

**XXX CONGRESSO NACIONAL DO
CONPEDI FORTALEZA - CE**

DIREITOS E GARANTIAS FUNDAMENTAIS II

JANAÍNA MACHADO STURZA

MARIA CREUSA DE ARAÚJO BORGES

FABRÍCIO VEIGA COSTA

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

D597

Direitos e garantias fundamentais II [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Fabricio Veiga Costa; Janaína Machado Sturza; Maria Creusa De Araújo Borges. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia

ISBN: 978-65-5648-809-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direitos. 3. Garantias fundamentais. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34



XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITOS E GARANTIAS FUNDAMENTAIS II

Apresentação

No quadro do XXX Congresso Nacional do CONPEDI (Conselho Nacional de Pesquisa e Pós-Graduação em Direito), realizado entre os dias 15 e 17 de novembro de 2023 na cidade de Fortaleza/CE, teve lugar um profícuo debate no campo da pesquisa dos Direitos e Garantias Fundamentais com a apresentação de trabalhos de professores, doutorandos e mestrandos. Destaca-se o avanço da pesquisa nesse campo com a inserção de temas que resultam dos impactos das configurações da sociedade digital contemporânea, os quais demandam inovação e o exame crítico das consequências da utilização da inteligência artificial. Essas novas configurações impactam na seara dos direitos fundamentais, exigindo uma produção da pesquisa, de modo crítico, desenvolvida na pós-graduação e demandam o posicionamento na seara dos Direitos Fundamentais, como os temas das BIG TECHS, da proteção de dados, da defesa da democracia e da liberdade de expressão. Enfatiza-se, também, as articulações interdisciplinares entre campos do saber, como o Direito Constitucional, o Direito Internacional dos Direitos Humanos, que tiveram lugar nas abordagens utilizadas nos textos, destacando as articulações multiníveis nessa seara. Nessa perspectiva, se inserem os textos aqui apresentados, os quais expressam essa inovação e as articulações interdisciplinares. É indiscutível a qualidade dos artigos apresentados que resultam de pesquisas realizadas no campo da pós-graduação em Direito no Brasil. Os textos aqui apresentados expressam essas articulações e a significativa contribuição para a Ciência Jurídica.

A COLETA DE INFORMAÇÕES PELAS BIG TECHS E O DIREITO FUNDAMENTAL A PROTEÇÃO DE DADOS

THE COLLECTION OF INFORMATION BY BIG TECH AND THE FUNDAMENTAL RIGHT TO DATA PROTECTION

**Laura Finoto dos Santos
Camila Museti Bezerra**

Resumo

O presente artigo possui o escopo de compreender como a coleta de informações feitas pelas gigantes tecnológicas, como Google, Facebook e Amazon, se relaciona com o direito à privacidade, sendo este, um direito fundamental, de caráter metaindividual. Utilizando uma abordagem de cunho analítico, examina-se a jurisprudência internacional concomitantemente à legislação vigente, destacando desafios metodológicos e legais. Conclui-se que as regulamentações atuais, embora relevantes, nem sempre conseguem acompanhar o ritmo acelerado da evolução tecnológica. Revela-se a tensão entre a busca por inovação e a proteção dos direitos individuais e transindividuais, sublinhando a necessidade de uma legislação ágil e adaptável. Com isso, o estudo oferece uma visão esclarecedora das complexas relações entre a coleta de informações pelas Big Techs e o direito à privacidade, ressaltando a importância de um equilíbrio regulatório eficaz para garantir o direito fundamental à proteção dos dados, direito este garantido pela Constituição Federal de 1988 para uma sociedade massificada, em um cenário de constante avanço da era digital.

Palavras-chave: Big techs, Proteção, Coleta, Dados, Direitos fundamentais

Abstract/Resumen/Résumé

The aim of this article is to understand how the collection of information by technology giants such as Google, Facebook and Amazon relates to the right to privacy, which is a fundamental right of a meta-individual nature. Using an analytical approach, international case law is examined alongside current legislation, highlighting methodological and legal challenges. It concludes that current regulations, although relevant, are not always able to keep up with the rapid pace of technological evolution. The tension between the search for innovation and the protection of individual and transindividual rights is revealed, underlining the need for agile and adaptable legislation. With this, the study offers an enlightening view of the complex relationships between the collection of information by Big Tech and the right to privacy, highlighting the importance of an effective regulatory balance to guarantee the fundamental right to data protection, a right guaranteed by the 1988 Federal Constitution for a mass society, in a scenario of constant advancement in the digital age.

Keywords/Palabras-claves/Mots-clés: Big techs, Protection, Collection, Data, Fundamental rights

INTRODUÇÃO

A Emenda Constitucional 115/2022 incluiu a proteção de dados no rol dos direitos e garantias fundamentais do cidadão e, estabeleceu a exclusiva responsabilidade da União em legislar sobre a proteção e o manuseio de informações pessoais. Essa medida, visa fortalecer a estabilidade jurídica nacional na implementação da Lei Geral de Proteção de Dados, deixando claro em sua redação que o direito à proteção dos dados pessoais abrange os meios digitais.

No período anterior à vigência da LGPD, as organizações eram capazes de coletar uma ampla gama de informações pessoais sem a necessidade de obter o consentimento explícito dos titulares dos dados. Esse cenário suscitava sérias inquietações relacionadas à segurança e à privacidade. A ausência de regulamentação substancial abria brechas para a utilização indevida dos dados, como vendas indiscriminadas para fins de *marketing*, compartilhamentos não autorizados com terceiros e até mesmo a exposição a vazamentos e violações de segurança.

A implementação da Lei Geral de Proteção de Dados representou uma mudança substancial nesse panorama. Foi estabelecido um arcabouço legal abrangente para a coleta, uso e tratamento de dados pessoais, com o objetivo primordial de salvaguardar a privacidade dos indivíduos e fomentar uma cultura de responsabilidade e transparência na manipulação de dados.

Essa legislação introduziu princípios fundamentais para a coleta de informações, exigindo que as organizações obtivessem o consentimento explícito dos titulares, oferecessem informações claras e transparentes quanto à finalidade da coleta e garantisse medidas adequadas de segurança para proteger os dados pessoais. Ademais, a lei conferiu aos titulares uma série de direitos, incluindo o acesso, retificação, exclusão e obtenção de informações acerca do compartilhamento e uso desses dados.

No entanto, mesmo diante dessas proteções, o controle da coleta e uso de dados pelas *Big Techs* apresenta-se como um desafio considerável, pois o fluxo incessante e volumoso de informações coletadas levanta a questão de uma regulamentação genérica e, por vezes, insuficientemente protetora aos direitos dos titulares.

Portanto, o propósito central deste artigo é analisar a abordagem que as entidades reguladoras de mídias sociais estão adotando no contexto da Lei Geral de Proteção de Dados, além de investigar de maneira específica o direito fundamental a proteção de dados; o poder de coleta de informações das *Big Techs*; a convergência e conflito entre as *Big Techs* e a Lei Geral de Proteção de Dados e trazer as perspectivas futuras sobre o tema.

A metodologia do artigo será por meio de uma pesquisa qualitativa, utilizando-se do método dedutivo, com as seguintes características: sob ótica de sua natureza, será uma pesquisa aplicada, quanto ao objetivo será uma pesquisa exploratória, buscando prover informações e investigações sobre o assunto. A respeito da técnica será uma pesquisa bibliográfica, utilizando-se doutrinas, websites, leis, jurisprudências, artigos científicos, internet, livros, adicionar entrevista, análise de conteúdo revistas, publicações em periódicos, jornais, boletins, monografias, dissertações, teses, material cartográfico e sites jurídicos, que disponham sobre o tema e proporcionem uma análise apurada sobre a temática.

2 O DIREITO FUNDAMENTAL A PROTEÇÃO DE DADOS

Os dados pessoais se tornaram o “novo petróleo” do mundo moderno, inferindo diretamente na privacidade e individualidade das pessoas. A vista disso, no contexto do direito internacional público, no âmbito do sistema de proteção universal da Organização das Nações Unidas (ONU), emerge um direito à proteção de dados que é especialmente derivado do direito à privacidade, embora estes dois conceitos não se confundam. E é nesse sentido que a Comissão de Direitos Humanos da ONU orienta, ao interpretar a abrangência do artigo 17 do Pacto Internacional de Direitos Civis e Políticos, juntamente com a jurisprudência da Corte Europeia de Direitos Humanos (CEDH) e do Tribunal de Justiça da União Europeia (TJUE), ancorados no artigo 8º da Convenção Europeia (Chiedermaier et al., 2021).

Apenas em 1981, na Convenção nº 108 para Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, que o direito à proteção de dados foi reconhecido como direito fundamental. Contudo, este conceito foi vinculado aos integrantes da União Europeia em 2009, com o Tratado de Lisboa (Doneda, 2011).

No Brasil, a Constituição Federal de 1988 revolucionou a proteção dos direitos individuais e coletivos, dispondo sobre a tutela a intimidade e privacidade, bem como ao sigilo de correspondência e comunicação telefônica. Nesse sentido, a Emenda Constitucional 115/2022, juntamente com o artigo 5º, LXXIX, garantiu o direito à preservação das informações pessoais, inclusive em ambientes digitais. Ademais, incorporou o artigo 21, XXVI, que estabelece a estruturação e supervisão da proteção e do tratamento de informações individuais (Brasil, 1988).

A Lei Geral de Proteção de Dados Pessoais, por sua vez, surge como um marco fundamental no reconhecimento da importância dos dados na sociedade. Ela regula o

tratamento das informações, especialmente em contextos digitais, relativos a indivíduos e entidades legais, tanto públicas quanto privadas, com o propósito de salvaguardar os direitos essenciais à liberdade e privacidade (Brasil, 2018).

Neste contexto, a Lei 13.709/2018 regulamentou a obrigatoriedade das empresas estabelecerem uma base legal para a coleta e tratamento dos dados pessoais (artigo 7º da Lei 13.709/2018). Entretanto, o expansionismo do mercado digital exponenciou o crescimento das *Big Techs*, que utilizam da coleta de dados como matéria prima para seu funcionamento, como a *Apple*, *Amazon*, *Google* e *Instagram* (Brasil, 2018).

Dessa forma, por mais abrangente que seja a legislação, as informações fornecidas pelos usuários dessas plataformas são vulneráveis diante de seu alcance global, de modo que é preciso analisar o cenário dos dados pessoais e a proteção deste direito fundamental frente o mercado moderno.

3 BIG TECHS: PODER E COLETA DE INFORMAÇÕES

As *Big Techs* personificam a modernidade e o dinamismo da era digital. Essas corporações transcendem a definição convencional de empresas, transformando-se em ecossistemas complexos que orquestram as interações digitais. Empresas, como *Amazon*, *Google*, *Facebook* e *Apple*, não apenas oferecem serviços, mas desempenham um papel central na maneira de se interagir, comunicar e consumir informações (Guitarrara, s.d). Seus produtos e serviços se imiscuem tão profundamente nas vidas dos usuários que se tornam quase inseparáveis de sua identidade digital. A comodidade aparente que oferecem contrasta com o custo oculto: a coleta incessante de dados.

As *Big Techs* são caracterizadas por sua amplitude de influência e sua capacidade de consolidar diversos serviços e plataformas sob uma única marca. O termo engloba empresas que abrangem campos como busca na web, redes sociais, comércio eletrônico, tecnologia móvel e muito mais. Essas corporações frequentemente ultrapassam fronteiras geográficas e setoriais, construindo um ecossistema que toca inúmeras esferas da vida moderna (Guitarrara, s.d).

O poder exponencial das *Big Techs* é manifestado na vastidão de dados que acumulam. Cada busca, clique, curtida e compartilhamento contribui para a construção desse universo de informações, uma pista digital que descreve inclinações, preferências e hábitos. Esses dados, por sua vez, são processados por algoritmos complexos que decifram padrões, preveem comportamentos e refinam suas estratégias. Assim, as *Big Techs*, não apenas fornecem

resultados de busca ou conteúdo relevante; elas influenciam o modo de ver o mundo (Guitarrara, s.d).

O surgimento de um novo paradigma de poder despertou um debate crucial sobre soberania digital. As *Big Techs*, muitas vezes multinacionais com operações globais, transcendem fronteiras geográficas e jurisdições nacionais e, isso coloca questões sobre quem regula e supervisiona essas entidades que, em muitos aspectos, se tornaram mais poderosas que nações inteiras. A busca por um equilíbrio entre a inovação que essas empresas geram e os potenciais riscos que representam para a sociedade é um desafio complexo (Jovelino, 2022).

A coleta de informações, no entanto, não é unilateral. Muitos usuários participam voluntariamente desse ecossistema, trocando dados pessoais por conveniência, personalização e acesso a serviços. O contrato implícito nessa troca é muitas vezes embutido em longos termos de serviço e políticas de privacidade, cuja extensão e complexidade frequentemente desafiam a compreensão do usuário comum. Isso levanta a questão crucial da transparência e consentimento informado, já que a coleta de informações deve ser uma escolha consciente e esclarecida (Jovelino, 2022).

As *Big Techs* também têm sido criticadas por explorar e monopolizar mercados, criando um ambiente que dificulta a concorrência saudável. Sua capacidade de coletar dados e utilizá-los para fortalecer seus negócios existentes ou adentrar novos setores gera preocupações de anti-competitividade. Isso levou a investigações antitruste e a discussões sobre a necessidade de regulamentação mais rigorosa para evitar abusos de posição dominante (“Big techs na mira: entenda as investigações antitruste”, 2021).

Diante disso, as *Big Techs* ocupam uma posição de destaque na intersecção entre tecnologia, sociedade e política. Elas desvendam as possibilidades do mundo digital, mas também acendem alertas sobre privacidade, poder e ética. Surge, portanto, um importante questionamento: é de fato possível controlar o que pode ou não ser feito com os dados coletados? Em um mundo em que a maioria dos indivíduos detêm acesso à internet deixam rastros, dados e informações por vezes pessoais demais, os quais são controlados por pessoas com interesses próprios, esse controle parece utópico.

O assunto é sensível e delicado e pode-se citar para fins de reflexão a seguinte situação, ao qual seja, se determinado governo começa a mostrar grande desejo em restringir seus poderes, qual garantia se tem de que funcionários ou os próprios donos das *Big Techs* não usem as informações que possuem para influenciar ou aliciar os governantes a não exercerem um controle excessivo sobre o que pode ou não ser feito? Esta incerteza ressalta a complexidade da

situação, em que a interdependência entre empresas tecnológicas e agentes políticos pode minar os esforços por uma regulamentação justa e imparcial.

O desafio se torna ainda mais acentuado quando se considera o alcance global dessas empresas. Suas operações transcendem fronteiras nacionais, deixando muitas vezes governos e reguladores em uma posição de desvantagem. À medida que essas empresas expandem suas esferas de influência, o controle efetivo sobre a coleta e uso de dados torna-se uma tarefa cada vez mais complexa, desafiando as estruturas tradicionais de governança.

3.1 O Novo Petróleo

A metáfora do petróleo, como fonte de riqueza e poder no século XX agora encontra uma ressonância surpreendente no contexto da era digital, onde os dados emergem como o novo recurso de valor inestimável. Assim como o petróleo alimentou as revoluções industriais passadas, os dados agora alimentam a revolução da informação, tendo sido reconhecidos por Clive Humby como o "novo petróleo" (*Data is the new oil*) do século XXI (Ripari, 2022).

As *Big Techs* são as principais protagonistas dessa exploração, e sua capacidade de coletar, analisar e monetizar dados moldou a paisagem tecnológica atual. Assim como o petróleo era cobiçado por suas múltiplas aplicações industriais, os dados são almeçados pelas *Big Techs*, por sua capacidade de informar decisões estratégicas, aprimorar produtos e direcionar anúncios. Cada interação digital deixa um rastro de dados, que, quando agregados e analisados, oferecem insights sobre padrões de comportamento, preferências e necessidades. Esse novo petróleo digital não apenas alimenta as operações internas das empresas, mas também é a base de uma economia global de dados que abastece uma variedade de indústrias e setores (“Como a mineração de dados pode ser importante para a empresa?”, 2023).

No entanto, essa analogia também traz à tona questões éticas e de poder. Assim como na era do petróleo, a exploração desenfreada de recursos pode levar a desequilíbrios e consequências indesejadas, a coleta massiva de dados pelas *Big Techs* levanta preocupações sobre privacidade e vigilância. À medida que dados pessoais são extraídos, processados e transformados em ativos valiosos, a proteção dos direitos individuais se torna crucial.

Da mesma forma que os países produtores de petróleo buscam garantir uma parte justa da riqueza gerada por seus recursos naturais, os usuários individuais também questionam a distribuição equitativa dos benefícios gerados a partir de seus dados. A crescente conscientização sobre o valor dos dados pessoais tem impulsionado debates sobre a propriedade

e o controle desses ativos digitais, reivindicando uma voz mais ativa na negociação das regras desse novo jogo.

3.2 A Economia dos Dados: Exploração e Monetização pelas *Big Techs*

No ecossistema digital contemporâneo, os dados emergiram como uma mercadoria de alto valor, sendo vendidos, negociados e transformados em uma nova forma de moeda. Este segmento mergulha nas entranhas da economia dos dados, onde as *Big Techs* lideram uma exploração complexa e multifacetada, transformando interações digitais em ativos monetizáveis (Guitarrara, s.d).

Essas grandes empresas operam em um ciclo incessante de coleta de dados, alimentado por interações online. A cada pesquisa, clique, postagem ou compra, uma miríade de informações é capturada e armazenada. Esses fragmentos de dados são então, agregados e processados em perfis detalhados de usuários, revelando preferências, comportamentos de consumo e tendências. Esse ciclo, aparentemente banal, é a base da riqueza que as empresas detêm (Guitarrara, s.d).

Uma das principais formas de exploração monetária de dados pelas *Big Techs* é a criação de anúncios altamente personalizados. Com base nos perfis de usuários, podem direcionar propagandas específicas que correspondam às preferências individuais. Isso não apenas aumenta a eficácia dos anúncios, mas também agrega valor aos espaços publicitários, gerando receita significativa para quem possui esse poder (“A nova aposta das big techs: Inteligência Artificial na geração de anúncios”, 2023).

Além da monetização direta através de publicidade, as *Big Techs* muitas vezes vendem dados agregados a terceiros, como empresas de análise de mercado e agências de publicidade. Eles podem ser usados para prever tendências, segmentar audiências e informar decisões de negócios. A venda de informações, embora seja uma fonte de lucro, também levanta questões sobre a privacidade e a potencial exposição de informações sensíveis (Quintiliano, 2022).

Além da publicidade e da venda direta de dados, algumas *Big Techs* adotaram modelos de negócios baseados em assinaturas. Nesses casos, as informações do usuário são usadas para personalizar serviços e conteúdo, aumentando o valor percebido pelos clientes e incentivando-os a pagar por assinaturas premium. Esses modelos transformam a própria experiência do usuário em uma fonte de receita contínua (Cuofano, 2023).

Os modelos de assinatura dependem da personalização para criar valor agregado. As *Big Techs* coletam e analisam meticulosamente os dados dos usuários, criando perfis detalhados

que informam sobre suas preferências, hábitos e necessidades. Esses perfis permitem que as empresas customizem a experiência do usuário, apresentando conteúdo, produtos ou serviços que se alinham diretamente com seus interesses. Dessa forma, a personalização torna-se a chave para atrair e reter assinantes (Cuofano, 2023).

A proposta de valor dos modelos de assinatura reside na entrega de uma experiência sob medida. Os dados coletados permitem que as *Big Techs* ofereçam recursos premium, exclusivos ou aprimorados, que não seriam possíveis sem insights profundos sobre o usuário. Isso pode incluir acesso a conteúdo premium, recursos avançados de personalização, remoção de anúncios ou suporte prioritário. Em essência, os dados do usuário se traduzem em uma experiência mais rica e satisfatória (Cuofano, 2023).

Além de elevar a experiência do usuário, os modelos de assinatura garantem uma fonte constante de receita para as Big Techs. Ao invés de depender de receitas voláteis de publicidade ou vendas únicas, essas empresas podem contar com uma base sólida de assinantes que contribuem mensalmente. Essa estabilidade financeira é altamente atraente, permitindo um planejamento mais estratégico e investimentos de longo prazo.

3.3 Forma de Coleta de Dados Pelas Redes Sociais

Sabe-se que as redes sociais coletam grande número de informações. Plataformas como *Facebook*, *Twitter*, *Instagram* e *LinkedIn* utilizam o tratamento de dados como meio indispensável para a atividade fim de seu serviço: oferecer conteúdo personalizado e de interesse para cada usuário. Existem dados bases que são coletados pela maior parte das redes sociais, sendo esses: de perfil do usuário; atividades e interações; publicações e compartilhamento, localização, dispositivos móveis, *cookies* e rastreamento online (“Política de Dados do Instagram: um guia simplificado, Blog do Instagram”, s.d.).

Ao criar um perfil em uma rede social, o usuário fornece suas informações pessoais, como nome, data de nascimento, gênero, localização e interesses. As atividades e interações se referem a curtidas, compartilhamentos, comentários e cliques realizados pelos usuários, que são utilizadas para direcionar o conteúdo conforme os gostos pessoais de cada um (“Política de Dados do Instagram: um guia simplificado, Blog do Instagram”, s.d.).

Referente às publicações e conteúdo compartilhado, quando os usuários praticam essas ações, os dados são coletados e armazenados, podendo as empresas controladoras da rede social em questão extrair insights sobre as preferências e características dos usuários, além de direcionar anúncios personalizados com base nesses dados. Já a localização pode ser fornecida

pelos titulares ao compartilhar seu local atual ou marcar locais visitados. Esses dados de localização fornecem informações valiosas para anunciantes e empresas, permitindo a segmentação geográfica precisa de anúncios e o fornecimento de recomendações personalizadas com base na localização (“Política de Dados do Instagram: um guia simplificado, Blog do Instagram”, s.d.).

O uso de dispositivos móveis é realizado por quase todas as redes sociais e elas solicitam o acesso a esses recursos, como a câmera, o microfone e os contatos, permitindo que as plataformas coletem dados adicionais, como fotos e gravações de áudio, que podem ser usados para melhorar a experiência do usuário e personalizar o conteúdo. Destarte, a solicitação de *cookies* pelas mídias sociais serve para monitorar a atividade dos usuários, direcionando melhor as publicações de interesse do indivíduo (“Política de Dados do Instagram: um guia simplificado, Blog do Instagram”, s.d.).

Por meio desses recursos, as *Big Techs* têm acesso a uma quantidade imensurável de dados por minuto. Isso pode ser analisado por meio de um estudo feito pela plataforma “Domo”, no ano de 2020, período em que a pandemia fez com que o mundo se mantivesse conectado pelos meios digitais:



Fonte: Domo Invest

Importante destacar que o gráfico indica a quantidade de dados coletados a cada minuto, ou seja, empresas como o *Instagram* atingiram a marca de mais trezentos e quarenta e sete posts nos stories por minuto, o que resulta na média de quase quinhentos mil publicações por dia. Portanto, diante da forma que os dados são coletados pelas *Big Techs* e da quantidade exorbitante de informações diárias, é possível compreender a dificuldade em estabelecer uma regulamentação eficaz, que abranja toda a proporção atingida por essas empresas.

3.4 Análise da Política de Dados do *Instagram* e *Facebook*

Para entender o funcionamento da coleta de dados pelas *Big Techs*, far-se-á uma análise de duas principais redes sociais: *Instagram* e *Facebook*. Primeiro, ressalta-se que essas duas redes sociais são da mesma empresa cujo nome é “Meta”.

De acordo com a página de política de privacidade da empresa, é explicado como os dados pessoais são tratados. Destaca-se que, com as informações que os usuários fornecem ao se cadastrarem e utilizarem a plataforma, há o seguinte uso:

(...) coletamos o conteúdo, comunicações e outras informações que você fornece quando usa nossos Produtos, inclusive quando você se cadastra para criar uma conta, cria ou compartilha conteúdo, envia mensagens ou se comunica com outras pessoas. **Isso pode incluir informações presentes ou sobre o conteúdo que você fornece (como metadados), como a localização de uma foto ou a data em que um arquivo foi criado. Isso pode incluir também o que você vê por meio dos recursos que fornecemos**, como nossa câmera, de modo que possamos realizar ações como sugerir máscaras e filtros de que você pode gostar, ou dar dicas sobre o uso de formatos da câmera. **Nossos sistemas processam automaticamente o conteúdo e as comunicações que você e outras pessoas fornecem a fim de analisar o contexto e o conteúdo incluído nesses itens para as finalidades descritas abaixo** (Instagram, 2022) (...)

Ademais, o *Instagram* também coleta informações do dispositivo móvel, conforme dispõe sua política de privacidade:

(...) coletamos informações sobre computadores, telefones, TVs conectadas e outros dispositivos conectados à Web que você usa e que se integram aos nossos Produtos, e combinamos essas informações dos diferentes dispositivos que você utiliza. Por exemplo, usamos as informações coletadas sobre seu uso de nossos Produtos em seu telefone para personalizar melhor o conteúdo (inclusive anúncios) ou os recursos que você vê quando usa nossos Produtos em outro dispositivo, como seu laptop ou tablet, ou para avaliar se você, em resposta a um anúncio que exibimos em seu telefone, realizou uma ação em um dispositivo diferente (Instagram, 2022).

No trecho citado, é possível compreender que a plataforma Meta utiliza dados pessoais para direcionar conteúdos e anúncios. Portanto, é evidente que as informações possuem um fim comercial, pois o que é consumido pelas pessoas se torna a base para o funcionamento da empresa.

As redes sociais são, dessa forma, o instrumento que utiliza os dados pessoais como base de sua atividade fim: ofertar conteúdo, publicidade e anúncios. Como exemplo, tem-se a própria disposição dos termos de uso, sobre o tratamento de informações como localização e anúncio:

Informações relacionadas à localização: **usamos informações relacionadas à localização, como sua localização atual, o local onde você mora, os lugares que você gosta de frequentar**, bem como as empresas e as pessoas que estão perto de você, **a fim de oferecer, personalizar e aprimorar nossos Produtos, inclusive os anúncios**, para você e outras pessoas. As **informações relacionadas à localização podem se basear na localização precisa do dispositivo** (caso você tenha nos dado permissão para coletar esse dado), em endereços IP e em informações sobre o uso dos Produtos da Meta por você e por outras pessoas (como check-ins ou eventos dos quais você participa). (...) Anúncios e outro conteúdo patrocinado: **usamos as informações que temos sobre você, inclusive informações sobre os seus interesses, ações e conexões, para selecionar e personalizar anúncios, ofertas e outros conteúdos patrocinados que exibimos para você**. Saiba mais sobre como selecionamos e personalizamos anúncios e sobre as suas opções em relação aos dados que usamos para selecionar anúncios e outros tipos de conteúdo patrocinados para você nas configurações do Facebook e nas do Instagram (Instagram, 2022).

Desse modo, a própria política de privacidade e informação de uma das maiores *Big Techs* que existe deixa claro a relevância dos dados pessoais para o seu funcionamento. Eles são o fomento que mantém a atividade fim dessas empresas, de modo que fica evidente, ainda que não seja tratado diretamente dessa forma, que as informações pessoais possuem finalidade comercial para as grandes corporações. Como evidência deste fato será descrito um dos casos mais emblemáticos envolvendo uso e comercialização abusiva dos dados pessoais.

3.5 Caso emblemático da Cambridge Analytica envolvendo a coleta de dados

A empresa Cambridge Analytica, com sede em Londres, operava coletando e analisando dados com o propósito de prestar serviços de marketing para campanhas políticas. O escândalo que envolveu a Cambridge Analytica ocorreu em 2016, durante as eleições nos Estados Unidos. O caso veio à tona quando o professor norte-americano David Carroll solicitou que a empresa lhe mostrasse os dados coletados sobre ele, mas teve seu pedido negado. Ele

então contratou um advogado e deu início a um processo que revelou a forma como a empresa coletava e usava os dados pessoais dos usuários do Facebook. O documentário "Privacidade Hackeada" traz uma análise detalhada desse caso ("Privacidade Hackeada | Netflix Official Site", 2019).

Durante a campanha eleitoral de Donald Trump, a Cambridge Analytica foi responsável pelo marketing online, por meio do chamado "Projeto Álamo". A empresa era responsável pela centralização dos dados, direcionando-os para os estados americanos com maior tendência a votar no candidato Donald Trump. Os dados eram obtidos por meio de questionários no *Facebook*, que identificavam o perfil de personalidade dos eleitores norte-americanos. A empresa focava especialmente naqueles chamados de "persuasíveis", ou seja, aqueles que ainda estavam decidindo em qual candidato votar ("Privacidade Hackeada | Netflix Official Site", 2019).

Christopher Wylie, um dos técnicos envolvidos na formação da Cambridge Analytica, afirmou que dados eram coletados por meio do aplicativo do *Facebook*, tanto das pessoas que acessavam o questionário, quanto de seus amigos. *Likes*, postagens, conversas, compartilhamentos e outras atividades realizadas na rede social eram coletados. Com essas informações, que chegavam a um total de 4 a 5 mil pontos por pessoa, a empresa construía o perfil psicológico de cada eleitor dos Estados Unidos. Mensagens personalizadas eram então enviadas com o objetivo de influenciar o voto das pessoas, que desconheciam a forma como seus dados estavam sendo obtidos ("Privacidade Hackeada | Netflix Official Site", 2019).

Estima-se que 50 milhões de pessoas tiveram seus dados vazados pela Cambridge Analytica, evidenciando que a empresa não seguia regulamentações nem limites na coleta e uso dos dados. Ficou claro que o objetivo do chamado *Big Data*, realizado pela empresa, era mudar comportamentos e influenciar os cidadãos dos Estados Unidos a votar em Donald Trump, o candidato para o qual trabalhavam e que acabou sendo eleito presidente na época ("Privacidade Hackeada | Netflix Official Site", 2019).

Durante seu depoimento, o fundador do *Facebook*, Mark Zuckerberg, afirmou que, ao tomar conhecimento da forma como os dados estavam sendo coletados pela Cambridge Analytica, entrou em contato com a empresa para exigir que os dados fossem deletados. No entanto, ficou evidente que a empresa ainda possuía esses dados, o que foi comprovado posteriormente por Brittany Kaiser, por meio de seu calendário empresarial. Zuckerberg também declarou desconhecer se funcionários do *Facebook* estavam diretamente envolvidos com a Cambridge Analytica e admitiu a responsabilidade de prevenir a venda de dados ("Privacidade Hackeada | Netflix Official Site", 2019).

Ao final do processo, a empresa se recusou a devolver os dados a David Carroll e se declarou culpada. Após o escândalo envolvendo a Cambridge Analytica, a empresa declarou falência e foi fechada. Após a controvérsia relacionada à Cambridge Analytica em 2016, a União Europeia introduziu a GDPR (*General Data Protection Regulation*), em 2018. Essa regulamentação teve como objetivo estabelecer diretrizes para a coleta de dados por empresas, visando proporcionar conscientização às pessoas e maior controle sobre o uso de suas informações pessoais. Embora tenha jurisdição nos países europeus, empresas e organizações que desejam fazer negócios no mercado europeu devem ajustar suas práticas de acordo com os requisitos legais estipulados pela legislação. Tal norma também serviu de base para a criação da Lei Geral de Proteção de Dados (“GDPR: entenda o que é o Regulamento Geral de Proteção de Dados”, 2018).

Todavia, apesar de toda regulamentação, o caso serve para evidenciar que o controle dos dados pessoais nas redes sociais é algo abstrato, uma vez que empresas à parte podem acessar informações dos usuários e utilizar disso para manipular e induzir escolhas. Como ocorreu no caso mencionado, a própria política de dados da empresa Meta deixa claro que há contratos para que outras corporações acessem dados dos usuários e direcionem publicidade para esses. Portanto, a regulamentação do uso e venda de informações encontra grandes dificuldades frente a modernização e expansão das *Big Techs*.

4 CONVERGÊNCIA E CONFLITO: BIG TECHS E PROTEÇÃO DE DADOS

Conforme amplamente demonstrado, a coleta de dados operada pelas *Big Techs* entra em conflito com a tutela determinada pela Lei Geral de Proteção de Dados. Nesse sentido, o artigo 7º da Lei 13.709/2018 determina que a empresa que realiza o tratamento de informações pessoais deve fazê-lo sob justificativa de uma das bases legais expressas no dispositivo (Brasil, 2018).

Diante da análise das *Big Techs*, verifica-se que o consentimento foi a base legal majoritariamente adotada para que essas empresas realizem a coleta e tratamento de dados. Assim, para a validação do consentimento, as empresas que atuam no meio digital se utilizam da política de privacidade para descrever quais dados serão coletados, a forma de tratamento e o ciclo de vida desses, de modo claro, fácil e preciso, conforme dispõe o art. 6º, VI, da Lei 13.709/2018 (Brasil, 2018).

De forma detalhada, o art. 9º da Lei 13.709/2018, com base no princípio da transparência, disserta sobre as informações que deverão ser fornecidas aos titulares, que são: a finalidade específica do tratamento; a forma e duração do mesmo; a identificação do controlador; as informações de contato desse e acerca do uso compartilhado de dados por ele e a finalidade; as responsabilidades dos agentes que realizarão o tratamento; e os direitos do titular (Brasil, 2018).

Dessa maneira, para que o consentimento seja válido, deve ser expresso, dado por escrito ou outro meio que demonstre a vontade dos titulares, como vídeos e áudios. No consentimento por escrito, a cláusula deste deve ser destacada e visível, informando a finalidade da empresa. Além disso, o artigo 244 do Código Civil estabelece que deve ser utilizada linguagem clara, objetiva e em língua portuguesa (Brasil, 2002).

Contudo, ao analisar a aplicação da lei pelas *Big Techs* nota-se impasses, uma vez que sua abrangência é tão expandida que prejudica a eficácia legal. Por exemplo, não há como fazer o controle de quantos usuários por dia criam perfil em aplicativos como *Instagram*, *Facebook* e *Tiktok*, de modo que é inviável tratar de maneira individualizada como cada titular dos dados tomará ciência de sua coleta e tratamento, além de verificar se esse consente com todos os termos. Por isso, essas empresas utilizam os *cookies* para que, aceitando os termos de uso do aplicativo, o usuário dê total liberdade para que elas colem e tratem seus dados pessoais (Alves, 2018).

Porém, ainda que nesses termos esteja expresso o ciclo de vida das informações, isso não impede que as *Big Techs* comercializem os dados de seus usuários. Como visto anteriormente, a política de privacidade da empresa Meta, por exemplo, deixa claro que os dados são vendidos à patrocinadores que os utilizam para fazer anúncios que sejam correspondentes com o perfil de cada pessoa.

Esse tema gera debates, haja vista que a comercialização de informações não é vedada se o titular houver consentido ou se outra base legal do artigo 7º da LGPD legitimar tal ação. Contudo, defende-se que para a comercialização ser legítima é preciso se adeque a todas as etapas do Teste Multifatorial de Avaliação do Legítimo Interesse (LIA), que pode ser entendido da seguinte forma:

A utilização da segunda base legal, o legítimo interesse apoia-se no fundamento que a comercialização do banco de dados ocorre para atender o legítimo interesse do controlador e de terceiros que utilizarão os dados para apoiar e promover as suas atividades. Para a utilização da base legal do legítimo interesse, é necessário que um Teste Multifatorial de Avaliação do Legítimo Interesse (LIA), devendo ser cumpridas quatro etapas para que esta

base legal possa ser utilizada de forma lícita: finalidade legítima no interesse do controlador; observância do princípio da necessidade; um teste de proporcionalidade, onde se verifica se o novo uso atribuído ao dados se encontra dentro das legítimas expectativas de seu titular, se o uso era esperado e o impacto em suas vidas, por fim, o dever (e princípio) de transparência deve ser devidamente cumprido, com a clara informação aos titulares sobre o tratamento dos dados (Martinez; Wurzius, 2022).

Destarte, ainda que o preenchimento das condições do Teste Multifatorial possa justificar a comercialização dos dados, majoritariamente entende-se sobre a impossibilidade. Como exemplo cita-se a ação civil pública movida pelo MPDF (Ministério Público do Distrito Federal), através de sua Unidade de Proteção de Dados e Inteligência Artificial, no juízo do Distrito Federal, contra o Serasa *Experian*, sob acusação de comercialização massiva de dados pessoais por meios dos serviços "Lista Online e "Prospecção de Clientes", suscitando a suspensão da comercialização das informações, sob pena de multa diária (Martinez; Wurzius, 2022).

A ação gerou debates sobre o legítimo interesse da empresa requerida, em face da legítima expectativa do titular de dados. O Ministério Público enfatizou que, ao aderir os termos de privacidade, o uso dos dados deve ser proporcional ao fim estabelecido pela empresa, de forma que a comercialização massiva ultrapassa os limites legais. Portanto, para que o ato da empresa fosse legítimo seria necessário consentimento claro e expresso do titular, anuindo o uso de suas informações em caráter econômico (Martinez; Wurzius, 2022).

Destaca-se, o posicionamento do Juiz de Direito Substituto José Rodrigues Chaveiro Filho: "É exatamente por meio do consentimento inequívoco que o titular dos dados consegue controlar o nível de proteção e os fluxos de seus dados, permitindo ou não que suas informações sejam processadas, utilizadas e/ou repassadas a terceiros"(Martinez; Wurzius, 2022).

Em contraponto, o posicionamento do Tribunal de Justiça de Santa Catarina, em uma ação contra o Serasa *Experian*, com o mesmo objeto da anterior, movida por uma pessoa física que se sentiu prejudicada pela venda de seus dados, determinou que não havia ato ilícito nem direito à dano moral (Martinez; Wurzius, 2022).

Em sede de recurso a decisão foi mantida, sob fundamento de não haver comprovação de prejuízos concretos, nem violação à inviolabilidade e intimidade, disposto no art. 5º, X da Constituição Federal (Martinez; Wurzius, 2022).

Ao comprar os dois julgados é possível constatar que o entendimento mais favorável ao titular prevalece quando a Lei Geral de Proteção de Dados, em conjunto com as demais normas, é priorizada. Dessa forma, torna-se evidente que a venda de conjuntos de dados com

o intuito de marketing configura uma circunstância sensível. O curso de ação mais apropriado consiste na plena conscientização e obtenção de consentimento por parte dos titulares, de maneira transparente e inequívoca, antes de ceder os dados a terceiros.

5 SOLUÇÕES E PERSPECTIVAS FUTURAS

No labirinto das questões jurídicas suscitadas pela coleta de informações das *Big Techs*, emerge a necessidade premente de delinear soluções sólidas e vislumbrar as perspectivas que moldarão o cenário futuro. O horizonte encontra-se adornado por desafios que clamam por inovação jurídica e reimaginação conceitual, à medida que as tecnologias avançam e as fronteiras do digital se expandem. Neste âmbito, considerações pragmáticas e reflexões holísticas convergem para esboçar um quadro articulado de respostas e possibilidades.

Por isso, é importante analisar quais aspectos precisam ser melhorados para que o desenvolvimento tecnológico acompanhe a demanda social em ter uma legislação abrangente e eficaz, que proteja a privacidade e os dados pessoais. Essas medidas envolvem: Expansão das regulamentações; consentimento informado e transparente; restrição de objetivo e dados e controles de autodeterminação.

Ampliação das Estruturas Regulatórias: essa aprimoração teria como ênfase regulamentação específica coleta de dados por parte das *Big Techs*. **Consentimento Informado e Transparente:** Fortalecer a importância do consentimento informado dos usuários, garantindo que eles compreendam completamente como seus dados serão utilizados. **Limitação de Finalidade e Minimização de Dados:** Implantar princípios de limitação de finalidade e minimização de dados, restringindo a coleta apenas ao necessário para alcançar um objetivo específico, reduzindo a exposição excessiva dos usuários e mitigar riscos de abuso. **Controles de Autodeterminação:** Desenvolver ferramentas e interfaces que concedam aos usuários maior controle sobre suas informações pessoais.

As perspectivas que permeiam o horizonte da coleta de informações pelas *Big Techs* repercutem em miríades de possibilidades intrigantes e desafios complexos. À medida que a interseção entre tecnologia e direito se expande, é imperativo lançar um olhar adiante e traçar as linhas que delinearão o futuro dessa relação em constante evolução. Sob a influência das tendências tecnológicas, das dinâmicas sociais e das demandas por proteção de dados, as perspectivas futuras geram cenários variados que inspiram tanto otimismo quanto cautela.

À medida que as *Big Techs* continuam a redefinir os limites do possível, a próxima fronteira na governança digital surge como um foco crítico. O panorama global exige a articulação de normas e regulamentos que transcendam fronteiras geográficas e se adaptem à natureza transnacional das operações das empresas tecnológicas. A colaboração internacional para estabelecer diretrizes claras e consensuais para a coleta e o uso de informações pessoais emergirá como uma peça central na busca pela harmonização regulatória. As perspectivas apontam para a formação de alianças intergovernamentais que compartilhem conhecimentos, experiências e melhores práticas, criando um terreno fértil para a consecução de uma governança global eficiente (“Participação da ANPD no cenário internacional e a regulamentação de transferências internacionais de dados pessoais”, 2022).

Ao passo que a tecnologia se entrelaça mais profundamente na vida cotidiana, a humanização da tecnologia surge como uma perspectiva intrigante. A integração da ética no desenvolvimento de algoritmos e sistemas torna-se uma exigência moral e uma abordagem prática para mitigar os riscos associados à coleta de informações. A exploração de inteligência artificial orientada por valores humanos, respeitando a dignidade e a privacidade dos indivíduos, redefinirá as práticas das *Big Techs*. A perspectiva de uma tecnologia mais compassiva e consciente abre caminho para a restauração da confiança pública e para uma coexistência harmoniosa entre a tecnologia e a sociedade (“Ética e Inteligência Artificial: qual a importância dessa relação?”, 2023).

As perspectivas futuras também apontam para a emergência de novos paradigmas na proteção de dados. O conceito de autodeterminação informacional ganhará destaque à medida que os indivíduos buscam um controle mais ativo sobre suas informações pessoais. Mecanismos inovadores, como a portabilidade de dados e a exclusão, empoderarão os usuários a participarem ativamente da gestão de suas pegadas digitais. A capacidade de transferir dados de uma plataforma para outra e de remover permanentemente informações pessoais de sistemas digitais será central na reinvenção das relações de poder entre os indivíduos e as empresas (Brasil, 2018).

Uma série de fatores integrados são necessários para a evolução dos padrões referentes ao tratamento de dados individuais e seu compartilhamento, como, modelo de governança global, jurisprudência evolutiva, *blockchain* e descentralização, e educação e conscientização (Borelli, 2021).

Modelos de Governança Global: A crescente interconexão global exige um olhar atento para modelos de governança que transcendam fronteiras. A colaboração internacional na formação de padrões e diretrizes poderia harmonizar a abordagem regulatória, evitando

inconsistências e lacunas. Jurisprudência Evolutiva: À medida que litígios relacionados à proteção de dados se acumulam, a jurisprudência se desenvolverá, contribuindo para a construção de um corpo normativo mais sólido e coerente. Blockchain e Descentralização: poderão fornecer soluções descentralizadas para o armazenamento e o compartilhamento de dados poderia revolucionar a forma como as informações são coletadas e gerenciadas. Educação e Conscientização: Investir em programas de educação e conscientização para capacitar os indivíduos a compreender seus direitos e riscos é fundamental para uma participação informada.

Esses elementos integrados garantem a tutela aos direitos metaindividuais de proteção de dados. Metaindividuais pois são direitos coletivos ou difusos, os quais se referem a prerrogativas que transcendem os interesses pessoais, abrangendo grupos amplos com interesses comuns. Também possuem caráter fundamental uma vez que visam equilibrar o avanço tecnológico com a preservação das liberdades individuais, garantindo que os dados pessoais sejam tratados com responsabilidade (Sampaio, 2020).

Desse modo, para que a perspectiva futura seja positiva a adoção dessas medidas devem começar a ser implementadas, de forma gradativa, a fim de que a tecnologia e humanidade possam conviver em harmonia, com respeito à ética e às relações interpessoais.

CONCLUSÃO

Ao concluir esta análise sobre a coleta de informações realizada pelas *Big Techs* e sua intrincada interação com o direito fundamental à proteção de dados, emergem reflexões profundas e projeções cautelosas para o cenário que se desenha no horizonte. A exploração meticulosa das nuances jurídicas e tecnológicas delineou um panorama rico em desafios e oportunidades, oferecendo insights perspicazes para a convergência desses dois domínios complexos.

A contextualização aprofundada proporcionada pela perplexidade inerente à discussão revelou a essência das questões subjacentes. A interface entre as demandas de inovação tecnológica e a salvaguarda dos direitos individuais tem gerado debates vigorosos, exemplificados pelas complexas ramificações das estruturas regulatórias. As ampliações legislativas específicas, com um foco na coleta de dados por parte das *Big Techs*, se destacam como uma resposta tangível às intrincadas operações dessas empresas. O fortalecimento das

entidades de supervisão, responsáveis pela aplicação efetiva das regulamentações, atua como um contraponto necessário às inovações tecnológicas em um ambiente em constante evolução.

O advento da governança digital transnacional assume um papel crucial para regular os fluxos de dados globalizados. As alianças internacionais emergem como uma resposta à necessidade de harmonização regulatória e compartilhamento de expertise. A humanização da tecnologia, com uma ênfase renovada na ética por *design* e na consideração dos valores humanos, aponta para uma mudança de paradigma, onde a tecnologia é concebida para servir a humanidade com integridade e responsabilidade.

A reconfiguração dos paradigmas de proteção de dados desencadeia um empoderamento inédito dos indivíduos. O enfoque na autodeterminação informacional, com mecanismos como a portabilidade de dados e a exclusão, restitui o controle aos titulares de dados em um ambiente caracterizado pela fluidez das informações.

Ao atar esses fios complexos em uma conclusão coesa, reitera-se que o diálogo entre a coleta de informações pelas *Big Techs* e o direito à proteção de dados não é meramente um exercício acadêmico. É um convite à ação colaborativa e multidisciplinar, onde a sabedoria normativa, as inovações tecnológicas e os valores humanos se entrelaçam para pavimentar um caminho viável em direção a uma coexistência benéfica entre a tecnologia e a sociedade. À medida que se tece essa narrativa, é incontestável que a trajetória adiante será caracterizada por desafios deslumbrantes e oportunidades incalculáveis, destacando a necessidade de uma abordagem holística e progressiva para enfrentar as adversidades dessa jornada complexa e empolgante.

REFERÊNCIAS

Azevedo, Alexandre. Você sabe qual é a quantidade de dados gerados a cada minuto? **Aunica**, [S.l.], 25/08. Disponível em: <https://aunica.com/artigos/domo/infografico-dados-gerados-domo/#hs-chat-open>. Acesso em 8 ago. 2023.

Alves, Paulo. O que são cookies? Entenda os dados que os sites guardam sobre você. **Tech Tudo**. 4 out. 2018. Disponível em: <https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml>. Acesso em 15 ago. 2023.

A nova aposta das big techs: Inteligência Artificial na geração de anúncios. **Pixeld**. 2023. Disponível em: <https://pixeld.news/ia-na-geracao-de-anuncios/>. Acesso em 5 ago. 2023.

Big Techs Na Mira: Entenda As Investigações Antitruste. **The Game**. 2021. Disponível em: <https://thegamecollective.com.br/blogs/tech/big-techs-na-mira-entenda-as-investigacoes-antitruste>. Acesso em 12 ago. 2023.

Brasil, **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm . Acesso em: 11 ago. 2023.

Brasil, **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 11 ago. 2023.

Borelli, Alessandra et al. **Lei Geral de Proteção de Dados Pessoais Comentada**. 3. Ed. São Paulo: Revista dos Tribunais. 2021.

Como a mineração de dados pode ser importante para a empresa? **Positivo Tecnologia**. 9 ago. 2023. Disponível em: <https://www.meupositivo.com.br/panoramapositivo/mineracao-de-dados/>. Acesso em: 17 ago. 2023.

Cuofano, Gennaro. O Guia Completo Do Modelo De Negócios De Assinatura. **FourWeekMBA**. 2023. Disponível em: <https://fourweekmba.com/pt/modelo-de-neg%C3%B3cios-de-assinatura/>. Acesso em: 22 ago. 2023.

Cf., por todos, Chiedermaier, Stephanie. Einleitung. In: Simitis, Spiros; Hornung, Gerrit; Spiecker Genannt Döhmann, Indra (Coord.). *Datenschutzrecht*. Baden-Baden: Nomos, 2019. p. 201

Doneda, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 15 ago. 2023.

Ética e Inteligência Artificial: qual a importância dessa relação? **Engineering**. 2023. Disponível em: <https://blog.engdb.com.br/etica-e-inteligencia-artificial/>. Acesso em 19 ago. 2023.

Guitarrara, Paloma. O que são big techs? **Brasil Escola**. Disponível em: <https://brasilecola.uol.com.br/o-que-e/geografia/o-que-sao-big-techs.htm>. Acesso em 27 de agosto de 2023.

GDPR: entenda o que é o Regulamento Geral de Proteção de Dados. **DocuSign**. 20 dez. 2018. Disponível em: <https://www.docusign.com.br/>. Acesso em: 13 ago. 2023

Instagram: Data Policy. Instagram Help Center. **Help Instagram**. Disponível em: <https://help.instagram.com/155833707900388>. Acesso em 30 jul. 2023.

Jovelino, Luiz. Congresso norte-americano é pressionado para retomar projeto que limita coleta de dados pelas Big Techs. **BL Consultoria Digital**. 10 out. 2022. Disponível em: <https://blconsultoriadigital.com.br/coleta-de-dados-big-techs/>. Acesso em 10 ago. 2023.

Martinez, F.P.; Wurzius, J.F. A comercialização de banco de dados para fins de marketing sob a óptica da LGPD. **Migalhas**. 2022. Disponível em:

<https://www.migalhas.com.br/depeso/370491/a-comercializacao-de-banco-de-dados-para-fins-de-marketing>. Acesso em 15 ago. 2023

Privacidade Hackeada. Direção: Karim Amer e Jehane Noujaim. **Netflix, The Others. Europa**. 2019.

Política de Dados do Instagram: um guia simplificado. **Blog do Instagram**. Disponível em: <https://about.instagram.com/pt-br/blog/announcements/instagram-community-data-policy>. Acesso em 3 ago. 2023.

Participação da ANPD no cenário internacional e a regulamentação de transferências internacionais de dados pessoais. **Gov.Br**. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/semana-da-protacao-de-dados-2022/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais>. Acesso em 20 ago.2023.

Quintiliano, Leandro. Posso vender meus dados pessoais? O resgate da doutrina da privacidade como propriedade. **Migalhas**. 2022. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protacao-de-dados/377587/posso-vender-meus-dados-pessoais>. Acesso em: 11 ago. 2023.

Ripari, César. Por que dados são considerados o novo petróleo? **Administradores**. 15 mar. 2022. Disponível em: <https://administradores.com.br/noticias/por-que-dados-sao-considerados-o-novo-petroleo>. Acesso em 20 ago. 2023.

Sampaio, Vinícius. **Proteção de dados pessoais**: da privacidade ao interesse coletivo. Rio de Janeiro. Lumen Juris. 2020.