UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
PROGRAMA DE GRADUAÇÃO NOTURNO
DEPARTAMENTO DE DIREITO PRIVADO
TRABALHO DE CONCLUSÃO DE CURSO
JOÃO LUCAS ATAIDE PERDIGÃO

RESPONSABILIDADE CIVIL DAS *BIG TECHS* E A PROTEÇÃO DOS DADOS PESSOAIS

FORTALEZA - CE

2024

JOÃO LUCAS ATAIDE PERDIGÃO

RESPONSABILIDADE CIVIL DAS BIG TECHS E A PROTEÇÃO DOS DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientadora: Profa. Fernanda Cláudia Araújo da Silva

Fortaleza

2024

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

P485r Perdigão, João Lucas.

RESPONSABILIDADE CIVIL DAS BIG TECHS E A PROTEÇÃO DOS DADOS PESSOAIS / João Lucas Perdigão. – 2024.

40 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2024.

Orientação: Profa. Ma. Fernanda Cláudia Araújo da Silva.

1. Big Techs. 2. LGPD. 3. Dados Pessoais. I. Título.

CDD 340

JOÃO LUCAS ATAIDE PERDIGÃO

RESPONSABILIDADE CIVIL DAS BIG TECHS E A PROTEÇÃO DOS DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado ao Programa de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Aprovada em: __ / __ / ____.

BANCA EXAMINADORA

_____

Profa. Fernanda Cláudia Araújo da Silva (Orientadora)
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Sidney Guerra Reginaldo
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. William Paiva Marques Júnior
Universidade Federal do Ceará (UFC)

Aos meus pais, Thais e Thiago, e minha pequena irmã, Maria Clara

AGRADECIMENTOS

À Prof. Fernanda Cláudia Araújo da Silva, pela excelente orientação e suporte nessa jornada árdua até a conclusão deste estudo e pela paciência com minhas dificuldades.

Aos professores participantes da banca examinadora Prof. Sidney Guerra Reginaldo e Prof. William Paiva Marques Júnior pelo tempo, pelas valiosas colaborações e essenciais sugestões.

À Universidade Federal do Ceará pela oportunidade e estrutura que proporcionou meu aprendizado até este momento.

Aos colegas da turma de graduação pela inspiração e apoio na confecção deste trabalho de conclusão.

"Privacidade não é opcional e não deveria ser o preço que aceitamos para apenas entrar na internet" (Kovacs G., Gary Kovacs: Rastreando os perseguidores, 2012).

RESUMO

Realizou-se uma análise e exploração didática sobre o papel da legislação brasileira na responsabilização e controle das grandes corporações tecnológicas, as *Big Techs*, na manipulação de dados pessoais de seus usuários, tal como nomes, *e-mails* ou endereços, bem como uma reflexão sobre a Lei Geral de Proteção de Dados(LGPD), a principal lei que rege o uso e coleta de dados pessoais; com o objetivo principal de estudar a eficácia destas medidas regulamentares. Além de expôr os perigos do uso indevido de tais dados e apontar caminhos a serem tomados para o aprimoramento da proteção dos dados pessoais. Por meio da reflexão da evolução histórica da privacidade como direito fundamental e através de uma pesquisa qualitativa com revisão bibliográfica de um assunto que assume um viés contemporâneo de relevância, este estudo apresenta a problematização do uso e venda de dados pessoais na era digital e discute como o processo legislativo luta para protegê-los. Apresenta-se uma conclusão dedutiva a respeito do estado atual da legislação brasileira frente às inovações tecnológicas das *Big Techs* e propõe novas medidas a serem tomadas para a conscientização da população do risco de seus dados na rede e como o processo legislativo pode evoluir para acompanhar os avanços digitais.

Palavras-chave: *Big Techs*; LGPD; Dados pessoais.

ABSTRACT

This undergraduate thesis was a didactic exploration and analysis of the Brazilian legislative's role on the regulation and accountability of "Big Techs" in reference to their manipulation of users' personal data, such as names, emails and addresses, as well as a reflection on Brazil's Lei Geral de Proteção de Dados (General Data Protection Law), the main law that rules the use and acquiring of personnel data, with the objective of studying it's regulatory efficacy and to expose the dangers of the misuse of such data, and presenting methods to upgrade its protection. Through analysis of the historic evolution of privacy as a fundamental right and research, aided by a qualitative research and bibliographic review of a topic with such a contemporary relevance, this thesis presents the recently emerging problem of the misuse and sale of personal data during the digital era, and discusses how the legislative process fights to protect it. By the conclusion this thesis will have covered the current state of Brazil's legislation towards Big Techs' technologic innovations, and will have proposed new ways to raise the population's awareness of their data on the web as well as how the legislative process could evolve to more closely follow these digital innovations.

Keywords: Big Techs; LGPD; personal data.

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados
BigTech	*Big Technological Companies* (Trad. Grandes Corporações de Tecnologias)
IBGE	Instituto Brasileiro de Geografia e Estatística
GDPR	*General Data Protection Regulation,* (Trad. Regulamento Geral de Proteção de Dados)
DNS	*Domain Name System* (Trad. Sistema de Nome de Domínios)
ONU	Organização das Nações Unidas
UE	União Europeia
MP	Medida Provisória
ANPD	Autoridade Nacional de Proteção de Dados
IA	Inteligência Artificial

SUMÁRIO

1 INTRODUÇÃO

O século XXI é marcado pela revolução digital, a vida da maior parte da população terrestre tornou-se profundamente integrada ao meio virtual, pessoas se conhecem e conversam pelas redes sociais e profissionais trabalham através de plataformas virtuais de cooperação. Neste contexto, o ser humano integrou-se ao meio digital parte de sua vida cotidiana, mas esta realidade paralela possui seus monarcas, as *Big Techs*, estas grandes corporações possuem domínio hegemônico sobre suas áreas de atuação no plano virtual, como a *Google* sendo o mecanismo de pesquisa mais comum e o *Facebook* como uma das rede sociais mais utilizadas.

Em uma era dominada pela tecnologia, as grandes corporações descobriram uma nova fonte de riquezas pronta para exploração e comercialização: os dados pessoais de seus usuários.

Com cerca de 164,5 milhões de brasileiros conectados em 2023[1], muitos já foram alvo de coletas de dados por meio do cadastro em páginas virtuais ou pela mera presença digital em redes sociais e profissionais *online.* Embora seja uma prática já regulada pela Lei Geral de Proteção de Dados (2018), a maior parte da população usuária de *internet* não possui consciência do que concordam quando rendem seus dados pessoais às *Big Techs*, inocentemente aceitando riscos a não somente sua privacidade, como também sua honra e segurança no mundo real.

Nas mãos erradas, tais informações pessoais podem ser utilizadas para compilação de perfis completos a respeito do indivíduo, personalização de notícias e propagandas específicas para o mesmo com o objetivo de manipulá-lo ao consumo desenfreado ou até mesmo influenciar opiniões políticas de milhões de usuários, pondo poder excessivo nas mãos de um punhado de empresas de tecnologia.

O objetivo principal deste trabalho é demonstrar o perigo que as *Big Techs* apresentam decido a coleta e uso indevido de dados pessoais; gerar conscientização sobre os perigos que aguardam o povo brasileiro decorrentes dos avanços tecnológicos iminentes, propondo um aprendizado a respeito deste tema moderno; além de demonstrar caminhos futuros a serem seguidos pela legislação de tal forma que possa acompanhar a evolução digital desenfreada presente na atual década.

---

[1] **Em 2023, 88,0% das pessoas com 10 anos ou mais utilizaram Internet.** 2024 https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet. Acesso em 19 Set 2024

O presente trabalho trata de um assunto multidisciplinar e relativamente recente na história da humanidade, então realizou-se uma pesquisa qualitativa a partir de notícias de grande meios de comunicação, análise da legislação relativa ao assunto e a revisão bibliográfica de material doutrinário jurídico brasileiro, além de artigos publicados por outros pesquisadores da área, muitos de trabalhos estudantes da área.

Por meio do método dedutivo, partiu-se das ideias como a importância da privacidade, o perigo de dados pessoais nas mãos de corporações, a carência de legislação para novas tecnologias, de forma que partir daí analisou-se o ordenamento jurídico contemporâneo para apontar os próximos passos a serem tomados pelo poder legislativo.

Buscou-se, no primeiro capítulo, realizar uma exploração geral dos aspectos básicos pertinentes ao tema, desde a exploração do progresso histórico da evolução do direito à privacidade como direito fundamental humano até os avanços mais recentes da legislação brasileira, como a Lei Geral de Proteção de Dados.

No capítulo seguinte há a definição do conceito de *Big Techs,* levando à análise do valor atribuído aos dados pessoais coletados de usuários, além de como tais informações são armazenadas, processadas e utilizadas em benefício das grandes empresas digitais, contando os riscos às liberdades individuais e o impacto social causado.

No último capítulo encerra-se a trabalho concluindo a reflexão a respeito da responsabilidade das *Big Techs* com dados pessoais coletados, como sua regularização e monitoramento pelos órgãos governamentais contribuem para a segurança da população, uma reflexão dos avanços tecnológicos recentes e como os mesmo devem ser tratados pela legislação, e por fim sugestões para medidas cabíveis para a conscientização populacional da importância da proteção de dados pessoais digitais, além de incentivar pesquisas futuras nesta área do direito ainda em desenvolvimento.

2 PROTEÇÃO DE DADOS E PRIVACIDADE: ANTIGUIDADE E MODERNIDADE

A privacidade tornou-se, recentemente, um dos direitos fundamentais mais discutidos, entre vendas de bancos de dados, exposições de dados pessoais em redes sociais e vazamento de informações embaraçosas em fóruns online, vive-se um período dominado por debates a respeito da privacidade do indivíduo em meios analógicos e digitais, mas para analisarmos o presente é necessário estudarmos o passado e entender como a sociedade chegou a tal ponto.

2.1 Evolução histórica

O mero conceito de privacidade e seu valor para sociedade apresentam-se, historicamente, profundamente ligados à luta pelos direitos individuais, de tal forma que podemos traçar as primeiras discussões a seu respeito até o período histórico clássico.

No imaginário clássico, Homero já evidenciava em sua obra "Odisseia" a importância da proteção da identidade do indivíduo, uma vez que seu protagonista Odisseu, conhecido por sua vitória na guerra de Tróia e seu título "Herói dos mil estratagemas", após enganar os ciclopes ao identificar-se como *Outiç*[2]*,* "Ninguém" e fugir de suas garras, foi orgulhoso ao ponto de gritar seu nome verdadeiro para provar sua superioridade e assim foi identificado pelo deus *Poseidon* e punido a vagar pelos mares por anos, demonstrando que o valor da proteção de identidade já estava no imaginário humano muito antes de aparecer nas constituições.

No plano terreno, os filósofos gregos já debatiam a respeito da separação da figura do cidadão quanto à política na *polis* (cidade) e seu círculo familiar privado, separando-os no tocante a sua utilidade, buscando compartilhar o que seria de uso público e mantendo recluso o restante. Pensadores e filósofos da época como Aristóteles entendiam o meio social privado e familiar precedendo o político da cidade, seguindo a ideia de que o homem seria um "animal político", pois após reunir-se em uma família, o homem buscaria tecer uma teia social ainda mais complexa e formaria relações sociais entre famílias distintas, o que levaria a formação de vilarejos e eventualmente às grandes cidades, mas ainda respeitando o seio privado da família.

---

[2] Homero, **Odisseia**,tradução e prefácio por Carlos Alberto Nunes. - [25. ed.] - Rio de Janeiro : Nova Fronteira, 2015., Disponível em:https://prioste2015.wordpress.com/wp-content/uploads/2015/03/homero-odisseia-trad.-carlos-alberto-nunes.pdf, pg 108

Na era romana, houve uma continuação do pensamento grego, uma vez que se via o conceito de "privacidade" de forma utilitarista, a separação entre a realidade pública e a pessoal se distinguia a partir de o que era de utilidade comunitária e o que era de uso e importância pessoal; além do seguimento de que a esfera pessoal deveria se curvar à pública, de forma que a figura do indivíduo ainda deveria estar disponível para a sociedade, uma vez que o conceito de privacidade da época ainda diferenciava-se do contemporâneo.

Foi apenas na Revolução Francesa que surgiu uma das principais fontes de direitos fundamentais na forma da "Declaração dos Direitos do Homem e do Cidadão de 1789", legislando a respeito da privacidade com a adição da dignidade como direito garantido constitucional, tal ideal advindo do iluminismo uma vez que buscavam os direitos pessoais do indivíduo frente às instituições públicas, uma reviravolta do caminho que vinha sendo trilhado na antiguidade clássica, mas que serviu de pontapé essencial para a formalização da privacidade como direito fundamental humano.

O entendimento moderno da privacidade no campo jurídico é, principalmente, advindo do artigo publicado no periódico *"Harvard Law Review*" em 15 de Dezembro de 1890, *"The Right to Privacy"* (O Direito à Privacidade), produzido pela dupla de advogados estadunidenses Samuel Warren e Louis Brandeis (1890), motivados principalmente pela cobertura sensacionalista e invasiva das festas e relações pessoais de Warren após seu casamento com a filha de um senador virar manchete local, além de publicações incluindo descrições dos corpos de sua irmã e mãe em seus respectivos velórios.

Já no começo de seu artigo, Warren e Brandeis deixaram claro o foco histórico atribuído às proteções individuais e evidenciaram a necessidade do constante avanço da *common law* em busca de adaptar-se às necessidades modernas do homem, e partiram em busca de produzir um dos materiais doutrinários mais importantes a respeito da conceituação jurídica da privacidade do indivíduo.

> Que o indivíduo deve ter plena **proteção pessoal e patrimonial** é um princípio tão antigo quanto o ***common law***; mas tem sido considerado necessário, de tempos em tempos, **definir novamente** a natureza exata e a extensão de tal proteção.(Warrens e Brandeis, 1890)

É de suma importância também ressaltar o contexto no qual os advogados em questão construíram os 'ossos' da doutrina a respeito da privacidade moderna, uma vez que em meados do século XIX ocorreu o invento da captura fotográfica instantânea, criação que permitia eternizar visualmente qualquer acontecimento que o fotógrafo testemunhasse e sua

subsequente publicações em meios de notícia da época, fato que possibilitou a exploração comercial de materiais pessoais embaraçosos ou de cunho sentimental ao indivíduo.

> … A imprensa está ultrapassando em todas as direções os limites óbvios do **decoro e da decência**. **A fofoca** não é mais o recurso dos ociosos e dos viciosos, mas **tornou-se um comércio**, que é praticado com diligência e descaramento. Para satisfazer um gosto lascivo, os detalhes das relações sexuais são **divulgados** nas colunas dos jornais diários. Para ocupar os indolentes, coluna após coluna está cheia de fofocas ociosas, que só podem ser obtidas por **intrusão no círculo doméstico**…(Warrens e Brandeis, 1890)

Em seu artigo, Warrens e Brandeis demonstraram as lacunas que a *common law* da época tinha a respeito da proteção da privacidade e como a mesma era analisada pelos juízes da época, e citam casos em que tribunais tiveram que estender os conceitos da época quanto à propriedade privada para abarcar casos envolvendo a publicação de cartas pessoais, que uma vez entregues já não pertenceriam ao seu emissário e não seriam consideradas sua propriedade privada, mas sua seguinte exposição poderia levar a danos à reputação e perturbação da "paz mental", tais casos levaram juízes a cunhar julgamentos que foram fundamentais para a consolidação do conceito de privacidade jurídica no sistema norte-americano.

> …**A proteção** conferida aos pensamentos, aos sentimentos e às emoções, expressos por meio da escrita ou das artes, na medida em que consiste em impedir a publicação, é apenas uma i**nstância de aplicação do direito** mais geral do **indivíduo ser deixado em paz**... (Warrens e Brandeis, 1890)

Após os horrores vivenciados nas duas guerras mundiais pelos soldados, prisioneiros e até a população civil global, os países vitoriosos uniram-se na forma da Organização das Nações Unidas e promoveram em 10 de dezembro de 1948 a "Declaração Universal dos Direitos humanos", documentação que marca o reconhecimento dos direitos fundamentais humanos, inclusive prevendo a garantia do respeito à privacidade como direito humano em seu 12º artigo, vide:

> Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques à sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques. (Declaração Universal dos Direitos Humanos, Artigo 12, 1948)

Embora seja apenas uma declaração e não um pacto com vínculo de obrigatoriedade, a Declaração Universal dos Direitos Humanos foi de suma importância para

a formalização do similar Pacto Internacional dos Direitos Civis e Políticos, este sim possuidor de caráter vinculativo jurídico e que também resguarda a garantia a segurança e respeito da vida privada dos países que o assinaram.

> 1. Ninguém será objeto de ingerências arbitrárias ou ilegais em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques ilegais à sua honra e reputação.
> 2. Toda pessoa tem direito à proteção da lei contra essas ingerências ou esses ataques. (Pacto Internacional dos Direitos Civis e Políticos, Artigo 17, 1966)

Toda essa sequência histórica explorada veio a culminar na formação jurídica brasileira atual, que além de beber de diversas fontes estrangeiras à respeito da caracterização como direito fundamental da privacidade do indivíduo, vivenciou seu próprio período de autoritarismo durante a Ditadura Militar entre 1964 e 1985, onde testemunhou-se no próprio solo nacional os riscos que a população corre quando seus direitos fundamentais não são garantidos por um regime autoritário, criando um período de invasões à propriedade e privacidade individual.

As reflexões sobre legislações estrangeiras e tratados internacionais somados à experiência da perda de direitos fundamentais decorrente do autoritarismo governamental culminaram na concepção da "Constituição da República Federativa do Brasil de 1988", regimento de caráter fundamental para o ordenamento jurídico brasileiro moderno, e que já continha em seu arcabouço original a garantia de respeito e segurança da intimidade e vida privada do cidadão brasileiro, que junto à doutrina influenciada pelos estudo estrangeiros, levaria à exploração das ramificações da proteção da privacidade em outros galhos da árvore jurídica, como o Direito Civil com a inviolabilidade da Vida Privada, e o Direito do Consumidor a respeito da proteção e esclarecimento do uso de dados e informações pessoais no vínculo entre o consumidor e o fornecedor.

> Art. 5º - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> *omissis*

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (Constituição da República Federativa do Brasil de 1988. Planalto. 1988)

2.2 Dados pessoais: a privacidade no ambiente digital

> "Muitos pensam que só as celebridades são alvo de paparazzi, quando na verdade você é a grande estrela do show" (Autor desconhecido)

A civilização humana avançou da entrega de pergaminhos por corredores à mensagem instantânea por *SMS;* de publicações impressas de notícias em jornais matinais à blogs atualizados a cada minuto, evoluiu de uma sociedade baseada em relações entre vilarejos e nos tornamos uma civilização global de comunicações e comércio ao redor do mundo, se antes dessa conectividade mundial o indivíduo poderia ser conhecido na sua vizinhança, hoje o mesmo está diante de pelo menos 5,3 bilhões de pessoas conectadas à *internet*, de acordo com a Organização das Nações Unidas em 2022[3], uma plateia de grandeza inédita, e é nessa "vila digital" de bilhões onde os humanos vivem a cada dia mais atrelados à *internet*, seja para aprendizado por meios de classes ao vivo por chamadas de vídeo em grupo, ou empregos à distância por meio de plataformas de cooperação online.

Com a crescente popularização da *internet*, viu-se também a oportunidade de formar conexões sociais fora ao profissionalismo, dando surgimento às redes sociais, plataformas de socialização em massa em um grau nunca antes visto, onde usuários costumam postar mensagens de alcance global e publicar vídeos e fotos que anos atrás iriam ser encontrados apenas em albúns e fitas para a visualização restrita ao seio familiar, mas que hoje em dia encontram-se circulando em grandes redes sociais à mostra para que todos possam assistir, pois embora algumas plataformas ofereçam a possibilidade de limitar a visibilidade de tais publicações, ainda corremos o risco de compartilhamentos indevidos desses conteúdos, uma vez que outros usuários normalmente possuem a capacidade de salvar estas mídias em suas próprias máquinas e decidir fins além da vontade original de quem as publicou.

[3] **Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede**. 2022. Disponível em: https://news.un.org/pt/story/2022/09/1801381. Acesso em 19 Set 2024

Tamanho grau de integração com o meio digital requer certo grau de confiança no sistema, uma vez que boa parte das plataformas que o usuário médio utiliza requerem cadastro virtual, geralmente exigindo informações como nome completo, CPF, endereço… Todos os dados pessoais de alto grau, que normalmente são criptografados e armazenados em bancos de dados, definidos pela Lei Geral de Proteção de Dados (LGPD) brasileira em seu 5º artigo como: "(...) conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico."

Estes bancos de dados contendo milhares e milhares de *terabytes* de informações de milhões de usuários são mantidos sob a promessa de segurança nas mãos de grandes empresas de tecnologias, conhecidas atualmente como *Big Techs,* mas conforme adentramos a era digital neste novo milênio, a população foi conscientizando-se a respeito da cibersegurança e atualmente a sociedade encontra-se numa época de constante preocupação com o armazenamento e compartilhamento de nossos dados cadastrais e informações pessoais, incluindo com a segurança envolvida em ambos os processos.

Conforme a sociedade passou a ter consciência dos perigos e riscos envolvidos com o manejo de dados digitais por meio de sites terceiros, as legislações do mundo buscaram adaptar-se às novas necessidades que o meio digital trouxe consigo, diante disso vimos iniciativas governamentais de regular o recolhimento e uso de dados de usuários, bem como apontar diretivas para a proteção dos mesmos.

2.3 Legislação Digital Brasileira

Apontado pela revista Forbes[4] em 2023 como terceiro lugar no *ranking* mundial do número de cidadãos conectados a redes sociais, o Brasil há décadas vem se mostrando um mercado farto e próspero para operações de empresas virtuais e serviços digitais. Em decorrência de uma enorme parcela da população conectada e em busca de fomentar o mercado digital que traria enormes investimentos para o país, autores da doutrina clamavam já na década de 2000 por regulamentações e proteções com relação ao meio digital no código jurídico brasileiro.

Em abril de 2014, houve aprovação e legalização do Marco Civil da *Internet*, que se tornou projeto de lei já em 2011, essencial como ponta-pé inicial para o desenvolvimento

[4] **Brasil é o terceiro maior consumidor de redes sociais em todo o mundo**. 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/. Acesso em 19 Set 2024

virtual do país, uma vez que o mesmo estabeleceu os primeiros princípios, garantias e direitos, além dos deveres, para o uso da *internet* no Brasil, atuando como uma espécie de "constituição" para o ambiente online e regulando as relações entre usuários, provedores de *internet* e o governo, lidando com tópicos como registro de conexões dos clientes, a neutralidade da rede e mais importante: privacidade e proteção de dados, especialmente na "Seção II - **Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas**".

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> III - proteção dos **dados pessoais**, na forma da lei; (Marco Civil, lei Nº 12.965, de 23 de Abril de 2014)

Embora agora o Brasil possuísse legislação específica para lidar com a realidade virtual, casos como o uso de dados, colhidos escusamente, de usuários da rede social americana *Facebook* em 2016 para impulsionamento de propaganda política direcionada e outros casos de vazamento e/ou uso indevidos de dados de cidadãos brasileiros provaram que o Marco Civil ainda possui lacunas quanto ao direito da privacidade digital e a coleta indevida de dados pessoais, o que levou o poder legislativo a compor o Projeto de lei nº 4060/2012 que. em agosto de 2018, seria sancionada como a Lei Geral de Proteção de Dados (LGPD), ou Lei nº 13.709/2018, uma lei complementar ao Marco Civil, que serviu para auxiliar na proteção de direitos como a privacidade, liberdade de expressão, opinião, informação e a inviolabilidade da intimidade, da honra e da imagem.

Inspirados no *General Data Protection Regulation* (GDPR) da União Européia, os legisladores basearam-se nos governos europeus para a composição da LGPD, uma vez que a possui semelhanças profundas com a primeira, tal como o elencamento de princípios que aa regem, a definição básica de Dados Pessoais e os graus de proporcionalidade estipulados nas punições previstas nas mesmas.

Além de alterar artigos do Marco Civil, a LGPD também buscou reagir sobre o gerenciamento e manipulação de dados civis tanto fisicamente quanto virtualmente, além de positivar novos termos jurídicos como a distinção entre Dados Pessoais e Dados Pessoais Sensíveis, um trata de informações básicas como nome completo, telefone, endereço.. Enquanto o último trata de dados de cunho íntimo e de potencial discriminatório ou embaraçoso, como religião, etnia e opinião política.

Para auxiliar a efetividade da LGPD, foi criada através da Medida Provisória (MP) Nº 869, de 27 de Dezembro de 2018, a Autoridade Nacional de Proteção de Dados

(ANPD), uma autarquia federal especial com o objetivo de realizar a fiscalização e impor o cumprimento da LGPD, capaz de acatar denúncias relativas à riscos e crimes de dados no território nacional, além de receber e tratar de comunicados a respeito de incidente de segurança de bancos de dados.

Além de promover o cumprimento das legislações pertinentes, a criação da ANPD como uma autoridade nacional independente de fiscalização fez com que o Brasil estivesse de acordo com o GDPR da União Europeia, tornando o país capacitado para o transacionamento de dados pessoais com países da UE.[5]

2.3.1 Princípios da LGPD

A LGPD, assim como a GDPR, é considerada uma lei principiológica, ou seja, estabelece princípios fundamentais que caracterizam um ramo do direito ou uma área específica de atuação, e ao invés de focar em regras detalhadas e específicas, define os valores gerais que devem orientar a interpretação e aplicação das normas. Como dito pela advogada especialista em direito digital, Patrícia Peck (2018, p.24):

> (A LGPD)...traz um rol de princípios que precisam ser atendidos. A melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não está atendido.

Dentre os princípios descritos pelo Art. 6º da LGPD, observa-se:

I- Finalidade: O tratamento dos dados fornecidos deve ser legítimo, lícito, específico e informado ao titular.

II- Adequação: O tratamento dos dados deve ter sua finalidade informada e esclarecida ao titular.

III- Necessidade: Limitar o tratamento dos dados ao mínimo necessário para realização de suas finalidades.

IV- Livre Acesso: Garantir consulta facilitada e gratuita ao titular dos dados quanto a forma e duração do uso de seus dados.

---

[5] **Brasil precisa de autoridade de dados para se manter próximo do mercado europeu.** 2018. disponível em: https://www.jota.info/opiniao-e-analise/artigos/brasil-precisa-de-autoridade-de-dados-para-se-manter-proximo-do-mercado-europeu, acesso em 19 Set 2024.

V- Qualidade dos dados: Garantir aos titulares a exatidão, clareza e atualizações dos dados conforme necessidade.

VI- Transparência: Garantir aos titulares informações claras sobre a realização do tratamento dos dados, além dos agentes que os manuseiam.

VII- Segurança: Garantir a proteção dos dados manuseados de tal forma que pessoas de acesso não autorizado ou acidentes não ocasionem o vazamento ou destruição dos mesmos.

VIII- Prevenção: Adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

IX- Não Descriminação: Impedir o tratamento de dados pessoais para fins discriminatórios ou abusivos.

X- Responsabilização e prestação de contas: Demonstrar o uso de medidas eficazes para a proteção e cumprimento das normas de proteção de dados pessoais, além de sua eficácia.

Tais princípios são essenciais para o direito digital brasileiro, uma vez que norteiam as relações entre provedores de serviços *online* e os usuários cujos dados são fornecidos e manejados para fins diversos.

2.4 *Big Techs*: definição e problemática

Caracterizado pelo dicionário inglês *Collins English Dictionary*[6] como substantivo "usado para descrever as maiores empresas de tecnologias", o termo *Big Techs* tornou-se profundamente integrado à sociedade moderna devido à consolidação e hegemonia do mercado da *internet* atingida pelas grandes corporações que dominam seus respectivos nichos, como, por exemplo, a *Google* nas ferramentas de pesquisas virtuais, *Meta* com seu domínio do mercado de redes sociais e a *Amazon* no campo de compras online.

Em uma primeira análise, tais pessoas jurídicas do direito privado especializadas em tecnologia podem ser vistas como corporações expansionistas promovendo o melhor serviço possível para o maior público possível online. No entanto, devido ao seu crescimento desenfreado, formação de monopólios no mercado e dificuldade em fazê-las passíveis de normas jurídicas, tornaram-se grandes fontes de dores de cabeça para juristas e políticos do mundo inteiro.

Conforme a sociedade tornou-se cada vez mais próxima com o meio digital, sua imersão no mesmo foi aprofundada, a ponto de inúmeras profissões tornarem-se

[6] https://www.collinsdictionary.com/dictionary/english/big-tech

completamente interligadas a esta realidade paralela, criando uma série de desafios jurídicos e políticos. Por exemplo, como é possível regular as atividades dessas empresas sem sufocar a inovação? Como deve-se proteger a privacidade dos usuários sem impedir o acesso à informação? Em que ponto é possível traçar a linha entre regulamento e opressão?

A submissão da sociedade moderna para com tais *Big Techs* move o equilíbrio da balança de poder entre consumidor e fornecedor na direção das *Big Techs,* levando muitas a acumular capital exorbitante ao ponto de serem avaliadas na casa dos trilhões como a *Google,* empresa estipulada em cerca de 2 trilhões de dólares em 2024 de acordo com o jornal online *Business Insider*; e acumulam influência a ponto de permitir que tenham poder de influência em decisões políticas refletem nas normas e leis criadas para regular-las, incidindo em inúmeros casos de corrupção ativa ou simples desobediência de soberanias nacionais, além da dificuldade de fazer uso da justiça local quando tais corporações possuem sedes em inúmeros países, armazenam seus bancos de dados em diversos servidores e possuem apenas representantes no território local.

Cada vez mais, usuários são exigidos confiar às *Big Techs* seus dados pessoais e íntimos para socializarem em redes sociais compostas por milhões de usuários, a cada dia mais e mais empregos tornam-se dependentes da *internet* para organização dos trabalhadores ou comércios organizados completamente *online*. Embora a legislação atual ajude na proteção de tais dados e na prevenção de seu uso indevido, é necessário analisar o perigo de bancos de dados tão extensos e potencialmente perigosos nas mãos de um punhado de gigantes da tecnologia, para isso é necessário entender como a coleta de dados é feita por eles, verificar o quão efetivas estão sendo as leis atuais e de que modo os governos podem intensificar a proteção do usuário de *internet* e sua privacidade.

3 *BIG TECHS* E O COLHIMENTO DE DADOS PESSOAIS

"Se você não está pagando pelo uso, você não é o cliente, você é o produto sendo vendido", esta icônica frase publicada em 2010 na rede social *Twitter* pelo usuário Andrew Lewis marcou seu tempo como uma reflexão importante sobre o uso da *internet* pelo usuário médio e sua mensagem tornou-se ainda mais evidente uma vez que a sociedade moderna encontra-se, desde a década de 2010, profundamente integrada com a *Internet*, essa relação somada aos números absurdos e crescentes de usuários levou às grandes corporações a descobrir um novo recurso a ser explorado, dados e informações pessoais. Previsto pelo matemático e analista de dados britânico Clive Humby ainda em 2006 com a icônica frase que repercute até hoje "Data is the new oil"[7] (Trad. Dados são o novo petróleo)

Enquanto em um primeiro momento, o colhimento de dados pessoais pelas grandes corporações era pensado inocentemente como uma forma de segurança e autenticidade ao relacionar uma conta digital com o seu nome e suas informações particulares ou ainda como uma conveniência que otimizaria o uso da *internet* por meio de recolhimento e processamento de dados cadastrais que poderiam ser automaticamente preenchidos em qualquer *site* navegado.

Atualmente percebe-se que um verdadeiro mercado de informações digitais formou-se entre as *Big Techs*, cujo bem transacionado é adquirido aos montes a cada momento que um cidadão cadastra-se em um *site* novo ou simplesmente tem seu histórico de navegação gravado por seu *browser* (navegador de *internet*) e enviado aos bancos de dados.

3.1 O quão valiosos são os dados pessoais na *internet* ?

Não é possível associar um valor monetário a um CPF, ou dois nomes completos, o grau de coleta, processamento e venda de dados pessoais e/ou sensíveis está na casa dos milhões devido aos seus inúmeros usos por grandes corporações normalmente requererem uma pletora de dados de diversos usuários para tornarem-se efetivos, por isso as transações normalmente se dão pelo acesso ou exportação de bancos de dados aos terceiros interessados.

---

[7] **Clive Humby**, School of Computer Science, Visiting Professor of Computer and Information Science. Disponível em: https://www.sheffield.ac.uk/cs/people/academic-visitors/clive-humby. Acesso em:19 Set 2024

> Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações. (Doneda, 2011)

Definidos pelo dicionário *Priberam* (s.d., online) como "Conjunto de dados organizados e relacionados, capaz de ser processado por um sistema informático.", bancos de dados são organizações de informações relacionadas, no contexto deste trabalho observa-se os bancos de dados de *Big Techs* alimentados pelos seus usuários, como o *website* de busca *Google* analisando pesquisas e localizações de inúmeros usuários para criar uma correlação entre assuntos e regiões de um país para fornecer resultados mais pertinentes para casos futuros; tal processamento de dados não gera um valor direto e contável, mas sim um lucro potencial às *Big Techs* e por isso o comércio de dados pessoais possui interesse na maior variedade e quantidade de informações pessoais possível e sua valorização depende da fatura de usuários analisados.

3.2 Práticas de Coleta e Uso de Dados pelas *BigTechs*

> A linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas.(PECK, P., 2018, p.25)

Dados pessoais podem ser recolhidos em plataformas virtuais de inúmeras formas, algumas são por meio do fornecimento do próprio usuário, como registros de acesso realizado em *websites* que os armazenam; enquanto outras operam de modo automático, coletando os dados conforme o indivíduo navega, como os *Cookies,* algumas formas são mais transparentes do que outras graças às previsões legais já estabelecidas, outras operam à margem da legislação, extrapolando entendimentos relativos aos princípios estabelecidos pela LGPD, alguns exemplos principais são:

3.2.1 O fornecimento voluntário no Login

Definido pela LGPD em seu Art. 5º, XII como: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", o consentimento como elemento chave da relação entre o agente de

tratamento de dados e usuário já está presente no cadastro em um *website*, o que configura uma forma de rendimento de informações pessoais pois durante o registro em uma rede social, por exemplo, é comum o preenchimento de dados extremamente pessoais como nome completo, número telefônico, gênero, idade e até mesmo fotografias do rosto para composição de um perfil público.

Além de reter perfeitas amostras de identidades inteiras, estas informações coletadas são salvas nos bancos de dados das grandes empresas que gerenciam estes *websites* e normalmente são utilizados pelas mesmas para traçar perfis dos interesses dos seus usuários e direcionar recomendações de amizades próximas ou com interesses em comum.

Os perigos nessa confiança de dados à uma *Big Tech* aparecem no momento em que há um cruzamento de dados entre diferentes sites de uma mesma companhia de tecnologia ou por meio da venda de tais bancos de dados para companhias parceiras, uma vez que as informações cadastrais fornecidas à uma rede social somadas às informações privadas fornecidas à um *website* de perfis profissionais é o suficiente para que técnicos analistas sejam capazes de traçar um resumo da vida de um usuário que mais tarde pode ser utilizado para fins diversos.

Este rendimento de dados mostra seus riscos em casos mais extremos, como citado anteriormente, quando a rede social *Facebook* em parceria com a companhia de pesquisas *Cambridge Analytica*, em 2016, forneceu dados de cerca de 50 milhões de usuários por meio da conexão da rede social com um aplicativo digital desenvolvido pela companhia de análises que previa apenas a coleta de dados pertencentes à usuários que consentiram, porém o aplicativo aproveitou-se de seu acesso e também colheu dados das pessoas presentes nas “listas de amigos” dos usuários originais, trazendo a tona a discussão a respeito da transparência dada pelas *Big Techs* na coleta e uso de dados.

O impacto de práticas indevidas por *Big Techs* é multiplicado pelo tamanho da corporação envolvida, uma vez que o caso acima, embora tenha sido focado na eleições americanas, afetou até mesmo o Brasil pois, segundo nota publicada pelo *Facebook* em sua página na internet em 4 de Abril de 2018, cerca de 443 mil contas brasileiras[8] teriam sido vítimas de uso indevido de dados pessoais da rede social, o que levou o Departamento de Proteção e Defesa do Consumidor (DPDC) a abrir processo administrativo contra a empresa que se chamava na época *Facebook Inc,* atual *Meta*, e citou como embasamento os artigos 4º, caput, I, III e IV; 6º, II, III, IV e VI, art. 18, art. 31; art. 37 e art. 43, todos do Código de

[8]**Facebook admite uso indevido de dados de 87 milhões de usuários, 443 mil no Brasil**. 2018. Disponível em: https://www.bbc.com/portuguese/geral-43646687. Acesso em: 25 Ago 2024

Defesa do Consumidor (CDC) brasileiro.

> Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
> I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo;
> III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores
> IV - educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo;
> (Código de Defesa do Consumidor, LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990.)

3.2.2 Cookies First-party e Third-party na coleta automática

Os *Cookies first-party*[9] (biscoitos de primeira parte) são ferramentas automáticas de *websites* que armazenam, no computador do usuário, informações e dados pessoais ou até mesmo ìntimos que foram utilizados durante seu acesso ao *website,* para que no futuro esses dados sejam lidos novamente pelos *websites* e preenchidos automaticamente para uma maior conveniência. Trata-se de uma ferramenta extremamente prática pois ajuda o usuário a preencher dados cadastrais mais rapidamente nas visitas seguintes a sites já visitados, a realizar *login* automaticamente pois suas credenciais estão salvas, ou auxiliam a filtrar pesquisas futuras com base nas características especificadas anteriormente, porém seu uso requer que o usuário ceda dados pessoais como senhas, nomes e endereços para os *websites,* o que já causa desconforto para aqueles que se preocupam com sua privacidade, afinal, tais informações estarão nas mãos de terceiros.

A problematização maior ocorre com os chamados "*cookies third-party"* (biscoitos de terceiros), estes são ferramentas similares mas cujos dados são acessados por outros *websites,* por exemplo, ao acessar uma rede social, o usuário criaria um *cookie first-party* do próprio site para acompanhar quais notícias e postagens o indivíduo prefere e passa mais tempo observando, o que para muitos já fere sua privacidade, porém também seria criado um *cookie* separado que além de colher estes mesmos dados, também leria quais abas o

[9] **O que são cookies?** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/cookies. 2024. Acesso em: 09 Set 2024

navegador atual teria aberto e levaria adiante estes dados salvos até que o usuário acessasse outro *website* que tem parceria com a rede social anterior e tem autorização para acessar este *cookie*, daí vem o nome de "*cookie* de terceiros".

Os *Cookies Third-party* oferecem um perigo ainda maior à privacidade do usuário médio pois os dados coletados costumam ser ainda mais extensos do que os de *First-party* e fazem parte do comércio de dados pessoas citados anteriormente, uma vez que eles são uma parceria entre o *site* X e Y para que ao acessar X e aderir à estes *cookies* de terceiros, o usuário terá diversos dados pessoais, íntimos e de navegação levados para a análise do *website* Y, que possuirá o potencial de traçar todos os hábitos de navegação e gostos pessoais do usuário, em busca de muitas vezes utilizar estes dados para criar automaticamente propagandas de produtos e estratégias de marketing que serão exibidas para o indivíduo em questão, e serão extremamente precisas para acatar aos interesses do mesmo e assim manipular o usuário ao consumo direcionado.

Ponderado seu potencial útil e equilibrando com o seu perigo, *Cookies* são atualmente uma ferramenta essencial da maioria dos *websites* de qualquer corporação de porte elevado, os dados fornecidos permitem que as empresas possam otimizar seus produtos e aprimorar a experiência dos usuários, mas para isso tanto a legislação estrangeira quanto a brasileira adaptaram-se para lidar com os *cookies,* como no Art. 7º da LGPD: "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular;", além de levar em conta os princípios explícitos pelo mesmo código, para navegar ao longo destas normas, os desenvolvedores de *websites* inventaram os *pop-ups* de aceitação de *Cookies,* as janelas de texto que são abertas ao entrar em um site e pede o consentimento do usuário para o uso de *Cookies,* além de direcionar à página de política de privacidade da empresa, onde o usuário pode analisar como seus dados serão utilizados.

3.3 Incidentes de vazamento de Dados Pessoais

A LGPD é inquisitiva não apenas na regularização da coleta e uso de dados pessoais, mas também na imposição de medidas protetivas no manejo e armazenamento dos mesmos, vide princípio contido em seu 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; (Lei Geral de Proteção de Dados, Lei nº 13.709/2018, de 14 de Agosto de 2018)

Além de prever a responsabilização dos agentes que não utilizam as medidas adequadas para o condicionamento seguro dos dados pessoais adquiridos, durante o tratamento dos mesmos e após o término da relação do usuário.

> Art. 47 - Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.(Lei Geral de Proteção de Dados, Lei nº 13.709/2018, de 14 de Agosto de 2018)

Não limitado aos riscos com o uso indevido de dados pessoais nos meios digitais e do comércio escuso de informações de indivíduos pelas grandes empresas, é preciso estar ciente da existência do perigo do mau gerenciamento e proteção dos dados confiados às *Big Techs*, nos quais bancos de dados expostos são descobertos por *hackers* ou falhas são encontradas na segurança dos mesmos e então todos perfis cadastrados e analisados pelos *websites* são copiados e/ou deletados, não apenas maculando os depósitos de armazenamento de inúmeros usuários, como também criando potencial para o mal uso destes dados por terceiros, uma vez que agora estas informações extremamente pessoais estão à solta na rede mundial.

De acordo com a pesquisa realizada em 2023 pelo Fórum Brasileiro de Segurança Pública e publicada no *website* "Lgpdbrasil.com.br", o Brasil registrou 208 golpes por hora em 2022, uma alta de 37,9% quando comparado a 2021[10], dentre eles, o aumento no número de golpes por meios eletrônicos chama a atenção dos órgãos governamentais, e apontam para o crescente perigo da digitalização de dados pessoais e da carência da aplicação de medidas de segurança adequadas, uma vez que os criminosos utilizam informações compradas provenientes de vazamentos de bancos de dados, tais como nomes completos e relações familiares para traçar golpes cujo grau de detalhes sob conhecimento dos estelionatários leva os cidadãos a crer no que está sendo dito e tornarem-se vítimas.

---

[10] **Brasileiros sofrem 208 golpes por hora; alta é de 37,9%**. 2023. Disponível em: https://www.lgpdbrasil.com.br/brasileiros-sofrem-208-golpes-por-hora-alta-e-de-379/. Acesso em: 30 Ago 2024

3.4 Impacto na sociedade

A quantidade de informações e dados pessoais de usuários sob posse das *Big Techs* traz consigo um maior risco de incidentes de vazamento ou ocasiões de mau uso dos dados providos. Além dos exemplos já mencionados neste trabalho, brasileiros já estão acostumados a receber propagandas de produtos criados e direcionados especificamente com base na "pegada digital" de cada usuário, não apenas uma invasão da privacidade prevista na Constituição, mas também uma forma de manipulação do desejo consumista do indivíduo, uma exploração das necessidades e gostos pessoais do usuário ao ponto de levá-lo a comprar itens ou adquirir serviços desnecessários, o que impede uma *Big Tech* de comércio como a *Amazon* de impulsionar anúncios de suas marcas de bebidas alcoólicas à um usuário que a análise de seus dados apontou que possui tendências de consumo de álcool excessivo?

Casos como o *Facebook* em conjunto com *Cambridge Analytica*, em 2016, demonstram o perigo do uso inapropriado dos dados coletados para fins políticos, o que somado ao poder das redes sociais controladas por *Big Techs*, criam um empecilho para a democracia, uma vez que as grandes empresas possuem um público cada vez maior de usuários passíveis de manipulação política para a propagação dos interesses corporativistas, movendo as massas por meio do impulsionamento de *posts* analiticamente escolhidos para gerar fortes emoções escolhidas, como revolta ou inspiração.

Tal impacto política também aponta para uma possibilidade de risco de segurança nacional[11], uma vez que devido ao seu grande público de usuários conectados, o Brasil passa a tornar-se um possível alvo para a influência estrangeira, uma vez que nenhuma das *Big Techs* comumente citadas são brasileiras e seu objetivo primário é a expansão de seus domínios nos mercados internacionais.

Torna-se evidente que sua capacidade de mover a opinião pública de seus usuários somado ao poderio econômico dessas gigantes da tecnologia tornam estas empresas capazes de enfrentar a soberania nacional e pôr dúvida em decisões jurídicas por meio de impulsionamento de postagens e conteúdos que condizem com qualquer narrativa que elas tenham interesse de incentivar a disseminação no público de um país.

---

[11] O assombroso poder das big techs na economia e na política dos países. 2024. Disponível em: https://jornal.usp.br/articulistas/paulo-feldmann/o-assombroso-poder-das-big-techs-na-economia-e-na-politica-dos-paises/

4 RESPONSABILIDADE LEGAL, MEDIDAS DE SEGURANÇA CABÍVEIS E O FUTURO DO TRATAMENTO DE DADOS PESSOAIS

Esclarecidos não apenas a ameaça da coleta indevida de dados pessoais, os perigos do seu uso impróprio ou vazamento de bancos de dados, é necessário investigar as medidas protetivas e preventivas aplicáveis a tais casos, além de uma análise sobre o risco social de tais práticas e uma estipulação dos passos que ainda são necessários para o avanço da proteção de dados pessoais no Brasil.

4.1 Medidas de Segurança atuais e Transparência

> Garantir que as pessoas/usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para a assegurar a liberdade e a privacidade. (Peck, P. 2018, p. 38)

A LGPD aplica-se a todas as empresas que colhem e lidam de dados pessoais, sejam organizações públicas ou privadas, além de pessoas físicas ou jurídicas, independentemente do meio, seja digital ou analógico e cuja jurisdição da mesma é alvejar empresas que encaixam-se com um dos elementos a seguir, elencados no Artigo 3º da lei em questão:

I- O uso e análise dos dados colhidos ocorrem em território nacional;

II- Possui como finalidade a oferta ou o fornecimento de bens, serviços ou o tratamento de dados de indivíduos localizados no território nacional;

III- Os dados tenham sido coletados no território nacional.

As *Big Techs* são suscetíveis à LGPD uma vez que atuam coletando e utilizando dados pessoais de usuários brasileiros, e por isso estão submissas aos princípios jurídicos da mesma, com especial foco em:

Finalidade: Promove a realização do uso dos dados coletados para propósitos legítimos, específicos, explícitos e informados ao titular, de tal forma que o cidadão possua total conhecimento de como seus dados serão utilizados, além de prever a impossibilidade de tratamento posterior dos dados que seja incompatível com essas finalidades pré estabelecidas.

Transparência: Garante aos titulares dos dados coletados, informações claras, precisas e facilmente acessíveis sobre a forma de recolhimento e uso de tais dados, tal como

os respectivos agentes deste tratamento de informações, observados os segredos comercial e industrial.

Advindo do respeito a estes princípios observou-se, no campo digital, a inovação de *design* com a abertura automática de janelas requisitando o reconhecimento do usuário dos termos de conduta e política de privacidade de *websites* que possuem intenção de absorver dados e traçar históricos de navegação a partir do preenchimento de formulários e/ou a implementação de *Cookies* de monitoramento de atividades *online.*

A legislação brasileira, através da LGPD, prevê sanções administrativas pela quebra de seus princípios, de caráter dissuasivo, em seu Artigo 52, uma forma de desestimular o uso indevido dos dados adquiridos. Tais medidas punitivas possuem diversos graus de incidência pois "O critério de aplicação deverá observar alguns requisitos, especialmente o da proporcionalidade" (Peck, 2018), esta proporcionalidade possui o objetivo de retificar erros de menor impacto, e escalar as punições de tal forma que atinjam as *Big Techs*:

I - A advertência com prazo para adoção de medidas corretivas serve de ferramenta branda para conserto de pequenas falhas e erros de comunicação entre os agentes de tratamento de dados e o titular dos mesmos.

II - A multa simples de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00) por infração, como uma forma de proporcionalmente atingir grandes empresas sem destruir menores.

III- Uma multa similar à anterior, porém aplicada diariamente.

VI - A eliminação dos dados pessoais a que se refere a infração, uma medida de imposição para apagar dados que estão sendo afetados e cuja contínua circulação pode trazer danos ainda maiores ao titular.

XII - A proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados trata-se da forma mais grave de punição aos transgressores, pois prevê a interrupção de suas atividades até segunda ordem.

Todas estas sanções apresentadas são aplicadas pelo órgão responsável após o devido processo legal contra os infratores e levam em consideração fatores como a gravidade da ofensa, reincidência, cooperatividade do agente, além do comprometimento e demonstração de adoções de medidas preventivas da proteção dos dados prevista no inciso II do §2º, do Art. 48 da LGPD, uma forma de incentivar a prevenção contra incidentes de vazamento de dados.

4.2 Desafios Futuros e Tendências

O Brasil, com mais de 164,5 milhões[12] de cidadãos conectadas à *internet,* é considerado um dos grandes epicentros do foco das *Big Techs* devido ao crescente número de usuários no aquecido mercado digital brasileiro, essa atenção traz consigo não somente benefícios como investimentos estrangeiros e ofertas de emprego no mercado digital, mas também novos desafios para os juristas na proteção de dados pessoais, pois o avanço tecnológico das *Big Techs* é acompanhado da chamada "Disrupção digital", um fenômeno de bruscas mudanças na sociedade, no sistema jurídico e no mercado de trabalho atribuído à novas tecnologias.

Um grande "disruptor" moderno trata-se das chamadas "Inteligências Artificiais" (I.A.), programas com capacidade de aprendizado a partir da análise de quantidades massivas de dados, e exportam conteúdo que trata-se da recombinação dos dados alimentados no contexto apresentado, então para que uma I.A. crie um quadro de uma pessoa, ela requer bancos de dados repletos de fotografias de rostos, e para a criação de um texto sobre um tópico específico, esses programas exigem o fornecimento de históricos de conversas e publicações de pessoas reais.

Para alimentar essas I.A.s, as *Big Techs* como *Google* e *Microsoft* estão atualizando os seus termos de privacidade e lentamente adicionando cláusulas que preveem o uso dos dados colhidos de usuários para alimentar os bancos de dados das IAs em desenvolvimento, ao passo em que a ANPD já manifestou-se em prol da proteção de dados digitais contra a *Meta*[13], uma medida preventiva que determina a suspensão imediata do uso de dados pessoais para treinamento de sistemas de IAs nas redes sociais *Facebook*, *Instagram* e *Messenger*, o órgão justificou a decisão com a possível violação dos princípios da LGPD, uma vez que a *Meta* atualizou seus termos de coleta de dados para incluir a cópia de mensagens e textos públicos em suas redes sociais para a composição de bancos de dados, executou esta mudança de forma escusa e não expôs com a transparência devida a finalidade para que seriam utilizados os dados pessoais no treinamento de IAs :

---

[12] **Em 2023, 88,0% das pessoas com 10 anos ou mais utilizaram Internet.** 2024 https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet. Acesso em 19 Set 2024

[13] **Meta é proibida de usar dados de usuários para treinamento de inteligência artificial no Instagram e Facebook**. 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/meta-e-proibida-de-usar-dados-de-usuarios-para-treinamento-de-inteligencia-artificial-no-instagram-e-facebook/. Acesso em: 08 Ago 2024.

> uso de hipótese legal inadequada para o tratamento de dados pessoais; falta de divulgação de informações claras, precisas e facilmente acessíveis sobre a alteração da política de privacidade e sobre o tratamento realizado; limitações excessivas ao exercício dos direitos dos titulares; e tratamento de dados pessoais de crianças e adolescentes sem as devidas salvaguardas. (ANPD, agenciagov.ebc.com.br, 2024)

É, também necessário atentar para o influxo de uma população cada vez mais jovem no meio digital, uma vez que, de acordo com dados do Instituto Brasileiro de Geografia e Estatística (IBGE)[14] de 2023, a proporção de crianças com 10 anos ou mais de idade que utilizaram a *Internet* no país passou de 84,7% em 2021 para 87,2% em 2022, um expressivo aumento do acesso digital infantil no país, o que embora considerado como positivo como indicador de acessibilidade *online* e indicador econômico, traz consigo a problemática do tratamento de dados de usuários infantis.

Embora já previsto no Art. 14 da LGDP, prevendo tratamento especial para com os mesmos, menores de idade ainda são o público mais vulnerável pela inocência e falta de experiência. O acesso prematuro de crianças à *internet* através da aprovação de pais expõe os dados pessoais de uma geração sensível, e que poderá causar problemas no futuro devido o uso indevido de suas informações e vazamento de bancos de dados, prejudicando os jovens no futuro.

4.3 Um futuro com maior segurança

O futuro da segurança de dados encontra-se com os legisladores. Ao considerar todos os riscos apresentados à privacidade no presente e os prováveis perigos no futuro, é evidente a necessidade de uma constante marcha pelo progresso na legislação pertinente à proteção dos dados pessoais e na regulamentação do seu uso pelas *Big Techs,* uma vez que o domínio destas sobre o mercado aumenta a cada dia, por isso é necessário que o Poder Legislativo esteja atento para atualizar a Lei Geral de Proteção de Dados conforme o progresso tecnológico avança.

Em 2024, o Brasil ainda não possui legislação específica relativa ao controle do desenvolvimento e uso de Inteligências Artificiais em território brasileiro, esta nova tecnologia apresenta uma lacuna no direito não apenas de proteção de direitos autorais e propriedade intelectual, como também nos esforços de proteção aos dados pessoais de

[14] https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet

usuários de plataformas cujas informações estão sendo colhidas pelas *Big Techs*, uma vez que a discordância com os termos de conduta que preveem o colhimento de dados para alimentar as IAs resulta no impedimento do acesso ao restante de cada plataforma, potencialmente coagindo milhares de brasileiros que dependem de tais *websites,* para trabalho ou relações sociais, à consentir com o uso de seus dados íntimos para treinamento dessa nova tecnologia.

No tocante ao consentimento de usuários para acessar plataformas digitais, ao acessar qualquer *website* e notar-se diante de uma caixa de texto perguntando se concorda com "os termos de serviço e política de privacidade" apresentados pela empresa, a maioria dos usuários não se dá ao trabalho de analisar os termos em questão, seja por ignorância da importância da proteção de seus dados pessoais, ou porque normalmente estes termos estão em uma outra página que o usuário deve acessar para ler e costumam não apenas estar em um linguajar extremamente profissional e indecifrável pelo cidadão médio, como tendem a ser extensos, uma vez que são escritos por times de advogados de direito digital buscando proteger a empresa de futuros processos; esta distância do usuário com o entendimento de o que ele está consentindo é um ferimento direto ao princípio da transparência da LGPD, requerendo programas governamentais em prol de uma conscientização populacional da importância da proteção de dados pessoais ou um esforço do poder legislativo para criar leis que exijam das empresas uma forma mais didática de explicar suas políticas de privacidade.

CONSIDERAÇÕES FINAIS

O estudo a respeito da responsabilidade das *Big Techs* com os dados pessoais de seus usuários é um tema complexo e multidisciplinar, com implicações significativas para a sociedade, a privacidade e o direito, e após extensa análise não apenas do contexto histórico da privacidade como direito fundamental humano, mas também dos riscos que o uso indevido e o armazenamento inseguro das informações fornecidas por usuários da *internet,* a jornada legislativa brasileira em busca da proteção dos dados pessoais dos cidadãos é vista como um nobre esforço da luta da justiça e soberania nacional contra os avanços tecnológicos e a hegemonia corporativa de grandes empresas digitais.

A privacidade como direito fundamental deve ser protegida na era digital e as *Big Techs* desempenham um papel central nos avanços tecnológicos modernos por meio da coleta e uso de dados pessoais, e é essencial que estas empresas sejam responsáveis e transparentes em suas práticas, por isso legislação deve ser fortalecida para garantir que as *Big Techs* sejam responsabilizadas por violações de privacidade e que os indivíduos tenham os meios para proteger seus dados pessoais por meio do suporte jurídico somado à conscientização dos riscos de render seus dados *online*.

A proteção dos dados pessoais é uma questão complexa que requer a colaboração de governos, empresas e indivíduos. É essencial que todos trabalhem juntos para garantir que a privacidade seja respeitada e que os dados pessoais sejam protegidos, de forma que o ambiente digital torne-se tão juridicamente seguro quanto o físico.

Espera-se que este trabalho tenha contribuído para a compreensão dos desafios relacionados à responsabilização das *Big Techs* com os dados pessoais, além de demonstrar a importância de continuar o debate a respeito da proteção da privacidade digital e o incentivo à mais futuras pesquisas pertinentes à área do direito digital, ramo tão recente da legislação brasileira.

REFERÊNCIAS

161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022. Disponível em: 2023.https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022. Acesso em: 07 Ago 2024

ALVES FERREIRA ,D. A. ; KERR PINHEIRO, M. M. ;MARQUES, R. M. **Privacidade e proteção de dados pessoais: perspectiva histórica.** Repositorio.ufmg.br, 2022. Disponível em: https://repositorio.ufmg.br/bitstream/1843/51713/2/Privacidade%20e%20prote%C3%A7%C3%A3o%20de%20dados%20pessoais%20evolu%C3%A7%C3%A3o%20hist%C3%B3rica%20e%20cen%C3%A1rio%20contempor%C3%A2neo.pdf. Acesso em: 22 Jan 2024.

ARENDT, H. **A Condição Humana.** 10. ed. Rio de Janeiro: Forense Universitária, 2007.

ARISTÓTELES. **A Política.** 2. ed. Bauru: Edipro, 2010 UNIVERSIDADE FEDERAL DO CEARÁ. Biblioteca Universitária.

BRANDEIS, Louis D; WARREN, Samuel D. **"O Direito à Privacidade"**. Tradução de Maria Clara de Souza Seixas e Marcus Seixas Souza. *Revista de Direito Civil Contemporâneo.* São Paulo: v. 38, p. 391-417, 2024.

Brasil é o terceiro maior consumidor de redes sociais em todo o mundo. 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/. Acesso em 19 Set 2024

BRASIL. **Constituição da República Federativa do Brasil de 1988**, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 Jun 2024.

BRASIL. **Lei 10.406, de 10 de janeiro de 2002. Código Civil**. Disponível em: http://www.planalto.gov.br/CCivil_03/Leis/2002/L10406.htm. Acesso em: 21 Jun 2024

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018b. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Disponível em: http://legis.senado.leg.br/legislacao/DetalhaSigen.action?id=27457334. Acesso em: 23 Jul. 2024.

DE SANCTIS JÚNIOR, Rubens José Kirk. **A REGULAÇÃO DAS BIG TECHS NO BRASIL: UM IMPERATIVO DEMOCRÁTICO**. Revista da Seção Judiciária do Rio de Janeiro, v. 28, n. 60, p. 74-100, 2024. Acesso em: 17 Jun 2024

Brasil precisa de autoridade de dados para se manter próximo do mercado europeu. 2018. disponível em: https://www.jota.info/opiniao-e-analise/artigos/brasil-precisa-de-autoridade-de-dados-para-se-manter-proximo-do-mercado-europeu, acesso em 19 Set 2024.

Brasileiros sofrem 208 golpes por hora; alta é de 37,9%. 2023, https://www.lgpdbrasil.com.br/brasileiros-sofrem-208-golpes-por-hora-alta-e-de-379/. Acesso em: 30 Ago 2024

Clive Humby, School of Computer Science, Visiting Professor of Computer and Information Science. Disponível em: https://www.sheffield.ac.uk/cs/people/academic-visitors/clive-humby. Acesso em: 19 Set 2024

Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede. 2022. Disponível em: https://news.un.org/pt/story/2022/09/1801381 . Acesso em: 19 Set. 2024.

DONEDA, D. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], Joaçaba, v. 12, n. 2, p. 91 108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 21 jul. 2024.

DONEDA, D. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 20 ago. 2024.

Em 2023, 88,0% das pessoas com 10 anos ou mais utilizaram Internet. 2024 https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet. Acesso em: 19 Set 2024

Escândalo do Facebook: uso indevido de dados pode ter afetado 443 mil no Brasil. 2018. https://oglobo.globo.com/economia/escandalo-do-facebook-uso-indevido-de-dados-pode-ter-afetado-443-mil-no-brasil-22558696. Acesso em: 12 de Ago 2024.

GDPR: o que é e qual a diferença em relação à LGPD? 2021. Disponível em: https://idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-diferenca-em-relacao-a-lgpd/. Acesso em 19 Set 2024.

Guia de normalização de trabalhos acadêmicos da Universidade Federal do Ceará. Fortaleza: Biblioteca Universitária, 2013. Disponível em: https://biblioteca.ufc.br/wp-content/uploads/2019/10/guia-de-citacao-06.10.2019.pdf. Acesso em: 9 Jun. 2024.

HIRATA, Alessandro. **Direito à privacidade.** Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em 29 Ago 2024.

Homero, **Odisseia**, tradução e prefácio por Carlos Alberto Nunes. - [25. ed.] - Rio de Janeiro : Nova Fronteira, 2015., Disponível em: https://prioste2015.wordpress.com/wp-content/uploads/2015/03/homero-odisseia-trad.-carlos-alberto-nunes.pdf. Acesso em: 19 Set 2024

Kovacs, Garry. **Gary Kovacs: Rastreando os perseguidores.** 2012, Apresentação carregada no Youtube. Disponível em: https://www.youtube.com/watch?v=f_f5wNw-2c0. Acesso em 10 Jun. 2024.

LEITE, Henrique Specian. **A Importância da Privacidade na Internet.** 2016. 61 f. TCC (Graduação) – Tecnologia em Análise e Desenvolvimento de Sistemas, Departamento de Tecnologia da Informação, Faculdade de Tecnologia de São Paulo, São Paulo, 2016. Disponível em: https://monografias.brasilescola.uol.com.br/computacao/a-importancia-privacidade-na-internet.htm. Acesso em: 22 Jun. 2024.

Meta é proibida de usar dados de usuários para treinamento de inteligência artificial no Instagram e Facebook. 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/meta-e-proibida-de-usar-dados-de-usuarios-para-treinamento-de-inteligencia-artificial-no-instagram-e-facebook/. Acesso em: 08 Ago 2024.

RODRIGUEZ, K. **Comparative Analysis of Surveillance Laws and Practices in Latin America**. Necessaryandproportionate.org. 2016. Disponível em: https://necessaryandproportionate.org/comparative-analysis-surveillance-laws-and-practices-latin-america/#credits. Acesso em: 14 Jul 2024.

SIMÕES FRANCISCO, M. F. **Aristóteles enquanto fonte das concepções de espaço público e espaço privado de Hannah Arendt.** 2007. Dissertação – faculdade de Filosofia da Educação, USP, 2007.

Peck, P. **Proteção de Dados Pessoais. Comentários à Lei nº13.709/2018**. 1ed. São Paulo : Saraiva Educação, 2018.

Tech giants may be huge, but nothing matches big data. 2013. Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em: 09 Ago 2024