) dos usuários, armazenando e compartilhando os referidos dados, sem o consentimento prévio dos usuários, a fim de realizar o processamento típico dessas empresas, conforme discorrido no Capítulo 1, item x do presente trabalho acadêmico.

O mecanismo que resultou na violação trata-se de "[...] uma ferramenta de inteligência artificial que automaticamente digitaliza o rosto dos usuários, visando a captura,

[29]Art. 13. Havendo condenação em dinheiro, será ela destinada a fundo gerido por conselho federal ou por conselhos estaduais, municipais ou distrital, dos quais participarão necessariamente o Ministério Público e representantes da comunidade, sendo seus recursos destinados à reconstituição dos bens lesados (Brasil, 1985).

armazenamento e compartilhamento de dados, sem o devido consentimento dos usuários[...]" (TJ/MA, 2024, p. 2) que foi implementado no serviço TIK TOK.

O Juiz de Direito, Dr. Douglas de Melo Martins, aborda a origem constitucional do tratamento e manipulação de dados pessoais, uma vez que estão relacionados à identificação de pessoa natural, estando submetidos aos "[...] limites delineados pela limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade [...]" (TJ/MA, 2024, p. 6). Importa mencionar que o magistrado reconhece a existência de relação de consumo entre os usuários e a empresa de tecnologia, relação que permanece, mesmo quando o serviço é fornecido de maneira gratuita, conforme entendimento do STJ acerca do tema (REsp n. 1.192.208/MG), de forma que o tratamento irregular de dados configura falha na prestação dos serviços (TJ/MA, 2024, p.8).

Ainda, antes mesmo do magistrado citar a LGPD na fundamentação da sentença, fez referência aos princípios constitucionais do tratamento de dados que são a finalidade, necessidade, adequação e proporcionalidade, que, como se sabe, são estruturas base da Lei Geral de Proteção de Dados (Lei 13.709/18). Também, o julgador elucidou o caso concreto sob a ótica das disposições do Marco Civil da Internet (Lei 12.965/2014), frisando, como princípios fundamentais do uso da internet, a proteção da privacidade e a proteção de dados (art. 3º, inciso II e III[30] e art. 7, inciso I, VIII e IX[31]) , por fim, destacou:

> Esses dispositivos do Marco Civil da Internet, ao estabelecerem a proteção da privacidade e dos dados pessoais, estão em consonância com o direito à autodeterminação informativa, que encontra suas bases no direito constitucional à privacidade e à proteção de dados. Dada sua densidade normativa, em 2018, foi positivado na Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que, ao reconhecer a importância da autodeterminação informativa, reforça a proteção dos dados pessoais como um elemento essencial para a preservação da privacidade e da liberdade individual. A autodeterminação informativa compreende a capacidade do indivíduo de controlar suas próprias informações, decidindo sobre sua coleta, utilização e compartilhamento por terceiros.

[30]Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II - proteção da privacidade;III - proteção dos dados pessoais, na forma da lei (Brasil, 2014).

[31]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; [...] VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (Brasil, 2014).

> Dessa forma, o arcabouço jurídico brasileiro solidifica a proteção do direito fundamental à privacidade e à proteção de dados no ambiente da internet. Assim, a coleta, uso e o tratamento indevido de dados de usuários, sem o necessário livre consentimento, configura violação dessas normas (TJ/MA - Ação Civil Pública nº 0816292-73.2020.8.10.0001).

No presente caso, a responsabilização da Bytedance Brasil Tecnologia Ltda., conforme a sentença proferida, se pautou no reconhecimento que a coleta de dados biométricos da empresa recaiu sobre os dados classificados como "dado pessoal sensível" e sua atividade, de fato, configurou tratamento de dados, nos termos do artigo 5, Inciso II e X da LGPD, ao passo que a ausência de informação expressa desse meio de tratamento nos termos de uso, infringiu a permissão legal para o tratamento de dados regular, que é o consentimento livre e consciente, nos termos do artigo 11, Inciso I da LGPD (TJ/MA, p. 08).

Dessa forma, o magistrado reconheceu que a conduta da ré configurou falha na prestação do serviço em decorrência da ausência de observação dos deveres inerentes à informação e da falta de observância das normas regulamentadoras da atividade de tratamento de dados, o que ensejou violação dos direitos fundamentais de privacidade e proteção de dados dos consumidores (TJ/MA, 2024, p. 08).

Diante dessa falha e do contexto exposto, o "[…] dano moral é presumido. Isso se justifica pelo fato de que, no contexto contemporâneo, a proteção da privacidade e dos dados pessoais é um direito fundamental cada vez mais relevante[…]" (TJ/MA, 2024, p. 10).

A decisão judicial também realizou a distinção entre o entendimento jurisprudencial acerca de vazamento de dados pessoais e o presente caso, que houve o tratamento de dados de natureza pessoal sensível (art. 5, Inciso II da LGPD), justificando a necessidade de comprovação de prejuízo no vazamento de dados de natureza apenas pessoal (art. 5, Inciso I da LGPD[32]) para gerar o dever de indenizar, ao contrário do caso dos autos.

No que tange à quantificação dos danos, o juiz fixou uma indenização por danos morais coletivos no valor de R$ 23 milhões, com base na gravidade da infração e na capacidade econômica da ré, com fins de destinação ao Fundo Estadual de Proteção e Defesa dos Direitos do Consumidor (FPDC), assegurando que os recursos revertam em benefício da coletividade.

Em relação aos danos morais individuais, a sentença estipulou o valor de R$ 500,00 para cada usuário diretamente afetado, condicionado à comprovação do uso do aplicativo até junho de 2021, quando a política de privacidade foi atualizada. O critério utilizado para a

[32]Art. 5º. Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; (Brasil, 2018).

fixação do valor individual considerou o caráter compensatório da indenização, proporcional ao dano sofrido, evitando o enriquecimento sem causa, mas garantindo a reparação mínima pelos prejuízos à dignidade dos consumidores.

### 2.3. Da (in)efetividade da LGPD na proteção e regulamentação dos poderes das *big techs*

A Lei Geral de Proteção de Dados, ante as evoluções tecnológicas, representou avanço legislativo no tocante à regulamentação de tratamento de dados, com a crescente necessidade de uma maior proteção e garantia da tutela dos direitos fundamentais conexos à atividade de tratamento de dados.

Em que pese a necessidade de uma regulamentação sobre o tratamento de dados, as premissas da confecção da norma foram carregadas de um viés colonialista e neoliberalista. Explica-se: com os escândalos da *Cambridge Anality*[33], a União Europeia se viu forçada a regulamentar a atividade de tratamento de dados em seu território, o que originou o Regulamento Geral de Proteção de Dados, documento que acabou legitimando o tratamento de dados pessoais e servindo de parâmetro global para o funcionamento dos serviços das empresas de tecnologia (Martins, 2023, p. 53).

Se justificando o caráter neoliberal e colonialista das atuais regulamentações, pela vedação do tratamento de dados de usuários europeus em países que não possuam proteção semelhante (UE, 2016, art. 44 e 45, 1) [34] e, considerando o interesse dos atores internacionais em manter relações econômicas com a União Europeia, os países e empresas devem, necessariamente, observar os ditames da RGPD para realizar o tratamento de dados dos usuários que tiveram seus dados coletados em jurisdição europeia (Martins, 2023, p. 28).

A padronização da regulamentação de dados, é atribuído ao fenômeno do *efeito Bruxelas,* que se traduz na uniformização regulatória em países que, muitas vezes, têm realidades completamente distintas, criando um verdadeiro cenário de colonialismo de dados,

[33]O escândalo da *Cambridge* Analytica envolveu a coleta massiva e não autorizada de dados de usuários do Facebook para influenciar eventos democráticos, como o Brexit em 2015 e as eleições presidenciais dos EUA em 2016. A empresa usou microtargeting para manipular o comportamento eleitoral, levantando sérias questões sobre privacidade e integridade democrática (Fornasier; Beck, 2020, p. 182-186).

[34]Artigo 45º. Transferências com base numa decisão de adequação 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica (UE, 2016).

porque, com intenções dar continuidade às relações econômicas internacionais, os países emergentes acabam se coadunando aos princípios e marcos regulamentares que não se amoldam especificamente à realidade nacional. (Martins, 2023, p. 30).

No tocante às *big techs,* se observa que essas passaram a adotar as disposições da RGPD em seus termos de uso e condições, à exemplo a "....Apple, em seu portal de privacidade, compromete-se com diversos padrões do RGPD, reproduzindo quase por completo o art. 6º da normativa no que diz respeito às hipóteses do tratamento de dados (APPLE, Privacy Policy, 2023)...."(Martins, 2023, p. 29).

Logo, o efeito bruxelas é perceptível nas regulamentações dos países e nos regulamentos internos das empresas, que, inclusive, realizam forte *lobby* para adoção de regulamentações semelhantes ao documento europeu (Martins, 2023, p. 29). Ademais, a necessidade da adoção de medidas regulamentares é fortemente revestida pelo interesse econômico dos países, como foi o caso do Brasil. Nesse sentido:

> "[…]é possível verificar a influência do Efeito Bruxelas, em ambos os seus aspectos, na adoção da CCPA estadunidense. Outros países desenvolvidos também passaram por processos semelhantes, como foi o caso do Japão, com a modificação do Act on the Protection of Personal Information (APPI), em 2021(….) Ademais, é possível atribuir a adoção de normas específicas sobre proteção de dados às demandas de ingresso na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), bloco econômico composto por diversos países ricos. A OCDE editou, ainda na década de 1980, as Diretivas sobre Proteção da Privacidade e Fluxo de Dados Transfronteiriços, e atualizou-as em 2013, de forma que recomendam que os países membros adotem legislações apropriadas, incluindo princípios como a limitação da coleta, qualidade dos dados, finalidade, entre outros. Trata-se de um grupo que o Brasil deseja aderir[…]"(Martins, 2023, p. 30).

O processo de elaboração da LGPD contou com forte participação do setor privado, os quais ressaltaram a necessidade de acompanhar o documento europeu, resultando na similaridade entre as normas. Conforme dito anteriormente, é de interesse comercial das *big techs* que haja um padrão global para a realização de tratamento de dados (Martins, 2023, p. 36).

No Brasil, conforme mencionado anteriormente, as Big Techs também exerceram forte lobby durante a elaboração da Lei Geral de Proteção de Dados (LGPD). O objetivo das empresas era alinhar a legislação brasileira às suas práticas globais, o que envolveu a inclusão de conceitos similares aos do RGPD, como a autodeterminação informativa e o consentimento para o tratamento de dados pessoais. No entanto, apesar das semelhanças com a legislação europeia, a LGPD mantém características alheias à realidade brasileira, refletindo tanto a

influência externa, quanto às pressões internas dos setores econômicos e tecnológicos. Esse processo evidencia como o Brasil, assim como outros países emergentes, foi influenciado pelas práticas regulatórias das *Big Techs*, que buscam padronizar as regras de proteção de dados para facilitar suas operações globais (Martins, 2023, p. 34-35).

Em um primeiro momento, parece interessante existir uma padronização de normas, diante do caráter universal da atuação das *big techs*, entretanto, a padronização não considera a hipossuficiência e a vulnerabilidade do titular de dados de um país emergente, criando uma assimetria informacional discrepante na relação entre o detentor dos dados e o titular dos dados (Martins, 2023. p. 41).

Segundo Martins (2023, p. 41), o consentimento informado é um requisito fundamental para a legitimidade do tratamento de dados, segundo o art. 5, inciso XII da Lei 13.709/18 (LGPD), porém, a autonomia privada é insuficiente para equilibrar o poder entre as partes envolvidas. Isso ocorre porque, de um lado, há multinacionais com vasto poder econômico e, do outro, os titulares de dados, muitas vezes em condição de vulnerabilidade, especialmente os residentes em países emergentes. Essa disparidade impede que o consentimento seja realmente livre e informado, tornando a relação entre as partes desproporcional.

Com efeito, existe uma assimetria de poder significativa na relação com os titulares de dados, especialmente em mercados digitais. Isso compromete a voluntariedade do consentimento, uma vez que os usuários são frequentemente forçados a aceitar os termos para acessar serviços essenciais (Costa et al., 2022, p. 14), motivo pela qual o *"*[...] consentimento mostra-se insuficiente na medida em que o titular não é nem mesmo capaz de compreender as tecnologias de coleta e como seus dados serão tratados […]"(Martins, 2023. p. 42).

A LGPD, embora represente um avanço em relação à proteção de dados no Brasil, é insuficiente para lidar com as peculiaridades dos países emergentes, onde a vulnerabilidade informacional dos usuários é mais acentuada. Nesse contexto, o Código de Defesa do Consumidor (CDC) assume papel ímpar na responsabilização das *big techs,* porque supre a provável inefetividade da norma quando aplicada afastada da legislação consumerista, uma vez que o CDC atrai para o usuário as proteções decorrentes da relação de consumo, logo essa normativa também é relevante, nas relações de consumo criado no ambiente digital. À exemplo, o CDC estabelece o direito à informação clara e adequada, o que é essencial para garantir que os usuários compreendam os termos de uso e as políticas de privacidade (Martins, 2023, p. 44).

No entanto, conforme Martins (2023, p. 41), apesar da LGPD adotar princípios como a autodeterminação informativa, que é fundamental, mas não garante um consentimento

realmente livre e informado, especialmente em um contexto onde os usuários frequentemente aceitam termos extensos e complexos por necessidade ao acesso dos serviços digitais (Martins, 2023, p. 41).

As grandes empresas de tecnologia, ao exercerem sua atuação global no tratamento de dados, precisam respeitar não apenas a legislação de proteção de dados, como a LGPD, mas também aos princípios mais amplos de ordem econômica e social, o que se traduz em uma espécie de função social das *big techs*.

A referida função social deve ser entendida como uma obrigação dessas empresas em contribuir para o bem comum, além de gerar lucro, de forma que o cumprimento da função social exige o incentivo ao desenvolvimento da tecnologia nacional, bem como da proteção de dados, promovendo justiça econômica e social no contexto digital (Martins, 2023, p. 48 - 49).

O atendimento da função social das *big techs* implicaria na redução do desequilíbrio entre as partes envolvidas, porque a atividade dessas grandes empresas acabam por beneficiar desigualmente o tratador de dados, inexistindo mecanismos de reversão dos benefícios obtidos em prol da população (Martins, 2023, p. 50-52)

Diante desse contexto, (i) impedir que as empresas interfiram negativamente na infraestrutura estatal, (ii) garantir que o tratamento de dados seja realizado localmente, ou exista sede da empresa no território do país e a (iii) instituição de taxa sobre a exploração de dados, a fim de reverter em proveito das necessidades da população, são medidas capazes de reduzir a dimensão da assimetria entre as partes envolvidas no tratamento de dados (Martins, 2023, p. 47-53).

À luz do exposto, conclui-se que o *modus operandi* das *Big Techs*, ao conferir-lhes vantagens desproporcionais frente aos seus usuários-consumidores, evidencia uma assimetria de poder que transcende a mera relação contratual, demandando uma reinterpretação da função social dessas corporações no contexto do tratamento de dados pessoais. Tal cenário impõe a necessidade de uma aplicação articulada entre a Lei Geral de Proteção de Dados (LGPD) e o Código de Defesa do Consumidor (CDC), este último reconhecendo a relação consumerista e oferecendo subsídios para a responsabilização objetiva das empresas em casos de violação. A integração normativa entre esses diplomas não apenas supre eventual desequilíbrio, mas também encontra respaldo nos recentes entendimentos dos Juízes de Direito de jurisdições diversas do Brasil, os quais vêm reafirmando a importância da responsabilização das *Big Techs* como meio de equilibrar a relação jurídica entre as partes e assegurar a proteção dos direitos

fundamentais à privacidade e à dignidade da pessoa humana, promovendo um ambiente digital mais equitativo e ético.

Ante o exposto, conforme discutido ao longo deste capítulo, a Lei Geral de Proteção de Dados (LGPD) surgiu como um marco regulatório fundamental da proteção dos dados pessoais no Brasil. A legislação impõe uma série de obrigações às atividades que envolvam tratamento de dados, especialmente no que se refere aos princípios de finalidade, necessidade, transparência e segurança, medidas que visam garantir a autodeterminação informativa do titular, assegurando que seus dados sejam coletados e tratados com seu consentimento explícito e dentro de limites claramente definidos.

Dos casos analisados, se percebe que a responsabilidade das *Big Techs* é geralmente tratada sob o regime de responsabilidade objetiva, principalmente em virtude da existência de uma relação de consumo com os usuários. Assim, conforme previsto no art. 14 do Código de Defesa do Consumidor (CDC), o fornecedor de serviços responde, independentemente de culpa, pelos danos causados ao consumidor. Essa abordagem foi reiterada nas decisões judiciais analisadas, reconhecendo que o mero descumprimento das obrigações legais na coleta e tratamento de dados constitui falha na prestação de serviço, ensejando reparação.

Entretanto, conforme discutido no item 2.3 do capítulo, a aplicação da LGPD esbarra em ineficiências práticas que comprometem sua eficácia, porque, embora a Lei brasileira adote padrões internacionais, como os delineados pelo Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, ela não considera plenamente a realidade socioeconômica brasileira, uma vez que há, inegavelmente, um desequilíbrio informacional entre as *Big Techs* e os titulares de dados.

Dessa forma, o consentimento meramente formal, por meio de adesão dos termos de usos, é insuficiente para garantir a ciência inequívoca e a proteção efetiva dos dados.

Não obstante, a doutrina ainda diverge quanto à natureza da responsabilização. Enquanto alguns autores defendem que a LGPD introduz elementos da responsabilidade subjetiva, como o dever de prestação de contas e a análise de culpa, outros argumentam que a aplicação do CDC solidifica a responsabilidade objetiva, em razão da hipossuficiência do titular dos dados. Nesse sentido, a LGPD, ao lado do CDC, compõe um arcabouço normativo robusto, mas sua efetividade depende da implementação prática e da capacidade de fiscalização.

Por fim, os valores de condenação em casos de danos coletivos e individuais demonstram uma tentativa de alcançar reparação e desincentivar práticas negligentes. No entanto, como apontado, esses montantes ainda são relativamente modestos frente à capacidade

financeira das grandes corporações. Assim, o desafio reside em fortalecer mecanismos que garantam não apenas a compensação adequada, mas também o caráter dissuasivo das penalidades impostas.

## III - DAS REGULAÇÕES SOBRE TRATAMENTO DE DADOS NO DIREITO INTERNACIONAL E A RESPONSABILIZAÇÃO DOS INFRATORES

Com diversas inovações tecnológicas que, pelo teor da sua funcionalidade, envolvem direitos irrenunciáveis, mormente atinentes à personalidade do indivíduo, o direito também inovou em relação aos direitos fundamentais. À exemplo, a Lei Geral de Proteção de Dados e a constitucionalização da proteção de dados no ordenamento jurídico brasileiro, trouxeram novos panoramas ao contexto da sociedade brasileira.

Nessa linha, torna-se necessário analisar as principais normas e regulações, bem como precedentes relevantes no direito internacional, a fim de compreender como o tema já foi e vem sendo tratado no cenário global.

### 3.1. Das regulações a partir do direito comparado:

Primeiramente, cabe elencar os principais comandos normativos, a partir do direito comparado, que refletem ou regulam os direitos fundamentais conexos ao tratamento de dados.

Nesse sentido, antes da implementação do novo Regulamento Geral de Proteção de Dados - Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril - RGPD, era aplicada **a Diretiva 95/46/CE de 1995,** aprovada quando a *Internet* ainda estava a dar os seus primeiros passos (Carvalho, Restier, 2020, p. 171) e tinha como objetivo "[…]garantir a livre circulação de dados pessoais entre os Estados-Membros e proteger as liberdades e direitos fundamentais das pessoas singulares (naturais)[…]"(Araújo, 2017, p. 205).

Sua aplicação se deu até 25 de maio de 2018, após, foi substituída pelo novo Regulamento Europeu. Entretanto, apesar da mudança, os princípios e objetivos norteadores da Diretiva foram mantidos na regulação sucessora. A necessidade de uma regulamentação nova, decorreu das significativas mudanças no âmbito tecnológico, tais como a intensificação da transferência de dados a outros países, que é inerente ao contexto de globalização em que vivemos. (Araújo, 2017, p. 206).

Da leitura da antiga Diretiva, se observa a preocupação na qualidade dos dados, porquanto devem ser obtidos de forma lícita e pautada na boa-fé. Ainda, se destaca a instituição dos princípios da finalidade coadunados com as legítimas expectativas acerca do âmbito do tratamento de dados do titular (UE, 1995).

Além disso, previa direitos relativos à prestação de contas, incluindo o direito de acesso às informações (artigo 12), esclarecimentos sobre a utilização de dados pessoais (artigo 10), bem como o direito de se opor ao tratamento de dados (artigo 14) (UE, 1995)

Também, destaca-se que a recomendação já previa restrições de transferências a países terceiros que não asseguravam um nível de segurança similar ao garantido pela Diretiva 95/46, ressalvando que, através de um mecanismo contratual, se podia relativizar a regra e possibilitar a transferência de dados mediante compromisso *inter partes*, com regras contratuais vinculativas (UE, 1995).

Um dos efeitos da transposição de Diretiva (95/46) para regulamentação (RGPD), é a implicação de uma maior aplicabilidade nos Estados membros da União Europeia, porque, enquanto detinha natureza de Diretiva, dependia da anuência específica do Estado membro. Acabando limitando a obrigatoriedade do cumprimento e aplicabilidade da Diretiva (Araújo, 2017, p. 206).

Também, se destaca a influência dos princípios da Convenção Europeia de Direitos Humanos (CEDH), bem como dos Princípios de "Práticas Justas de Informação" *(Fair Information Practice Principles*), formulados após o escândalo Watergate[35], na alma da Diretiva, isto porque à época, se cultivava preocupação e receio futuro com os avanços tecnológicos que vinham surgindo, os quais, de alguma forma, relacionava-se com direitos fundamentais (Hustinx, 2021, p. 78).

Dessa forma, a referida Diretiva serviu como orientação para a proteção e regulamentação do direito à proteção de dados pessoais, que também, posteriormente, foi protegido na Carta dos Direitos Fundamentais da União Europeia.

A referida Carta de Direitos Fundamentais da União Europeia foi adotada em 2000 e integrada ao Tratado de Lisboa em 2009. Ela reforça a proteção de dados pessoais como um direito fundamental autônomo para os cidadãos europeus (Sarlet, 2020, p. 183).

[35]O escândalo Watergate envolveu a invasão da sede do Partido Democrata, em 1972, orquestrada pelo Comitê para a Reeleição do Presidente Richard Nixon. Essa operação de espionagem, financiada ilegalmente, foi seguida por tentativas de encobrimento por Nixon, incluindo ordens ao FBI para interromper as investigações. O caso, amplamente exposto pela imprensa e marcado pela violação da privacidade dos adversários políticos, levou à renúncia de Nixon e gerou reformas na legislação sobre transparência e financiamento de campanhas (Sampaio, 2024).

O artigo 8º[36] garante que os dados pessoais devem ser tratados de maneira justa e segura, exclusivamente para finalidades legais e com o consentimento do titular, ou com base em outra justificativa legítima (UE, 2000).

A Carta Europeia é um importante comando normativo em âmbito europeu, porquanto reforça *"*[…] a proteção dos direitos fundamentais, à luz da evolução da sociedade, do progresso social e da evolução científica e tecnológica[…]*"* (UE, 2000), assim, se denota forte presença da norma nas fundamentações dos casos internacionais em que há coalizão de preceitos fundamentais positivados ou decorrentes destes.

Com diversos avanços tecnológicos e o surgimento de novos serviços personalizados com base em informações do usuário, o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, implementado em 2018, sucessora da referida Diretiva 95/46, reforça e atualiza a proteção de dados pessoais do cenário europeu.

A norma estabelece um arcabouço jurídico tangível de regras, visando regulamentar o tratamento de dados pessoais em âmbito europeu. O quadro legal objetiva não apenas a proteção da privacidade, mas também a promoção da transparência e do controle sobre o uso de informações pessoais (autodeterminação informativa).

Com relação aos princípios do RGPD, pode-se argumentar que estes têm origem nos *Fair Information Practice Principles*, desenvolvidos desde a década de 1970 nas primeiras legislações de proteção de dados. O regulamento europeu adota princípios fundamentais, como a necessidade, requerendo que o tratamento de dados seja limitado ao essencial para os fins propostos; a licitude, assegurando que o tratamento ocorra de maneira justa e dentro dos limites legais; e a proporcionalidade, que exige que as ações de tratamento estejam adequadamente equilibradas em relação aos objetivos informados. Além disso, destaca-se a transparência, que reforça a obrigação de comunicação clara e acessível ao titular dos dados, e a finalidade, que estabelece que o uso dos dados deve ser restrito às finalidades específicas e explícitas informadas no momento da coleta (Martins, 2023, p. 33-34).

Tais princípios objetivam garantir um tratamento de dados adequado e pautado no respeito aos direitos dos titulares. Também visa assegurar o cumprimento das normas de

[36]Artigo 8. o Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. [...] (UE, 2000)

proteção por meio de criação de agências especializadas, que são os entes competentes para fiscalização do tratamento de dados.

O conjunto principiológico procura estabelecer certo grau de ética no processo de coleta de informações, determinando que a coleta deve ocorrer com uma comunicação clara e compreensível sobre a utilização dos dados. Incluindo descrição explícita da finalidade do tratamento, bem como a base legal em que se fundamenta, além dos possíveis riscos envolvidos. (Carvalho e Restier, 2020, p. 175).

O princípio da transparência também se materializa na obrigatoriedade das empresas em divulgar de forma completa e precisa as políticas de privacidade, incluindo detalhes sobre a coleta de dados, o tempo de armazenamento e as medidas de segurança aplicadas para proteção das informações pessoais. A implementação efetiva deste princípio é crucial para a construção de uma cultura de proteção de dados que seja ética e robusta, assegurando que os titulares tenham controle pleno sobre suas informações pessoais (Martins, 2023, p. 29).

Também, vale destacar, o princípio da limitação da finalidade, que determina que os dados pessoais devem ser coletados para fins específicos, explícitos e legítimos, não podendo ser tratados posteriormente de maneira incompatível com essas finalidades iniciais (Carvalho e Restier, 2020, p. 173).

A minimização dos dados é outro pilar do RGPD. De acordo com este princípio, as informações coletadas devem ser adequadas, relevantes e limitadas ao necessário para os propósitos para os quais são processadas. Sua aplicação é fundamental para reduzir riscos de violação de dados, uma vez que limita a quantidade de informações coletadas ao essencial, evitando excessos e garantindo maior proteção ao titular Carvalho e Restier, 2020, p. 173).

O princípio da exatidão também é destacado no RGPD, que exige que os dados sejam mantidos corretos e atualizados, permitindo ao titular solicitar a retificação ou exclusão de dados incorretos. Esse princípio é essencial para garantir que as decisões tomadas com base nos dados pessoais sejam justas e precisas. (Carvalho e Restier, 2020, p. 174).

Dessa forma, o RGPD estabelece um novo padrão de proteção de dados, promovendo não apenas a segurança das informações pessoais, mas também incentivando uma cultura de responsabilidade e transparência nas organizações que lidam com dados. Esses princípios servem como base para a regulação e proteção de dados em outros países, como o Brasil, que adotou a Lei Geral de Proteção de Dados (LGPD), inspirada em grande parte nas diretrizes europeias (Martins, 2023, p. 29) e acrescentou elementos como o livre acesso, segurança,

prevenção e não discriminação, ampliando alguns dos princípios originais do regulamento europeu (Martins, 2023, p. 34).

Mais recentemente, aprovado pela União Europeia em 2022, ante a preocupação em equilibrar a assimetria informacional no tratamento de dados das *big techs* em relação aos usuários, surge o Digital Services Act (DSA), que foi inspirado pelos princípios e disposições contidas no GDPR, a norma visa estabelecer uma estrutura de responsabilização das plataformas digitais, com foco particular nas grandes empresas de tecnologia que operam na União Europeia (AMNESTY INTERNATIONAL, 2022, p. 01).

O DSA impõe requisitos rigorosos para que as chamadas *Very Large Online Platforms* (VLOPs) realizem avaliações anuais de risco sobre os impactos dos seus sistemas, inclusive algoritmos de recomendação e sistemas de publicidade. Essa análise deve identificar riscos à privacidade, à liberdade de expressão e ao direito à não discriminação, considerando como o design da plataforma e o uso de algoritmos podem amplificar conteúdos prejudiciais, como desinformação e discurso de ódio (AMNESTY INTERNATIONAL, 2022, p. 02).

Entre as principais obrigações do DSA estão as medidas de mitigação de riscos. As plataformas precisam adotar ações proporcionais e eficazes para mitigar os riscos identificados nas avaliações anuais, o que inclui ajustar a forma como conteúdo e publicidade são exibidos aos usuários. O DSA exige, por exemplo, que algoritmos de recomendação sejam ajustados para evitar a amplificação de conteúdo prejudicial, além de proibir anúncios direcionados com base em dados sensíveis, como religião e orientação sexual, em conformidade com o GDPR (EUROPEAN COMMISSION, 2024).

Para promover a transparência, o DSA requer que as grandes plataformas publiquem auditorias independentes anuais e tornem públicas as avaliações de risco e as medidas de mitigação aplicadas. No entanto, algumas informações podem ser omitidas por questões de segurança ou segredos comerciais, o que gera preocupação sobre a possibilidade de limitações na transparência. Essas medidas são vistas como essenciais para garantir que as plataformas sejam responsabilizadas por práticas que possam afetar os direitos dos usuários (AMNESTY INTERNATIONAL, 2022, p. 04).

Por fim, o DSA estabelece um sistema de sanções, com multas de até 6% do faturamento global anual da plataforma infratora, e supervisão pela Comissão Europeia, que coordena a fiscalização junto às autoridades nacionais. A estrutura concentrada de fiscalização objetiva evitar a escolha de jurisdições mais permissivas e assegurar uma aplicação consistente das

regras em toda a União Europeia, promovendo um ambiente digital mais justo e seguro (AMNESTY INTERNATIONAL, 2022, p. 07).

Na América do Norte, a lei federal Americana "*Privacy Act",* promulgada em 1974, é apontada como um importante marco da proteção à privacidade, estabelecendo base para um direito geral da privacidade (Passos 2017, p. 72).

Um dos pontos centrais da lei, é o "[...] reconhecimento de que a privacidade de um indivíduo é diretamente afetada pela coleta, manutenção, uso e disseminação das informações pessoais por parte das agências federais[…]" (Passos, 2017, p. 73), de modo a considerar os desafios impostos pelos avanços tecnológicos da época.

Dessa forma, embora a aplicabilidade da lei seja restrita às agência do governo, o instrumento se demonstra eficaz para garantir aos cidadãos o direito de acesso aos seus próprios "[...] dados pessoais armazenados em agências governamentais, bem como à garantia de retificação daqueles equivocados e, por fim, ao estabelecimento de regras definidas e circunstanciais para a divulgação destas informações pelo governo[...]" (Passos, 2017, p. 74).

Ainda no âmbito da América do Norte, se teve a recente edição da *California Consumer Privacy Act (*CCPA) e da *California Privacy Rights Act* (CPRA), que se tratam de leis estaduais do Estado da Califórnia nos Estados Unidos.

O California Consumer Privacy Act (CCPA) foi implementado em janeiro de 2020, é visto como uma legislação abrangente, frequentemente chamada de "GDPR da Califórnia", enquanto o California Privacy Rights Act (CPRA) foi aprovado em novembro de 2020 e expande o CCPA, introduzindo novos direitos para os consumidores e responsabilidades para as empresas (LAW BUSINESS RESEARCH LTD., 2021, p. 465).

A atualização legislativa introduziu novos direitos e aumentou as proteções ao consumidor. Entre as principais mudanças, o CPRA implementou o direito à correção de dados, a limitação do uso de informações para publicidade comportamental e o fortalecimento dos direitos de consentimento para menores. Além disso, exige que as empresas firmem contratos específicos com prestadores de serviços para proteger os dados pessoais compartilhados.(LAW BUSINESS RESEARCH LTD., 2021, p. 463).

Um dos avanços mais relevantes do CPRA é a criação da California Privacy Protection Agency (CPPA), a primeira agência de proteção de dados dos EUA, responsável por monitorar e regulamentar a aplicação dessas leis. Esse movimento coloca a Califórnia na vanguarda da privacidade de dados nos EUA e serve como modelo para outras jurisdições, estimulando a

discussão sobre uma possível legislação federal de proteção de dados (LAW BUSINESS RESEARCH LTD., 2021, p. 464 - 465).

## 3.2 PRECEDENTES INTERNACIONAIS

Assim, tendo em vista as principais regulações e complementos normativos que abarcam o tema "tratamento de dados" no cenário internacional, também é prudente analisar os precedentes estrangeiros envolvendo a responsabilização das *big techs:*

### 3.2.1. *Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos e Mario Costeja González (2014)*:

Trata-se de decisão do Tribunal de Justiça da União Europeia, publicada no ano de 2014, versando sobre pedido de remoção de links nos resultados de pesquisa do Google que relacionavam um cidadão espanhol a um anúncio de penhora de imóveis oriundo de uma dívida pretérita e já resolvida.

O referido caso é um dos primeiros registros de responsabilização e regulação de tratamento de dados pessoais. Destaca-se que referido entendimento ocorreu anteriormente à edição da RGPD, mas mesmo assim, àquela época já se delineava os preceitos hoje existentes acerca da legítima finalidade no tratamento de dados pessoais. Nesse sentido, nos termos da decisão europeia:

> "[...]ao responsável pelo tratamento assegurar que os dados pessoais sejam objeto de um tratamento leal e lícito, sejam recolhidos para finalidades determinadas, explícitas e legítimas e não sejam posteriormente tratados de forma incompatível com essas finalidades», sejam adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente», sejam exatos e, se necessário, atualizados» e, por último, sejam conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente[...]"(UE, p.17)

O trecho da decisão se refere ao teor do artigo 6, b) da Diretiva 95/46[37], que remonta a necessidade de uma finalidade legítima e determinada para a coleta de dados pessoais,

[37]Artigo 6. o da Diretiva 95/46, inserido no seu capítulo II, secção I, intitulada Princípios relativos à qualidade dos dados, tem a seguinte redação:(...) b) Recolhidos para finalidades determinadas, explícitas e legítimas e não ser

princípios que foram positivados no texto da RGPD  e LGPD e, atualmente, constitui, indubitavelmente, premissas norteadoras do tratamento de dados pessoais.

Adiante, *in casu*, o Tribunal europeu entendeu que o Google não é meramente um intermediário passivo. Mesmo que não crie ou altere os conteúdos das páginas web de terceiros, o Google desempenha um papel ativo na organização, apresentação, armazenamento e acesso aos dados pessoais, por meio dos resultados de busca, entendo assim que a atividade praticada pela Google se classifica, de fato, como tratamento de dados pessoais, definidos nos artigos 2(b) e 2(d) da Diretiva 95/46/CE[38], o que enseja na sua responsabilização quando utilizado em descompasso a uma finalidade legítima (*Google Inc. v Mario Costeja González, 2014, p. 22*).

Logo, se verifica que antes de existir regulamentação específica nesse âmbito, já se desenvolvia nas ciências jurídicas ideais de responsabilização dessas grandes companhias que se valiam do tratamento de dados pessoais para a efetividade dos serviços oferecidos.

### 3.2.2. G 264/2015

Trata-se de decisão exarada pelo Tribunal Constitucional da Áustria, versando sobre caso, no qual um médico se opôs à divulgação de avaliações sobre seu atendimento, em determinado site, fundamentando a obrigatoriedade da retirada do conteúdo com base na legislação nacional, que apregoava como direito absoluto a objeção em lides envolvendo dados pessoais (G 264/2015).

O Tribunal reconheceu o conflito entre a norma nacional e o artigo 10 da Convenção Europeia dos Direitos do Homem[39], porque o direito absoluto à vedação não encontrava

---

posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-Membros estabeleçam garantias adequadas;(UE, 1995)

[38]Artigo 2.o da Diretiva 95/46 dispõe que, para efeitos da mesma, entende-se por: a) 'Dados pessoais', qualquer informação relativa a uma pessoa singular identificada ou identificável ('pessoa em causa'); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social; b) 'Tratamento de dados pessoais' ('tratamento'), qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição [...] (UE, 1995)

[39]Artigo 10 Liberdade de expressão 1. Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber ou de transmitir informações ou ideias sem que possa haver ingerência de quaisquer autoridades públicas e sem considerações de fronteiras. O presente artigo não impede que os Estados submetam as empresas de radiodifusão, de cinematografia ou de televisão a um regime de autorização prévia. 2. O exercício desta liberdades, porquanto implica deveres e responsabilidades, pode ser

pacificação com os preceitos da liberdade de expressão e os balizadores do interesse público, os quais, segundo o Tribunal Constitucional, devem ser considerados no caso concreto. Tal entendimento ensejou na declaração de inconstitucionalidade de um artigo da lei nacional (G 264/2015).

No caso mencionado, se percebe que a Corte entendeu pela abusividade de um direito absoluto à vedação de exposição de dados pessoais, sem considerar direitos reflexos, como o interesse público oriundo de um viés de liberdade informativa. Também, se pode afirmar que a mencionada Corte limitou a autodeterminação informativa absoluta, considerando o choque com o interesse público, que detinha o legítimo interesse na exposição daqueles dados, ainda que pessoais e atinentes à personalidade de alguém.

### 3.2.3. Gonzalez v. Google LLC

A Suprema Corte dos Estados Unidos, em 2023, decidiu sobre o caso Gonzalez v. Google LLC, que versa acerca da possibilidade do Google (proprietário do YouTube) ser responsabilizado por supostamente facilitar o uso de sua plataforma por membros do ISIS para disseminar propaganda e realizar recrutamento (Suprema Corte dos Estados Unidos, 2023).

Os demandantes argumentaram que o Google forneceu assistência material ao ISIS ao permitir que a organização utilizasse a plataforma YouTube para promoção de suas atividades terroristas, violando assim o Anti-Terrorism Act (ATA). Eles também alegaram que a receita publicitária gerada por vídeos do ISIS representava um apoio financeiro ao grupo terrorista (Suprema Corte dos Estados Unidos, 2023).

A Corte concluiu que as alegações dos demandantes falharam em estabelecer uma base para responsabilização tanto direta quanto secundária sob o ATA. Além disso, a aplicação da Seção 230 do Communications Decency Act (CDA) impediu a responsabilização do Google, uma vez que a empresa não poderia ser tratada como "publicadora" do conteúdo gerado por terceiros, neste caso, o ISIS (Suprema Corte dos Estados Unidos, 2023).

submetido a certas formalidades, condições, restrições ou sanções, previstas pela lei, que constituam providências necessárias, numa sociedade democrática, para a segurança nacional, a integridade territorial ou a segurança pública, a defesa da ordem e a prevenção do crime, a protecção da saúde ou da moral, a protecção da honra ou dos direitos de outrem, para impedir a divulgação de informações confidenciais, ou para garantir a autoridade e a imparcialidade do poder judicial (CEDH, 1950).

Embora a referida decisão não verse especificamente acerca de dados pessoais, a questão de fundo do litígio, é referente ao algoritmo direcionado da empresa, o qual foi devidamente arguido pela parte autora, *vide:*

> "[..] As únicas exceções foram as alegações dos autores de responsabilidade direta e secundária, baseadas nas acusações de que o Google aprovou vídeos do ISIS para publicidade e, em seguida, compartilhou os lucros com o ISIS por meio do sistema de compartilhamento de receita do YouTube…."(Gonzalez v. Google LLC, 2023, p. 02. )(tradução nossa)

No caso, a Corte afastou a responsabilidade, entendendo que o algoritmo é um serviço neutro e inerente da plataforma, não tendo liame causal com as atividades da entidade terrorista, com respaldo na citada Seção 230 da Communications Decency Act (CDA).

### 3.2.4. C-645/19

A decisão do Tribunal de Justiça da União Europeia (TJUE), no caso C-645/19, traz um aprofundamento relevante sobre a aplicação do Regulamento Geral de Proteção de Dados (RGPD) em cenários de tratamento transfronteiriço de dados pessoais. No caso em questão, a Autoridade de Proteção de Dados da Bélgica (*Gegevensbeschermingsautoritei*t) processou o Facebook, alegando a coleta indevida de dados de navegação, incluindo de usuários não cadastrados, por meio de *cookies e plugins sociais,* sem o devido consentimento informado, em violação aos princípios de transparência e legalidade estabelecidos nos artigos 5º e 6º do RGPD[40] (TJUE, 2021), *in verbis:*

[40]Artigo 5.º: Princípios relativos ao tratamento de dados pessoais Os dados pessoais devem ser: a) Tratados de forma lícita, leal e transparente em relação ao titular dos dados (licitude, lealdade e transparência); b) Recolhidos para finalidades determinadas, explícitas e legítimas e não ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos não é considerado incompatível com as finalidades iniciais (limitação das finalidades); c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização dos dados); d) Exatos e, se necessário, atualizados; devem ser tomadas todas as medidas razoáveis para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora (exatidão); e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados por períodos mais longos, na medida em que serão tratados exclusivamente para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, sujeitos à aplicação das medidas técnicas e organizativas adequadas previstas no presente regulamento, a fim de garantir os direitos e liberdades do titular dos dados (limitação da conservação); f) Tratados de uma forma que garanta a segurança adequada dos dados pessoais, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando-se as medidas técnicas ou organizativas adequadas (integridade e confidencialidade). O responsável pelo tratamento é responsável pelo cumprimento do disposto no número anterior e deve ser capaz de o demonstrar (responsabilização). (UE, 2016) Artigo 6.º: Licitude do tratamento O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

> "[…]Quanto ao mérito, esse órgão jurisdicional declarou que a rede social em causa não informava de forma suficiente os internautas belgas sobre a recolha das informações em causa e sobre a utilização destas informações. Por outro lado, o consentimento dado pelos internautas à recolha e ao tratamento das referidas informações foi julgado inválido. Por conseguinte, o Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunal de Primeira Instância de Língua Neerlandesa de Bruxelas) ordenou que a Facebook Ireland, a Facebook Inc. e a Facebook Belgium, primeiro, relativamente a qualquer internauta estabelecido no território belga, deixassem de colocar, sem o seu consentimento, cookies que permanecem ativos durante dois anos no dispositivo que o internauta utiliza quando navega numa página da Internet que tenha o nome de domínio Facebook.com ou quando é direcionado para o sítio Internet de um terceiro, bem como de colocar cookies e recolher dados através de módulos sociais, píxeis ou meios tecnológicos semelhantes em sítios Internet de terceiros, de forma excessiva atendendo aos objetivos assim prosseguidos pela rede social Facebook, segundo, deixassem de fornecer informações que podem razoavelmente induzir em erro as pessoas em causa quanto ao alcance real dos mecanismos disponibilizados por esta rede social para a utilização de cookies e, terceiro, destruíssem todos os dados pessoais obtidos através de cookies e de módulos sociais"(UE, 2021, item 32).

Em que pese a questão prejudicial do feito ter centralizado a discussão na controvérsia da competência transfronteiriça para de tratamento de dados, que em âmbito europeu é regulada pelo mecanismo de "balcão único" previsto nos artigos 56º e 60º do RGPD, essa decisão ajuda na compreensão de como os direitos fundamentais vem sendo entendidos pelas Cortes europeias.

No presente caso, a autoridade de controle principal seria a Comissão de Proteção de Dados da Irlanda, uma vez que a sede europeia da empresa está localizada nesse país. Apesar disso, o TJUE destacou que, embora o mecanismo de "balcão único" estabeleça a competência primária da autoridade de controle principal, ele não elimina completamente a possibilidade de intervenção de autoridades locais em determinadas situações urgentes. O Tribunal apontou que a aplicação do RGPD exige cooperação leal e eficaz entre as autoridades de controle envolvidas (TJUE, 2021). Assim, as autoridades nacionais podem intervir em situações de urgência ou quando o tratamento impacta significativamente os titulares de dados em um único Estado-Membro.

---

a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para proteger interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular dos dados que exigem a proteção dos dados pessoais, especialmente se o titular dos dados for uma criança.(UE, 2016)

Dessa forma, o Tribunal fundamentou sua decisão nos artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia, que protegem o direito à privacidade e à proteção de dados pessoais, além do artigo 47º, que assegura o direito a um recurso judicial efetivo (TJUE, 2021). Assim, a interpretação garante certa uniformização das regras de proteção de dados, bem como elimina obstáculos à livre circulação de dados pessoais no mercado interno europeu.

### 3.2.5. C-300/21

O caso C-300/21, UI v. *Österreichische Post AG,* originou-se pelo processamento de dados pessoais sem o devido consentimento. A Österreichische Post, mediante uso de algoritmos, inferiu preferências políticas de seus clientes com base em dados demográficos, presumindo a filiação a partidos políticos e aplicando esses dados em campanhas de publicidade direcionada.

O cidadão, que, movido por sentimentos de violação, entendeu que a atribuição a uma posição política, sem sua autorização, era ofensiva, configurando um dano emocional, visando compensar o que descreveu como um dano não material, se traduzindo no desconforto interno e o impacto potencial à sua reputação. No entanto, o tribunal austríaco rejeitou a demanda, considerando que o direito à compensação por danos não materiais exigia que o dano fosse mais do que um simples sentimento de desconforto.

O Supremo Tribunal da Áustria, buscando esclarecimento sobre o escopo do Artigo 82 do GDPR[41], questionou o Tribunal de Justiça da União Europeia (TJUE) sobre se uma violação do GDPR, sem um dano material concreto, poderia justificar o direito à compensação, e se o sentimento subjetivo de desconforto poderia ser considerado um dano não material compensável.

[41]Artigo 82**.** Direito à indenização e responsabilidade 1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais em razão de uma violação deste regulamento terá o direito de receber uma indenização do responsável pelo tratamento ou do operador pelos danos sofridos. 2. Qualquer responsável pelo tratamento envolvido no tratamento será responsável pelos danos causados pelo tratamento que violem este regulamento. Um operador será responsável pelos danos causados pelo tratamento apenas quando não tiver cumprido as obrigações deste regulamento especificamente direcionadas a operadores ou quando tiver agido fora ou em contrário às instruções legais do responsável pelo tratamento. 3. Um responsável pelo tratamento ou operador será isento de responsabilidade ao abrigo do parágrafo 2 se provar que não é, de forma alguma, responsável pelo evento que deu origem aos danos.. [...] (UE, 2016).

Em 4 de maio de 2023, o tribunal decidiu que a simples violação das disposições do GDPR, por si só, não confere automaticamente ao titular dos dados o direito à compensação. Para que esse direito seja garantido, o dano deve existir e estar relacionado com a violação (UE, 2023).

Um ponto crucial abordado pelo TJUE foi a natureza do dano não material. Porque, ao contrário do que havia sido sugerido pelo Advogado-Geral, o direito à compensação por danos não materiais não exige "elevado nível de gravidade" para que o dano seja compensável. Em outras palavras, o GDPR não impõe um nível mínimo de gravidade para danos não materiais, sendo suficiente demonstrar que houve um dano direto e concreto ao titular dos dados (UE, 2023).

Outro aspecto relevante da decisão, conforme destacado por Burri e Nickl (2023), é a autonomia dos Estados-Membros na definição dos critérios para a avaliação do valor da compensação. O GDPR não apresenta regras específicas para o cálculo dos danos, deixando que os Estados-Membros regulamentem essas questões internamente, desde que respeitem os princípios de equivalência e efetividade do direito da UE. Esse posicionamento visa garantir que os titulares de dados recebam compensações "plenas e efetivas" pelos danos sofridos, sem, no entanto, incluir compensações punitivas, o que preserva o caráter compensatório do GDPR. (Perfect Law, 2023).

A decisão em análise é pertinente, pois cria parâmetros para o direito à compensação oriundo da violação dos preceitos da RGPD. No presente caso, entendeu-se que o direito à indenização não é automático, porque é necessário a comprovação de um dano específico ao titular. Isso coloca uma ênfase maior na relação causal entre a infração e o dano (UE, 2023).

Por fim, se conclui que a referida decisão reconheceu que o direito à indenização não é *in re ipsa*, porquanto fixa a presença de alguns requisitos para originar o direito à que remonta ao art. 82 da RGPD, tais como: a existência (i) de violação do regulamento, (ii) um dano (material ou não material) e (iii) uma relação causal entre a violação e o dano sofrido, entretanto, repassa aos Tribunais nacionais a análise acerca de eventual liquidação sobre a extensão do dano não material ocasionado.

### 3.3. Comparação dos entendimentos internacionais com o cenário brasileiro.

A proteção de dados pessoais no Brasil, delineada pela LGPD, inspira-se diretamente nos princípios europeus estabelecidos pela Diretiva 95/46/CE e pelo Regulamento Geral de

Proteção de Dados (RGPD), destacando a finalidade específica e legítima no tratamento de dados. Nesse sentido, os julgados da região europeia, preconizam que o tratamento de dados respeite as finalidades legítimas e observe os preceitos da lealdade e licitude, de forma a resguardar a proteção dos direitos fundamentais da personalidade.

Na medida em que os Estados Unidos se utilizam de uma perspectiva mais alinhada à autonomia privada e à liberdade de mercado. Isto porque, a Suprema Corte considera os algoritmos das plataformas como sistemas neutros, eximindo as empresas de responsabilidade pelo conteúdo gerado por terceiros, mesmo sob efeito da sistemática dos algoritmos, de forma a seguir a literalidade da *Seção 230 do Communications Decency Act*. A interpretação Americana permite que as empresas operem sem o peso de sanções significativas, mesmo em casos de disseminação de conteúdos prejudiciais, contrastando com o modelo europeu, que considera a irregularidade no tratamento de dados, porém exige a comprovação de dano efetivo para responsabilização.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) tenta equilibrar esses modelos, integrando princípios de proteção de dados inspirados no RGPD. À exemplo, nos julgamentos brasileiros, a atração das normas consumeristas, reforçam a responsabilização direta das plataformas pela coleta e tratamento de dados sem o consentimento adequado. No entanto, as sanções aplicadas ainda carecem de impacto econômico suficiente para dissuadir práticas abusivas, tendo em vista o *modus operandi* das *big techs.*

## CONSIDERAÇÕES FINAIS

A presente monografia, teve por objetivo percorrer as evoluções tecnológicas que ensejaram maior atenção dos órgãos estatais e da sociedade civil na defesa dos direitos da personalidade, haja vista os meios de que as *bigs techs* dispõem e se utilizam para aperfeiçoar a assertividade de seus produtos.

Em um contexto de globalização, os dados do usuário ganham relevância comercial e dão origem a uma nova matéria prima, porque as informações coletadas são utilizadas no aperfeiçoamento de seus algoritmos, do seu ecossistema ou compartilhados com terceiros "parceiros", o que resulta no processo de monetização desses dados. Essa coleta é armazenada em banco de dados e processadas, com fins de processamento e refinamento, assim as empresas detém características da personalidade, das necessidades ou até mesmo dos desejos dos usuários. O monitoramento comportamental e social do usuário, que é inerente da atividade das maiorias das *big techs,* se mostra uma verdadeira linha tênue entre licitude e ilicitude.

Os Estados e a sociedade civil, ao se depararem com o potencial de manipulação dos usuários, por meio dos serviços oferecidos com base na análise refinada das informações coletadas, solidificaram em seus ordenamentos jurídicos, normas específicas sobre o tratamento de dados.

Antes de haver regulação específica sobre o tema, se valia de preceitos universais, como o direito à vida privada e os princípios inerentes da lealdade, para legitimar ou deslegitimar o tratamento de dados. No início do auge da *Internet*, preocupada com os avanços tecnológicos, a União Europeia editou a Diretiva 95/46, que tratava sobre a proteção de dados, porém, ostentava natureza de recomendação, sendo opcional a adoção das recomendações pelos países-membros da UE.

Com intuito de reforçar e uniformizar a aplicabilidade das normas protetoras de dados no âmbito europeu, a UE editou o Regulamento Geral de Proteção de Dados, norma que acabou legitimando a atividade de tratamento de dados, delineando limites e impondo sanções aos que excederem os princípios-mor do regulamento, quais sejam: a legalidade, lealdade e transparência. O regulamento assegura que os dados sejam tratados de forma ética e dentro do arcabouço legal; com limitação da finalidade, que impede o uso de dados para fins distintos dos autorizados pelo titular; e minimização dos dados, que assegura que apenas informações estritamente necessárias sejam coletadas.

Tais princípios são fundamentais para garantir um equilíbrio entre inovação tecnológica e a proteção dos direitos fundamentais dos indivíduos, contribuindo para o fortalecimento do Estado de Direito.

No contexto constitucional brasileiro, o direito à privacidade e o livre desenvolvimento da personalidade estão intrinsecamente ligados ao direito à proteção de dados, uma vez que a Constituição Federal, em seu artigo 5º, incisos X e XI, garante a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, direitos que se estendem à proteção das informações pessoais em meio digital. A defesa do livre desenvolvimento da personalidade, por sua vez, está relacionada à capacidade de cada indivíduo de construir sua identidade e autonomia sem interferências indevidas, o que é diretamente afetado pelo controle sobre seus próprios dados. Esses princípios constitucionais servem como base para a Lei Geral de Proteção de Dados (LGPD), reforçando a necessidade de um arcabouço legal que proteja os dados pessoais contra usos abusivos e manipulações, especialmente em um ambiente digital dominado por grandes empresas tecnológicas.

A LGPD estabelece uma série de princípios fundamentais para o tratamento de dados, incluindo a finalidade, adequação, necessidade e transparência. O princípio da finalidade assegura que os dados sejam utilizados apenas para objetivos legítimos e claros; o da adequação, que o tratamento seja compatível com as finalidades comunicadas ao titular; e o da necessidade, que restringe a coleta e tratamento ao mínimo essencial. A transparência permite que os titulares tenham acesso às informações sobre como seus dados estão sendo tratados, promovendo um controle mais efetivo, em respeito aos preceitos da autodeterminação informativa. Além disso, os princípios da segurança e prevenção estabelecem que os agentes de tratamento devem adotar medidas técnicas e organizacionais para proteger os dados contra acessos não autorizados e incidentes.

No que tange à responsabilidade, conforme exposto no Capítulo II, a doutrina diverge entre a modalidade de responsabilidade a ser adotada nos casos de descumprimento da LGPD, entretanto, em específico às *big techs*, se percebe, na realidade brasileira, a incidência do CDC nas relações entre usuários e prestadoras, o que atrai a incidência de regras de responsabilização objetiva, porquanto o descumprimento das normas contidas no LGPD enseja falha na prestação dos serviços, entretanto, o dever de indenizar o dano deverá ser pautado no caso concreto, considerando a espécie de dado do titular violado.

Em comparação internacional, a União Europeia, com o RGPD, estabelece um regime semelhante, mas com maior experiência acumulada e padronização na aplicação das regras.

Isso se reflete em decisões consistentes e robustas em relação à proteção de dados, que têm servido de referência global. Nos Estados Unidos, a abordagem varia, com leis estaduais como o CCPA da Califórnia adotando princípios similares, mas com menor uniformidade. A diferença principal reside na força das sanções e no rigor da aplicação, onde a UE demonstra maior efetividade.

Dado o cenário de monetização crescente das informações pessoais pelas *big techs,* os usuários enfrentam uma desvantagem significativa no controle sobre seus dados. A assimetria de poder entre consumidores e empresas exige um regime legal forte e eficaz. Qualquer falha na prestação dos serviços de dados deve, portanto, ensejar a responsabilização dos agentes, garantindo a proteção dos direitos fundamentais dos cidadãos em um ambiente digital cada vez mais complexo e influente.

Assim, a análise comparativa entre o Brasil e outros países mostra um esforço contínuo para equilibrar inovação tecnológica e proteção de direitos, um desafio constante no contexto globalizado e digital em que vivemos.

## REFERÊNCIAS BIBLIOGRÁFICAS


AMNESTY INTERNATIONAL. **What the Digital Services Act means for human rights and harmful Big Tech business models.** AI Index: POL 30/5830/2022, 7 de julho de 2022. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiKztXLvdaJAxXoppUCHecBOocQFnoECBoQAQ&url=https%3A%2F%2Fwww.amnesty.org%2Fen%2Fdocuments%2Fpol30%2F5830%2F2022%2Fen%2F&usg=AOvVaw3HnJ7pRJgZ9cDApx7Lznyt&opi=89978449. Acesso em: 3 nov. 2024.

ARADY MIRANDA, Felipe. **O direito fundamental ao livre desenvolvimento da personalidade.** Revista Internacional de Direito e Bioética, v. 2, n. 10, p. 11175-11211, 2013. Disponível em: http://www.idb-fdul.com/. Acesso em: 11 nov. 2024.

ARAYA, E. R. M.; VIDOTTI, S. A. B. G. **Criação, proteção e uso legal de informação em ambientes da World Wide Web.** São Paulo: Editora UNESP; São Paulo: Cultura Acadêmica, 2010. 144 p. ISBN 978-85-7983-115-7. Disponível em: SciELO Books.

BARROS, F. K. F. **Fake News, legislação simbólica e a proteção dos direitos fundamentais e da personalidade digital.** In: OMMATI, J. E. M. (org.). Escritos de direitos fundamentais. Belo Horizonte: Conhecimento Editora, 2021.

BECHARA, F. R.; TASINAFFO, F. L. V.; CASTILHO, A. A. **Análise crítica da responsabilidade penal das pessoas jurídicas frente ao poder econômico das Big Techs**. Diálogos Possíveis, v. 21, n. 2, 2022.

BORTOTTO, G. B. **Big techs e financeirização: desenvolvimento tecnológico e capitalismo no século XXI**. In: SILVA, J. R.; COSTA, M. P. (Org.). *Tecnologia e Sociedade no Século XXI.* São Paulo: Editora Acadêmica, 2022. p. 55-78.

BRASIL. Conselho da Justiça Federal. **Enunciado nº 683.** IX Jornada de Direito Civil, 2022. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/1822 . Acesso em: 15 nov. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Diário Oficial da União: seção 1, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 nov. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 16 nov. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 16 nov. 2024.

BRASIL. Poder Judiciário do Estado do Maranhão. **Sentença nº 0816292-73.2020.8.10.0001.** Comarca da Ilha de São Luís, Vara de Interesses Difusos e Coletivos. Juiz: Douglas de Melo

Martins. São Luís, 07 mar. 2024. Disponível em: https://www.tjma.jus.br/midia/cgj/noticia/512691/justica-condena-tik-tok-a-pagar-dano-moral-coletivo-e-individual. Acesso em: 16 nov. 2024.

BRASIL. Poder Judiciário do Estado de Minas Gerais. **Processo nº 5064103-55.2019.8.13.0024.** 29ª Vara Cível da Comarca de Belo Horizonte. Juiz: Jose Mauricio Cantarino Villela. Belo Horizonte, 24 jul. 2023. Disponível em: https://www4.tjmg.jus.br/juridico/sf/proc_resultado2.jsp?listaProcessos=50641035520198130024 . Acesso em: 16 nov. 2024.

BRASIL. Poder Judiciário do Estado de Minas Gerais. **Processo nº 5127283-45.2019.8.13.0024.** 29ª Vara Cível da Comarca de Belo Horizonte. Juiz: Jose Mauricio Cantarino Villela. Belo Horizonte, 24 jul. 2023. Disponível em: https://www4.tjmg.jus.br/juridico/sf/proc_resultado2.jsp?listaProcessos=51272834520198130024 . Acesso em: 16 nov. 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6649**, Distrito Federal. Relator: Min. Alexandre de Moraes. Diário da Justiça Eletrônico, Brasília, 25 jul. 2023. Disponível em: https://www.stf.jus.br. Acesso em: 16 nov. 2024.

BURRI, A.; NICKL, J. ECJ **specifies right to compensation under Art. 82 GDPR in C-300/21 – Österreichische Post. Perfect Law**, 2023. Disponível em: https://perfectlaw.co.uk/ecj-specifies-right-to-compensation-under-art-82-gdpr-in-c-300-21-osterreichische-post/. Acesso em: 2 nov. 2024.

CALIFÓRNIA. **California Consumer Privacy Act of 2018**. California Civil Code §§ 1798.100-1798.199. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 16 nov. 2024.

CALIFÓRNIA. **California Privacy Rights Act of 2020.** California Civil Code §§ 1798.100-1798.199. Disponível em: https://cppa.ca.gov. Acesso em: 16 nov. 2024.

CARVALHO, A. S.; POÇAS, I. R. **Big data e o regulamento geral de proteção de dados da União Europeia.** Revista Ibérica do Direito, v. 1, n. 2, p. 170-177, jul./dez. 2020.

CARVALHO, G. P. de. **Uma reflexão sobre a rede mundial de computadores.** Sociedade e Estado, Brasília, v. 21, n. 2, p. 549-554, maio/ago. 2006.

CARVALHO, Victor Miguel Barros de. **O direito fundamental à privacidade ante a monetização de dados pessoais na internet: apontamentos legais para uma perspectiva regulatória. 2018.** 145 f. Dissertação (Mestrado em Direito) – Universidade Federal do Rio Grande do Norte, Natal, 2018. Disponível em: https://repositorio.ufrn.br/handle/123456789/26851. Acesso em: 11 nov. 2024.

CASTELLS, M. **A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade.** Rio de Janeiro: Zahar, 2003.

COSTA, F. V.; BARROS, F. K. F.; DOS SANTOS, J. M. M. G. **Contornos sobre a responsabilidade civil das grandes empresas de tecnologia "big techs" em casos de**

**violação ao direito fundamental à proteção de dados.** Revista Brasileira de Direito Civil em Perspectiva, v. 8, n. 1, p. 1-24, 2022.

CRISANTO, J. C.; EHRENTRAUD, J.; FABIAN, M.; MONTEIL, A. **Big tech interdependencies – a key policy blind spot. Basel: Financial Stability Institute, Bank for International Settlements**, 2022. Disponível em: https://www.bis.org/fsi/publ/insights44.htm. Acesso em: 3 nov. 2024.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. O**s desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias**. Revista Jurídica Luso-Brasileira, Lisboa, v. 6, n. 2, p. 389-418, 2020. Disponível em: https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf. Acesso em: 11 nov. 2024.

ESTADOS UNIDOS. **Privacy Act of 1974**, Public Law 93-579. 93rd Congress, 21 dez. 1974. Disponível em: https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf. Acesso em: 16 nov. 2024.

EUROPEAN COMMISSION. **New rules to protect your rights and activity online in the EU**. 16 de fevereiro de 2024. Disponível em: https://commission.europa.eu/news/new-rules-protect-your-rights-and-activity-online-eu-2024-02-16_en

FIGUEIREDO, J. F. **O movimento das big techs e o contexto da digitalização dos meios de pagamentos no Brasil.** 2022. Monografia (Bacharelado em Ciências Econômicas) – Instituto de Economia, Universidade Estadual de Campinas, Campinas, 2022.

FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 439-459, 1993.

GARRIDO, Patricia P. Proteção de Dados Pessoais: Comentários À Lei N 13709/2018 (Lgpd) - 4ª Edição 2022. 4th ed. Rio de Janeiro: Saraiva Jur, 2023. E-book. p.I. ISBN 9786555599480. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555599480/. Acesso em: 17 nov. 2024.

GUNST, S.; VILLE, F. D. **The Brussels effect: how the GDPR Conquered Silicon Valley.** European Foreign Affairs Review, v. 26, n. 3, p. 437–458, 2021. Disponível em: https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.3/EERR2021036. Acesso em: 10 out. 2024.

HUSTINX, P. **Data protection and international organizations: a dialogue between EU law and international law.** International Data Privacy Law, v. 11, n. 2, p. 77-80, 2021. Disponível em: https://academic.oup.com/idpl/article/11/2/77/6295718?login=true. Acesso em: 3 nov. 2024.

JACOBIDES, Michael G.; LAMBERTO, Zingales. **Regulating Big Tech in Europe: Why, So What, and How.** 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3765324. Acesso em: 11 nov. 2024.
KIRKPATRICK, D. **O efeito Facebook: os bastidores da história da empresa que está conectando o mundo**. Tradução de Maria Lúcia de Oliveira. Rio de Janeiro: Intrínseca, 2010.

LAW BUSINESS RESEARCH LTD. United States. In: **The Privacy, Data Protection and Cybersecurity Law Review.** 8. ed. Londres: Law Business Research, 2021.

LEINER, B. M.; CERF, V. G.; CLARK, D. D.; KAHN, R. E.; KLEINROCK, L.; LYNCH, D. C.; POSTEL, J.; ROBERTS, L. G.; WOLFF, S. **The past and future history of the Internet. Communications of the ACM**, v. 40, n. 2, p. 102-108, 1997.

MĂRĂCINE, V.; VOICAN, O.; SCARLAT, E. **The Digital Transformation and Disruption in Business Models of the Banks under the Impact of FinTech and BigTech**. Proceedings of the International Conference on Business Excellence, Walter de Gruyter GmbH, 1 jul. 2020. Disponível em: https://www.researchgate.net/publication/343703519_The_Digital_Transformation_and_Disruption_in_Business_Models_of_the_Banks_under_the_Impact_of_FinTech_and_BigTech. Acesso em: 16 abr. 2024.

MIRANDA, F. A. **O direito fundamental ao livre desenvolvimento da personalidade.** Centro de Investigação de Direito Privado, Ano 2, 2013. Acesso em: 8 jun. 2024.

MONTENEGRO, R. H. M. O **devido processo tecnológico na prestação de serviços digitais (tratamento de conteúdo digital) sob responsabilidade das big techs**. International Journal of Digital Law, Belo Horizonte, v. 4, n. 1, p. 9-34, jan./abr. 2023.

NUNES, C. J. C. de O. **Política antitruste em mercados digitais: o caso das Big Techs.** Uberlândia: Universidade Federal de Uberlândia, Instituto de Economia e Relações Internacionais, 2023. Trabalho de Conclusão de Curso (Graduação em Ciências Econômicas).

O DILEMA DAS REDES. The Social Dilemma. Documentário, Estados Unidos, 2020, 89 minutos. Direção: Jeff Orlowski. Distribuição: Netflix.

PASSOS, B. R. S. **O direito à privacidade e a proteção aos dados pessoais na sociedade da informação: uma abordagem acerca de um novo direito fundamental.** 2017. Dissertação (Mestrado em Direito Público) – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2017.

PORTAL SEGINFO. **8 fatores que a nova Lei CPRA da Califórnia tem em comum com a GDPR.** *SegInfo*, 02 fev. 2021. Disponível em: https://seginfo.com.br/2021/02/02/8-fatores-que-a-nova-lei-cpra-da-california-tem-em-comum-com-a-gdpr/. Acesso em: 3 nov. 2024.

REIMANN, Martin et al. **Embodiment in judgment and choice.** Journal of Neuroscience, Psychology, and Economics, v. 5, n. 2, p. 104, 2012.

ROCHA, G. C.; FILHO, V. B. S. **Da guerra às emoções: história da internet e o controverso surgimento do Facebook.** In: *ENCONTRO REGIONAL NORTE DE HISTÓRIA DA MÍDIA*,

4., 2016, Rio Branco. *Anais […]*. Rio Branco: Alcar — Associação Brasileira de Pesquisadores da História da Mídia, 2016.

SAMPAIO, V. **O caso Watergate e a origem do termo lavagem de dinheiro.** Consultor Jurídico, São Paulo, 19 out. 2024. Disponível em: https://www.conjur.com.br/2024-out-19/o-caso-watergate-e-a-origem-do-termo-lavagem-de-dinheiro/. Acesso em: 3 nov. 2024.

SANTANA, Wesley**. Apple e Google são amigas ou rivais? Empresas têm acordo bilionário**. 2024. Disponível em: https://investidor10.com.br/noticias/apple-e-google-sao-amigas-ou-rivais-empresas-tem-acordo-bilionario-106536/. Acesso em: 16 nov. 2024.

SARLET, I. W. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos Fundamentais & Justiça, Belo Horizonte, v. 14, n. 42, p. 179-218, jan./jun. 2020.

SOUZA, Queila R.; QUANDT, Carlos O. Metodologia de Análise de Redes Sociais. In: DUARTE, F.; QUANDT, C.; SOUZA, Q. R. (Org.). **O Tempo das Redes.** São Paulo: Perspectiva, 2008. p. 31-63.

SOARES, Rafael Ramos. **Lei Geral de Proteção de Dados – LGPD: Direito à privacidade no mundo globalizado.** 2020. Monografia (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Escola de Direito e Relações Internacionais, Goiânia, 2020.

SUPERIOR TRIBUNAL DE JUSTIÇA. LGPD: **Um marco na regulamentação sobre dados pessoais no Brasil.** *STJ*, 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em: 15 nov. 2024.

SUPREME COURT OF THE UNITED STATES. **Gonzalez v. Google LLC**, 598 U.S. (2023). Decisão de 18 maio 2023. Disponível em: https://www.supremecourt.gov/opinions/22pdf/21-1333_8m58.pdf. Acesso em: 16 nov. 2024.

TJUE. Tribunal de Justiça da União Europeia. **Decisão do caso C-300/21, UI v. Österreichische Post AG.** *ECLI:EU:C:2023:370*, 4 maio 2023. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=271248&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=7523226. Acesso em: 2 nov. 2024.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia.** Jornal Oficial da União Europeia, C 202/389, 7 jun. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12016P/TXT. Acesso em: 3 nov. 2024.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Jornal Oficial das Comunidades Europeias, Luxemburgo, L281, p. 31-50, 23 nov. 1995.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao**

**tratamento de dados pessoais e à livre circulação desses dados**. Jornal Oficial da União Europeia, L 119, p. 1-88, 4 maio 2016.

UNIÃO EUROPEIA. **Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022. Relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE**. Jornal Oficial da União Europeia, L 277, p. 1-60, 27 out. 2022.

UNIÃO EUROPEIA. **Tribunal de Justiça da União Europeia. Caso C-131/12, Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos e Mario Costeja González.** Sentença de 13 maio 2014. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131. Acesso em: 16 nov. 2024.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. **Caso C-645/19, Facebook Ireland Ltd contra Autoridade Belga de Proteção de Dados.** Sentença de 15 jun. 2021. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=242146&doclang=PT. Acesso em: 16 nov. 2024.

VALENTE, J. C. L. **Tecnologia, informação e poder: das plataformas online aos monopólios digitais.** Revista Sociedade e Estado, v. 35, n. 3, 2020.

VIEIRA, Victor Rodrigues Nascimento. **O que é o livre desenvolvimento da personalidade?** JusBrasil, 2020. Disponível em: https://www.jusbrasil.com.br/artigos/o-que-e-o-livre-desenvolvimento-da-personalidade/1108676532. Acesso em: 15 nov. 2024.

WILSON, Fred. **The 30% tax**. 2018. Disponível em: https://avc.com/2018/08/the-30-tax/. Acesso em: 16 nov. 2024.

ZANATTA, Rafael A. F. **Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais.** Preprint. Fevereiro de 2019. Disponível em: https://www.researchgate.net/publication/331287708. Acesso em: 12 nov. 2024.