

OS DESAFIO DOS DIREITOS HUMANOS NA ERA DIGITAL: PROTEÇÃO E PRIVACIDADE EM UM MUNDO CONECTADO

Jéssica Laiane de Oliveira

Graduando (a) em Direito pelo UNIPTAN

e-mail: jessicalaiane99@hotmail.com

Pedro Arruda Júnior

Doutor em Direito

e-mail: pedroarrudajunior@yahoo.com

Resumo: A era digital trouxe inúmeras transformações em nossas vidas, com avanços tecnológicos e uma crescente conectividade global. No entanto, essa nova realidade também apresenta desafios significativos para a proteção dos direitos humanos. Este artigo analisou os desafios enfrentados na era digital, com foco na proteção dos direitos fundamentais e na garantia da privacidade dos indivíduos. O objetivo geral foi examinar os desafios enfrentados pelos direitos humanos na era digital e destacar a importância da proteção da privacidade em um ambiente digital. Posto isso, tem-se como problema de pesquisa a exclusão digital afeta negativamente o exercício de direitos fundamentais, como a liberdade de expressão e o acesso à informação? Concluiu-se, preliminarmente, que os desafios enfrentados pelos direitos humanos na era digital são complexos e multidimensionais. A proteção da privacidade e a segurança cibernética são questões centrais que exigem ações concretas por parte de governos, empresas e sociedade civil. Além disso, é essencial abordar as desigualdades digitais por meio de investimentos em infraestrutura e programas de inclusão digital. Somente através de uma abordagem abrangente e colaborativa poderemos enfrentar os desafios dos direitos humanos na era digital e construir um mundo conectado onde a proteção e a privacidade sejam garantidas.

Palavras-chave: Direitos Humanos, Proteção da privacidade, Era Digital.

INTRODUÇÃO

Na era contemporânea, caracterizada pela rápida evolução tecnológica e pela interconexão global, os direitos humanos enfrentam desafios inéditos e complexos no contexto

digital. A crescente dependência da tecnologia digital trouxe consigo uma série de oportunidades, no epicentro desses desafios encontra-se a crucial questão da proteção e privacidade em um mundo profundamente conectado.

A conectividade digital tem estendido os limites do possível, permitindo comunicações instantâneas em escala global, acesso ilimitado a informações e oportunidades sem precedentes para a colaboração e inovação. No entanto, essa conectividade onipresente tem uma face menos visível, que envolve a coleta massiva de dados pessoais, a vigilância generalizada e a vulnerabilidade crescente com as ameaças cibernéticas. À medida que as fronteiras entre o físico e o digital se desvanecem, surge uma urgente necessidade de avaliar como esses desenvolvimentos impactam os princípios fundamentais dos direitos humanos.

Esses princípios são fundamentais para a dignidade e liberdade de todos, e estão intrinsecamente ligados ao avanço tecnológico. A internet e a proliferação de dispositivos digitais permitiram uma comunicação instantânea, acesso a informações e a formação de comunidades virtuais. Contudo, essa mesma tecnologia também deu origem a desafios que abrangem desde a coleta massiva de dados pessoais até o uso indevido dessas informações.

Um dos principais desafios é a proteção da privacidade em meio à constante troca de dados pessoais. As informações fornecidas voluntariamente pelos usuários em plataformas online muitas vezes são coletadas e utilizadas para fins não autorizados, comprometendo a autonomia e a autodeterminação. A coleta e o processamento de dados pessoais por corporações e governos têm levantado questões sobre consentimento informado, controle individual sobre informações sensíveis e os limites da vigilância digital. Além disso, diante do aumento da aplicação de algoritmos de aprendizado de máquina e inteligência artificial na análise de dados, surgem preocupações éticas relacionadas à discriminação algorítmica e à perpetuação de preconceitos sociais.

Outro ponto crucial é o acesso equitativo à tecnologia e à informação. A exclusão digital amplifica as disparidades socioeconômicas e dificulta o exercício pleno dos direitos humanos, como a educação, a participação cívica, a liberdade de expressão, o acesso à informação e a participação na vida pública. Garantir que todos tenham igualdade de oportunidades e acesso aos benefícios da era digital é um desafio urgente a ser enfrentado.

Tudo isso com o propósito de trazer luz ao seguinte problema de pesquisa: a exclusão digital afeta negativamente o exercício de direitos fundamentais, como a liberdade de expressão e o acesso à informação?

Isto posto, com o objetivo geral deste trabalho foi analisar os desafios enfrentados pelos direitos humanos na era digital e destacar a importância da proteção da privacidade em um

ambiente digital. Para isso, definiu como objetivo específicos: analisar da expansão da tecnologia digital, que vem permitindo uma conectividade global sem precedentes; analisar o direito humano fundamental que é a proteção da privacidade, e a coleta indiscriminada de dados pessoais por parte de empresas e governos que levanta preocupações sobre a vigilância em massa e o uso indevido dessas informações.

Para isso, utilizou-se a análise qualitativa que é definido como aquele em que se busca conhecer o fenômeno ou fato em profundidade, através de descrições, comparações e interpretações (Botelho; Cruz, 2013). Além de utilizar-se como metodologia a pesquisa bibliográfica, assim, como, o proveito de códigos de legislações, além de artigos científicos com o intuito de atualizar, desenvolver o conhecimento do tema.

Diante disso, explorar os desafios dos direitos humanos na era digital, com ênfase na proteção da privacidade e segurança, é de vital importância. Através deste artigo, foi possível examinar os aspectos essenciais dessa temática complexa, avaliando as implicações dos avanços tecnológicos nos direitos fundamentais e destacando a necessidade de abordagens multidisciplinares e colaborativas para garantir que os princípios básicos da humanidade sejam preservados em um mundo cada vez mais conectado.

BREVE DEFINIÇÕES DOS DIREITOS HUMANOS CORRELATO AOS DIREITOS FUNDAMENTAIS, ENFATIZANDO O DIREITO DA PRIVACIDADE

Quando se define os direitos humanos e os direitos fundamentais percebe-se que existe uma conexão intrínseca e uma notável semelhança no aspecto ético e na intenção de salvaguardar a dignidade humana, ao mesmo tempo em que buscam restringir o exercício do poder, conceitos que permeiam ambas as ideias. No entanto, há uma pequena diferença entre esses direitos que se materializa a partir da esfera em que sua proteção é estabelecida. Os direitos humanos englobam os direitos fundamentais que são garantidos internacionalmente. Por outro lado, os direitos fundamentais, como reconhecidos pela doutrina, e que estão protegidos no âmbito das nações individuais. (Enciclopédia Jurídica da PUCSP, 2017, P.1)

Os direitos fundamentais se destacam notadamente dos demais, principalmente pela sua natureza ética e por serem compostos por valores intrinsecamente ligados à dignidade inerente à pessoa humana. Devido a relação da dignidade humana e à influência da mudança de contexto que molda a noção de uma vida digna ao longo do tempo, à análise concreta é necessária para se verificar o respeito a essa dignidade. Diante disso, é mais fácil enxergar as violações a dignidade do que definir o seu conceito em si. (BASTOS, 2002).

Nesse sentido, é possível delinear o conceito de dignidade humana de forma sucinta, ou seja, a dignidade em sua definição é o que tem valor, e quando se trata da dignidade humana o valor da vida humana, o valor do ser humano, desse modo, quando o ser humano é tratado como um objeto pode ser colocado como uma violação aos direitos humanos. Consecutivo com as palavras de Celso Ribeiro Bastos, compreende a relação existente entre a dignidade e o direito humano:

Embora dignidade tenha um conteúdo moral, parece que a preocupação do legislador constituinte foi mais de ordem material, ou seja, a de proporcionar às pessoas condições para uma vida digna, principalmente no que tange ao fator econômico. Por outro lado, o termo “dignidade da pessoa” visa a condenar as práticas como a tortura, sob todas as suas modalidades, o racismo e outras humilhações tão comuns no dia-a-dia de nosso país. Este foi, sem dúvida, um acerto do constituinte, pois coloca a pessoa humana como fim último de nossa sociedade e não como simples meio para alcançar certos objetivos, como, por exemplo, o econômico. **Bastos, 2002, p. 248 e 249.**

Em síntese, é importante destacar as semelhanças e diferenças entre os conceitos de direitos humanos e direitos fundamentais. Em termos de conteúdo e valores éticos, ambos compartilham muitos princípios, apesar de algumas diferenças. Em relação a outros tipos de direitos, existem distinções que tornam a fronteira entre direitos humanos e direitos fundamentais menos rígida. (MATHIAS, Márcio José Barcellos, 2006).

Já que em relação a aplicação os direitos humanos são frequentemente promovidos por organizações internacionais ou sistemas legais nacionais, abrangendo diversas situações, incluindo a questão da nacionalidade. Desse modo, quando se fala sobre a proteção de dados pessoais os direitos humanos e os direitos fundamentais se correlacionam, como o direito à privacidade que é um dos direitos fundamentais mais importantes, que faz parte dos direitos humanos. Ele garante que os indivíduos tenham controle sobre suas informações pessoais, sejam protegidos contra interferências arbitrárias em suas vidas privadas, e tenham o direito de decidir quando e como compartilhar informações sobre si mesmos. (DONEDA, 2000.)

A privacidade também está relacionada à proteção da intimidade, do espaço pessoal, das comunicações e das atividades individuais. Abrangendo assim várias dimensões como a autonomia pessoal, confidencialidade, proteção de dados, dignidade e respeito entre tantas outras dimensões. Assim, além de resguardar a possibilidade de isolamento, o direito à privacidade passa a garantir o controle sobre a circulação de informações e vai mais além, podendo servir como fundamentação à licitude de atos relacionados ao controle do próprio corpo, como o direito ao aborto (DONEDA, 2002, p. 7-8). A privacidade é reconhecida

internacionalmente por meio de documentos como a Declaração Universal dos Direitos Humanos e é incorporada nas constituições de muitos países. Ela é crucial para garantir a liberdade individual, promover o desenvolvimento pessoal e manter um equilíbrio saudável entre as necessidades da sociedade e os direitos individuais.

No livro "Direito à Intimidade e Vida Privada" de José Adércio Leite Sampaio (1998), é explorada a evolução dos direitos de propriedade e liberdade para a consagração dos direitos fundamentais à intimidade e vida privada, incluindo a proteção de dados como parte integrante desses direitos. Sampaio define a vida privada como a capacidade de autodeterminação na própria existência e na definição pessoal, sexual e familiar, e a intimidade, um componente essencial que abrange informações pessoais e o controle destas informações.

Durante o decorrer do século XX, com a proliferação de inovações tecnológicas e a crescente valorização da informação como produto, o acesso a informações privadas tornou-se significativamente mais fácil. A divulgação dessas informações já não estava mais limitada à comunidade local da pessoa envolvida, mas, potencialmente, podia alcançar toda a sociedade. (SAMPAIO, 1998)

Além disso, a privacidade deixou de ser um privilégio restrito, expandindo-se para abranger a sociedade como um todo. Isso culminou na Declaração Universal dos Direitos Humanos (1948), que afirmou que "[...] ninguém sofrerá interferências arbitrárias em sua vida privada". Contudo, foi na última década do século XX que um novo espaço social se abriu, dando início à coletivização de dados e revolucionando mais uma vez as formas de comunicação e interação da sociedade. Isso impulsionou a circulação de informações para o mundo digital, graças à criação da internet.

A internet inaugurou uma nova plataforma para diálogos, transformando e ampliando as maneiras de interagir, além de proporcionar acesso a uma quantidade virtualmente infinita de informações. A sociedade passou a viver em constante conexão, e concordando com a definição de Greenwald (2014, p. 15), que afirma que "a internet não é apenas um meio de comunicação, como o correio ou o telefone; ela se tornou "[...] o lugar onde quase tudo acontece [...]", onde "[...] são criados e armazenados os dados mais pessoais de cada um. É na internet que desenvolvemos e expressamos nossa personalidade e individualidade".

Depois que a internet que foi se desenvolvendo, surgiu a necessidade de se construir um direito atinente ao fluxo de informações, ao dado em movimento. Em 1890, foi publicado um artigo na Harvard Law Review que impulsionou o significado e a importância da privacidade, fundamentada na inviolabilidade da personalidade. O artigo "*The Right to Privacy*" explora os contornos conceituais dessa transformação da privacidade, conectando-a a fundamentos

espirituais. Ele se concentra na proteção de elementos como pensamentos, emoções e sentimentos pessoais, independentemente da maneira ou forma de expressão. Isso se diferencia do direito à reputação, pois salvaguarda os sentimentos íntimos das pessoas mesmo quando confrontadas com a alegação de fatos verdadeiros, sem considerar a intenção maliciosa do comunicador.

Além disso, se distingue dos direitos de propriedade intelectual ou artística, uma vez que oferece proteção independentemente do valor financeiro, artístico ou histórico da informação violada. A privacidade pode ser violada de várias maneiras, dada sua natureza como uma salvaguarda geral da individualidade, preservando o direito à própria personalidade. Porém esse direito para os autores não seria absoluto, como os outros direitos fundamentais, a privacidade também pode ser sujeita a restrições em certos contextos. Essas restrições não impediriam a divulgação de informações relevantes para o interesse público ou coletivo, ou a divulgação de eventos da vida privada realizada pela própria pessoa. (WARREN, BRANDEIS, 1890)

Por fim, o infrator ainda poderia se defender e demonstrar a ausência de intenção maliciosa, sendo assim seriam considerados ao analisar situações específicas. O artigo foi o marco inicial para que a sociedade observasse a importância da proteção da privacidade, mas levou-se um tempo para que essa preocupação chegasse ao posicionamento jurisprudencial.

Em suma, a relação entre direitos humanos e direito à privacidade é evidente nas disposições de tratados e convenções de direitos humanos, como o Pacto Internacional sobre Direitos Civis e Políticos. Este tratado reconhece explicitamente o direito à privacidade, destacando a importância de proteger a vida privada, a correspondência e a honra das pessoas. Em muitos países, o direito à privacidade é consagrado na Constituição ou em leis de direitos fundamentais. Essas disposições legais estabelecem limites para a coleta, armazenamento e uso de informações pessoais por parte do governo e de empresas privadas. (CNE, s.p)

Em sínteses, os direitos humanos incluem uma ampla gama de direitos fundamentais, e o direito à privacidade é um desses direitos que é fundamental para a dignidade e liberdade das pessoas. Diante, mostra-se a importância e que é dever do governo e sociedades em proteger e respeitar o direito à privacidade, garantindo que as informações pessoais sejam tratadas com cuidado e que a interferência indevida em suas vidas privadas seja limitada e justificada.

EVOLUÇÃO DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS AO REDOR DO MUNDO

A ascensão das legislações de proteção de dados ao redor do mundo tem sido um processo significativo nas últimas décadas, impulsionado pelo avanço da tecnologia e pela crescente conscientização sobre a importância da privacidade e da necessidade de regulamentar o tratamento de informações pessoais em um mundo digital. De acordo com o site LGPD Brasil (2017), a primeira lei de proteção de dados foi criada em 1970, em Hessen, na Alemanha, nesse período, o progresso da computação e da indústria nas nações mais avançadas teria motivado o governo alemão a estabelecer regulamentações para gerenciar a privacidade dentro do país. Isso marcou a primeira vez em que o conceito de proteção de dados foi introduzido no contexto jurídico da Alemanha. Apesar de ter sido concebido no início da década de 70, a legislação só foi finalizada e posta em prática em 1978. Durante o mesmo ano, nações como França, Noruega, Suécia e Áustria também promulgariam suas próprias leis regulando como as informações de seus cidadãos poderiam ser usadas e compartilhadas.

Em 1980 foi estabelecida, as Diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para a Proteção da Privacidade e para o Fluxo Transfronteiriço de Dados Pessoais, juntamente com a Convenção 108 do Conselho da Europa, adotada em 1981, que desempenharam papéis fundamentais na disseminação de normas relacionadas à proteção de dados. (LGPD Brasil, 2017)

Diante disso, vários países foram criando suas legislações e regulamentação aos longos anos sobre as proteções dos dados e privacidade. Em 1995, o Parlamento Europeu e o Conselho da União Europeia estabeleceram a Diretiva 95/46/CE, que definiu normas para proteção de dados a serem seguidas por todos os países membros. Essa regulamentação já antecipava conceitos modernos de proteção de dados, como a coleta com finalidade específica, o direito do consumidor ao acesso aos dados e a responsabilidade das empresas pela segurança das informações. Além disso, a diretiva exigia que cada país membro designasse um órgão ou profissional responsável pela supervisão e implementação das regulamentações, promovendo a conformidade com a 95/46/CE. (LGPD Brasil, 2023)

Posteriormente, a União Europeia implementou o General Data Protection Regulation (GDPR), considerado uma das legislações mais completas e complexas sobre proteção de dados. Esta regulamentação estabeleceu bases legais e princípios fundamentais, como transparência, licitude, minimização de dados e responsabilidade. (LGPD Brasil, 2023)

Em 2000, foi estabelecido um acordo denominado Safe Harbor entre os Estados Unidos e a Europa, com o objetivo de facilitar a troca de informações pessoais entre essas duas regiões. No entanto, em 2015, o acordo foi revogado devido a preocupações com espionagem, o que levou à criação do Privacy Shield no ano seguinte. O Privacy Shield foi um programa que

oferecia maior segurança aos cidadãos europeus em relação à transferência internacional de dados com empresas dos EUA. (LGPD Brasil, 2023)

Já no Brasil, foi adotada alguns pontos sobre proteção de dados, na Constituição Federal de 1988, em seu artigo 5º de forma geral, sobre a privacidade dos brasileiros “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”.

Entretanto, em 1996, a Lei 9.296 que regulamenta o inciso XII, parte final do art. 5º da Constituição Federal brasileira acrescentou que é “inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” como completo ao artigo.

Já nos anos 90, o Brasil deu passos significativos no desenvolvimento de regulamentações relacionadas às relações entre empresas e clientes. Um marco importante foi a criação do Código de Defesa do Consumidor (CDC), que não apenas evoluiu com o tempo, mas também abordou questões cruciais relacionadas à proteção de informações. O Código de Defesa do Consumidor incluiu uma seção específica dedicada a cadastros e bancos de dados. Isso representou um avanço fundamental, pois assegurou o direito do consumidor de acessar suas próprias informações mantidas por empresas e solicitar correções caso houvesse informações incorretas.

O artigo 13º do CDC enfatizou a proibição de dificultar o acesso às informações do consumidor e a necessidade de comunicar ao titular sobre o registro de seus dados, estabelecendo infrações para tais práticas. Além disso, outros artigos da legislação buscaram garantir a privacidade dos dados do consumidor e responsabilizar as empresas pela segurança das informações, exemplificado pelo artigo 11º, capítulo 3, que estabelece que os dados pessoais do consumidor devem ser mantidos em sigilo e utilizados exclusivamente para os fins do atendimento.

Porém, foi somente em 2013, com o Marco Civil da Internet, que ficou claro para a justiça brasileira que as ações na internet têm impactos no mundo real. Desse modo, foram introduzidos conceitos importantes, como a neutralidade de rede e a liberdade de expressão, além de estabelecer as responsabilidades das entidades governamentais na prestação de serviços de internet. Em março de 2013, o decreto nº 7.962 ainda acrescentou orientações adicionais que complementam o Código de Defesa do Consumidor. O artigo 2º do decreto estipula que as diretrizes do Plano Nacional de Consumo e Cidadania incluem a "autodeterminação, privacidade, confidencialidade e segurança das informações e dados pessoais prestados ou

coletados, inclusive por meios eletrônicos". Isso enfatiza a importância da proteção dos dados pessoais e da privacidade dos consumidores no ambiente digital. Contudo, apenas 2020, que foi criada a Lei de Proteção de Dados (LGPD) que trouxe uma maior atenção aos dados sensíveis, a portabilidade de dados e a imposição de sanções administrativas em caso de descumprimento, a todas as empresas que coletam ou processam dados no território nacional ou de cidadãos brasileiros. Com as muitas mudanças da era digital, nota-se da importância da proteção dos dados pessoais, desse modo em 2022, a emenda constitucional nº 115 alterou a Constituição Federal e incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais, além de fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Indubitavelmente, essas diretrizes e convenção contribuíram significativamente para ampliar a concepção de privacidade e reconhecer a necessidade de uma harmonização regulatória. Com o avanço da tecnologia da informação, tornou-se evidente que a proteção da vida privada demandava uma abordagem transfronteiriça, um desafio que persiste até os dias atuais.

Sendo assim, é fundamental salientar que o direito à proteção de dados pessoais representa um aprofundamento das concepções de vida privada e intimidade e, em conjunto com o direito à autodeterminação informativa que passa a integrar o núcleo dos direitos da personalidade. A proteção de dados pessoais envolve a salvaguarda do tratamento de informações de indivíduos (titulares) com o potencial de identificá-los ou torná-los identificáveis, seja esse tratamento realizado por pessoas físicas ou jurídicas, de direito público ou privado, e independente do meio onde esses dados estejam, seja em formatos físicos ou digitais. (KODAMA, R; TÉCNICO, A; PEREIRA, A., 2020, p.10)

Nesse sentido, é importante ressaltar que a proteção de dados vai além da mera prevenção contra decisões automatizadas. O movimento atual em torno da regulamentação do desenvolvimento e operação de sistemas de inteligência artificial não aborda integralmente o significado da proteção de dados. Vai além da simples adoção de padrões de segurança da informação; busca, em última instância, preservar a autonomia dos titulares em relação à sua consciência, perspectiva de mundo e expressão de sua vontade, sendo crucial para a livre formação de sua personalidade. Assim, a preocupação com a proteção de dados está destinada a crescer à medida que a tecnologia avança, e as leis de proteção de dados continuarão a evoluir para lidar com as complexidades do mundo digital e as crescentes preocupações com a privacidade. Empresas e organizações em todo o mundo estão cada vez mais sujeitas a

regulamentações rigorosas e devem estar em conformidade com as leis de proteção de dados relevantes em suas jurisdições.

O “EFEITO CAMBRIDGE ANALYTICA” NA MUDANÇA E CRIAÇÃO DA LEI DE PROTEÇÃO DE DADOS

A crescente evolução da tecnologia e a expansão da internet têm sido um fenômeno revolucionário nas últimas décadas, moldando profundamente a forma como vivemos, trabalhamos e nos conectamos com o mundo. Essa transformação tem ocorrido em várias frentes, trazendo consigo uma série de mudanças significativas em diversos aspectos de nossa sociedade. No entanto, essa crescente evolução tecnológica e a dependência da internet também levantam desafios. Questões de privacidade e segurança de dados tornaram-se preocupações críticas, à medida que mais informações pessoais são compartilhadas online.

Diante disso, ao longo dos anos, várias leis foram promulgadas para regular a proteção da privacidade e dos dados pessoais. No entanto, com as constantes evoluções da internet, torna-se claro que as leis e diretrizes precisam se adaptar às mudanças emergentes. A adequação das leis e à evolução da internet é um desafio constante para os sistemas jurídicos ao redor do mundo. A rápida e constante transformação do ambiente digital, exige que as regulamentações acompanhem de perto as mudanças tecnológicas. Um exemplo marcante dessa necessidade é a questão da proteção de dados pessoais.

A empresa Cambridge Analytica (CA), conhecida por sua atuação com serviços de análise de dados para fins comerciais e na consultoria política, teve destaque na participação em campanhas eleitorais e ganhou notoriedade devido ao seu envolvimento nas eleições presidenciais dos Estados Unidos em 2016, apoiando o antigo presidente dos Estados Unidos, o republicano Donald Trump.

De acordo com os jornais The New York Times e The Guardian a empresa empregou uma estratégia na qual dados de cada usuário foram utilizados para direcionar anúncios políticos de maneira personalizada. (The New York times, 2018, p.1). Esse método permitiu a veiculação de diversas propagandas políticas, cada uma direcionada a públicos específicos, resultando assim em uma influência em grande escala. É incontestável o impacto que essa abordagem teve na campanha presidencial de Trump, gerando resultados favoráveis. E estes mesmos dados também influenciaram a votação no referendo do Brexit no Reino Unido no mesmo ano. Através da obtenção ilegal de dados pessoais de milhões de usuários do Facebook, a empresa utilizou essas informações para influenciar o comportamento dos eleitores por meio de anúncios

direcionados e outras táticas de marketing digital. Esse escândalo resultou em uma série de investigações e consequências legais tanto nos Estados Unidos quanto no Reino Unido. (The New York times, 2018, p.1)

As autoridades norte-americanas conduziram audiências e investigações no Congresso para examinar o papel desempenhado pela Cambridge Analytica nas eleições de 2016. Essa notícia teve um impacto significativo no Facebook, que passou a ser questionado em relação à sua capacidade de proteger os dados dos usuários de forma adequada.

A empresa utilizava três tipos de métodos para obter os dados dos usuários. O primeiro tinha a responsabilidade de coletar, armazenar e processar informações pessoais no Facebook. Isso incluía uma ampla gama de dados, como fotos pessoais, postagens triviais do dia a dia, listas de amigos, lista de pessoas bloqueadas, grupos aos quais as pessoas se juntaram e grupos nos quais estavam ativamente envolvidas. Essa tarefa envolvia lidar com um vasto banco de dados, comumente conhecido como (big data)¹, e categorizá-lo. (The Guardian, 2019, p.1)

O processo envolvia os usuários em responder perguntas em pesquisas dentro do Facebook, no entanto, ao fazer isso, eles não estavam apenas respondendo a questões simples, como "Qual minha comida preferida?" ou "Quem é o presidente dos Estados Unidos?", como também respostas variando entre incorreto, neutro e correto. Com isso, essas respostas eram usadas para determinar o tipo de comportamento do usuário em várias situações e cenários. Então, quando o usuário clicava para fazer um teste de personalidade no Facebook, a maioria que não lia os termos e condições da pesquisa e a política de privacidade do aplicativo, inadvertidamente concedia à CA acesso a uma série de dados pessoais. Isso incluía informações como idade, cor, religião, altura, região de residência e trabalho, geolocalização, padrões de movimentação, acesso a todas as postagens, fotos e arquivos compartilhados na rede social, conforme divulgação feita pelo jornal G1.

Devido a essa falha de design da rede social Facebook, milhões de usuários ficaram vulneráveis e ocorreu a quebra de sua privacidade. Como a coleta de dados era contínua, bastava fazer o teste de personalidade uma vez para que a CA desenvolvesse uma visão em tempo real dos comportamentos e tendências em constante evolução de todos os usuários, entretanto, a violação do direito à privacidade não se limitava somente a isso. Com o conhecimento ou consentimento dos usuários, todos os amigos da pessoa que realizava o teste de personalidade que o usuário compartilhou, também tinham seus dados coletados. (The Guardian, 2019, p.1)

¹ Conjunto de dados extremamente amplos que, por isto, necessitam de ferramentas especiais para comportar o grande volume de dados que são encontrados, extraídos, organizados, transformados em informações que possibilitam uma análise ampla e em tempo hábil.

Consequentemente, o escândalo teve um impacto significativo em outras empresas, que se viram obrigadas a revisar suas políticas de privacidade e segurança de dados. Diante disso, fica evidente que o caso da Cambridge Analytica desencadeou um debate global sobre a proteção da privacidade na era da informação. Este incidente concreto levanta sérias questões sobre a integridade da democracia, levando-nos a ponderar se essa é a primeira empresa a ter acesso e utilizar tais dados para influenciar processos eleitorais e a sociedade, ou se é simplesmente a primeira a ter sua prática exposta ao público em larga escala. Depois desse escândalo, teve a necessidade de uma regulamentação mais robusta na proteção de dados pessoais dos usuários da internet e das redes sociais. Isso levou à implementação de leis como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, a Lei Geral de Proteção de Dados (LGPD) no Brasil, que visou proteger os direitos fundamentais dos usuários e a garantir que suas informações pessoais sejam tratadas com respeito e segurança, além de provocar debates sobre a necessidade de leis de privacidade mais abrangentes nos Estados Unidos. Embora os EUA não tenham uma lei federal de privacidade de dados abrangente, vários estados, como a Califórnia, implementaram suas próprias leis de privacidade, como a Lei de Privacidade do Consumidor da Califórnia (CCPA), trazendo discussões no Congresso dos EUA sobre a aprovação de uma lei de privacidade federal. (Privacy Tech, 2021)

O caso Cambridge Analytica trouxe uma maior conscientização pública sobre a importância da privacidade de dados e dos riscos associados à coleta indiscriminada de informações pessoais. Isso pressionou as empresas a revisar suas práticas de coleta e tratamento de dados, implementando medidas de privacidade mais rigorosas, via portal G1.

O escândalo também levou as empresas de tecnologia, como o Facebook, a revisar suas políticas de privacidade e segurança de dados. Muitas dessas empresas implementaram medidas mais estritas para proteger os dados dos usuários e fornecer opções de controle mais transparentes sobre como os dados são usados. O caso Cambridge Analytica teve um impacto significativo na forma como as leis de proteção de dados são moldadas e aplicadas em todo o mundo, promovendo uma maior ênfase na privacidade dos dados e na responsabilização das organizações que lidam com informações pessoais.

ANÁLISE JURISPRUDENCIAL

Neste tópico serão apresentadas algumas decisões referentes a Lei de Proteção de Dados brasileira, o direito à privacidade e vazamento de dados, julgados que foram decididos pelo Supremo Tribunal Federal (STF) e Supremo Tribunal de Justiça (STJ).

DECISÃO DO SUPREMO TRIBUNAL FEDERAL

Em decisão proferida pelo STF, na data 15 de setembro de 2022, tendo como relator o Min. Gilmar Mendes no Tribunal Pleno, julgou parcialmente procedente os pedidos de ação de inconstitucionalidade do Decreto 10.046/2019.

Ementa: DIREITO CONSTITUCIONAL. DIREITOS FUNDAMENTAIS À PRIVACIDADE E AO LIVRE DESENVOLVIMENTO DA PERSONALIDADE. TRATAMENTO DE DADOS PESSOAIS PELO ESTADO BRASILEIRO. COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. ADI E ADPF CONHECIDAS E, NO MÉRITO, JULGADAS PARCIALMENTE PROCEDENTES. INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO. DECLARAÇÃO DE INCONSTITUCIONALIDADE COM EFEITOS FUTUROS.

O presente pedido de medida cautelar, foi interposto pelo Conselho Federal da Ordem dos Advogados do Brasil contra o Decreto 10.046/19, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

Alegou o requerente que o referido decreto sofre de inconstitucionalidade formal, uma vez que o Presidente da República, ao editá-lo, ultrapassou os limites regulamentares, violando o artigo 84, incisos IV e VI, 'a', da Constituição Federal. Argumenta, que o decreto traz conflito com as leis constitucionais e infraconstitucionais relacionadas à proteção de dados e à privacidade, o que acarreta riscos e desalinhamentos que prejudicam o sistema de proteção de dados delineado em nosso ordenamento jurídico e enfraquecem as liberdades e os direitos fundamentais. Além disso, argumenta-se a inconstitucionalidade material do dispositivo, uma vez que ele viola diretamente a dignidade da pessoa humana, a inviolabilidade da intimidade, privacidade, vida privada, honra e imagem das pessoas, bem como o sigilo dos dados e a garantia do habeas data como meio de proteção do direito à autodeterminação informativa.

Ademais, o decreto também ofende os princípios básicos e as diretrizes da Lei de Proteção de Dados, pois permite o amplo compartilhamento de informações entre órgãos públicos federais sem protocolos claros e identificação precisa dos agentes envolvidos e instituir uma base de dados unificada que pode ser compartilhada livremente, aumentando o risco a vazamento e incidentes de segurança. A alegação de inconstitucionalidade material de um decreto presidencial baseia-se em argumentos específicos que devem ser analisados de acordo com a legislação e a Constituição do país em questão. Nesse caso, a alegação se baseia em vários argumentos relacionados à Lei Geral de Proteção de Dados (LGPD), à segurança de dados e ao potencial de controle político da população. Diante disso, pede que seja declarada a inconstitucionalidade integral do Decreto 10.046/2019, e como consequência a extinção do Cadastro de Base do Cidadão e do Comitê Central de Governança de Dados.

Diante disso, o Procurador Geral da União, expressou seu entendimento de que a Ação Direta de Inconstitucionalidade não é apropriada. Destacando-se, que embora não ultrapasse as barreiras legais estabelecidas pela LGPD, o decreto *“silenciou sobre aspecto cuja observância, de todo modo, é imposta na norma legal e que se presta a viabilizar a efetiva fiscalização pelos órgãos de controle e pelos cidadãos e, em última análise, a garantir que a faculdade conferida à Administração Pública de realiza tratamento compartilhado de dados pessoais se circunscreva à perseguição de interesses públicos e legítimos.”*.

Portanto, como medida para evitar a violação dos direitos fundamentais, argumenta-se que é essencial interpretar o decreto contestado de tal forma que o mecanismo de compartilhamento de dados e as regras estabelecidas pelo Comitê Central de Governança de Dados ou pelo gestor de dados, conforme definido no artigo 4º, parágrafos I e II, da norma, devem incluir como requisito prévio ao compartilhamento de dados a formalização de um pedido fundamentado pela autoridade solicitante. Conclui-se que a decisão também abordou o tratamento de dados pessoais em atividades de inteligência e estabeleceu parâmetros específicos, como a necessidade de medidas proporcionais, motivação formal e segurança dos dados. A responsabilidade civil do Estado foi mencionada em caso de tratamento inadequado de dados, com a possibilidade de responsabilização de servidores públicos.

Além disso, a decisão declarou a inconstitucionalidade do artigo 22 do Decreto 10.046/2019, preservando a estrutura do Comitê Central de Governança de Dados por um prazo de 60 dias, com o objetivo de garantir mudanças na composição do órgão para torná-lo mais independente e plural. Em resumo, a decisão enfatizou a necessidade de conformidade estrita com a LGPD e princípios de transparência e segurança no compartilhamento de dados pessoais entre órgãos públicos, com a imposição de responsabilidades em caso de violações. Além disso,

buscou garantir a adequação do Comitê Central de Governança de Dados à legislação e à democracia, além de equilibrar a necessidade de compartilhamento de informações entre órgãos públicos com a proteção dos direitos de privacidade e o cumprimento das disposições legais.

DECISÃO DO SUPREMO TRIBUNAL JUSTIÇA

Na decisão proferida em 07 de março de 2023, pelo Supremo Tribunal de Justiça de São Paulo tendo como relator o Min. Francisco Falcão, julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa.

Ementa: PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO.

O presente agravo foi interposto pelo agravante contra decisão do Tribunal de Justiça do Estado de São Paulo, em grau recursal, que deu provimento ao recurso de apelação da autora, reformulando a decisão de primeiro grau para condenar a concessionária ré ao pagamento de indenização por danos morais.

A empresa alegou que Corte de origem se equivocou ao enquadrar os dados vazados como sensíveis, nos termos do art. 5º, II, da LGPD, uma vez que estes seriam básicos de qualificação de qualquer pessoa, muitos dos quais fornecidos corriqueiramente pelos indivíduos nas mais variadas e simples operações diárias da vida civil, tanto assim que podem ser encontrados nos próprios autos, os quais, por opção da recorrida, não foram acobertados pelo segredo de justiça, já que não houve pedido nesse sentido. Sustentou ofensa aos arts. 186, 884, 927, e 944, do CC/2002, e ao art. 42, caput, da LGPD, por não ser passível de indenização evento incerto futuro, como eventual ou potencial dano decorrente do vazamento dos dados da recorrida. Tampouco o vazamento de dados não sensíveis poderia, por si só, causar lesão à esfera íntima da pessoa humana.

Desse modo, considerando as informações apresentadas, é importante destacar que a situação seria diferente se estivéssemos diante de um vazamento de dados sensíveis que afetasse a intimidade de uma pessoa natural. No entanto, no caso em questão, se trata de uma exposição

inconveniente de dados pessoais comuns, que não foi acompanhada de evidências que comprovassem a ocorrência de dano, conforme destacado na decisão de primeira instância

É importante ressaltar que, para caracterizar o dano moral e justificar a necessidade de indenização, o incidente deve resultar em uma séria ofensa à honra, dignidade ou atributos da personalidade da pessoa afetada. No presente caso, o simples fato de ocorrer um vazamento de dados pessoais não é suficiente para justificar uma compensação por dano moral, uma vez que não foram apresentadas provas concretas de que algum dano tenha ocorrido. Portanto, conforme enfatizado na decisão que está sendo revista, é essencial notar que os dados em questão se referem às informações comuns fornecidas em qualquer cadastro, inclusive em sites consultados no cotidiano, não estando, portanto, protegidos por sigilo. O conhecimento desses dados por terceiros não configura uma violação ao direito de personalidade da recorrida. O vazamento de dados pessoais, embora seja uma falha indesejável no tratamento de informações de uma pessoa natural por uma pessoa jurídica, por si só, não tem o potencial de gerar um dano moral que seja passível de indenização. Em outras palavras, o dano moral não é presumido; é necessário que o titular dos dados prove qualquer dano resultante da exposição dessas informações.

Diante dessa realidade, torna-se evidente que a crescente tendência de compartilhar informações pessoais em diversos websites, mídias sociais e plataformas online se consolidou como uma prática difundida na era da internet. Isso traz consigo desafios significativos no que diz respeito à detecção de possíveis vazamentos de dados por parte de organizações governamentais e empresas, resultando em obstáculos adicionais para a proteção dos direitos humanos e do direito à privacidade. A implementação de medidas adequadas torna-se uma tarefa complexa diante desse cenário.

CONCLUSÃO

Em suma, a era digital apresenta desafios complexos no que diz respeito aos direitos humanos, principalmente relacionados à proteção da privacidade em um mundo cada vez mais interconectado. Nesse sentido, foram analisados desafios enfrentados pelos direitos humanos na era digital, destacando a importância da proteção da privacidade em um mundo conectado. A rápida evolução da tecnologia e a disseminação generalizada da internet têm ampliado consideravelmente as oportunidades e vantagens para muitos indivíduos. Contudo, também têm acentuado as disparidades preexistentes na sociedade, culminando em uma profunda divisão digital.

Essa exclusão digital afeta negativamente o exercício de direitos fundamentais, como a liberdade de expressão e o acesso à informação. Aqueles sem acesso à tecnologia e à internet frequentemente se encontram à margem da sociedade globalizada, incapazes de participar plenamente da troca de informações e do diálogo público online. Isso limita sua capacidade de expressar opiniões, acessar informações cruciais e usufruir dos benefícios da sociedade da informação.

Paralelamente, a coleta indiscriminada de dados pessoais por empresas e governos representa uma ameaça significativa à privacidade. A prática da vigilância em massa, que envolve a coleta massiva e constante de informações pessoais, mina a privacidade das pessoas e cria um ambiente em que os cidadãos podem se sentir constantemente observados e inibidos em suas ações. Além disso, o uso indevido dessas informações pode resultar em abusos, discriminação e violações dos direitos humanos.

Encontrar um equilíbrio entre a necessidade legítima de coletar dados para segurança e prestação de serviços e o respeito pela privacidade das pessoas é fundamental. Para abordar essa questão, muitos países promulgaram leis de proteção de dados e regulamentações que buscam garantir que a coleta, armazenamento e uso de dados pessoais sejam realizados de maneira transparente, consentida e segura. Além disso, organismos internacionais, como a União Europeia, implementaram regulamentações como o Regulamento Geral de Proteção de Dados (GDPR) para estabelecer padrões mais elevados de proteção da privacidade.

A análise e a regulamentação eficaz da coleta de dados pessoais são fundamentais para garantir que as preocupações sobre a vigilância em massa e o uso inadequado de informações sejam abordadas de maneira a proteger os direitos humanos e promover a confiança na era digital. Essas medidas buscam equilibrar a necessidade de segurança e inovação tecnológica com o respeito pelos direitos individuais, permitindo que as pessoas desfrutem dos benefícios da conectividade digital sem comprometer sua privacidade.

Para enfrentar esses desafios, é essencial que governos, organizações internacionais e empresas de tecnologia colaborem para garantir que o acesso à internet seja universal e equitativo. Além disso, a proteção da privacidade e dos dados pessoais deve ser reforçada para garantir que os direitos individuais sejam preservados em um mundo digital. A busca por soluções inclusivas e equitativas na era digital é fundamental para garantir que os direitos humanos sejam respeitados e protegidos em um mundo cada vez mais interconectado. Desse modo, a conscientização sobre o compartilhamento e divulgação de dados é um aspecto fundamental da era digital. Com o aumento da conectividade e da presença online, as informações pessoais se tornaram um recurso valioso, e a falta de cuidado no compartilhamento

e na divulgação desses dados pode ter sérias consequências. E essa conscientização desempenha um papel fundamental na promoção de uma cultura de ética digital. Ela desperta a compreensão de que não apenas possuímos direitos em relação aos nossos próprios dados, mas também carregamos responsabilidades éticas no que diz respeito ao uso dos dados de terceiros.

Quando as pessoas adquirem o conhecimento sobre como preservar sua privacidade na internet, isso lhes confere um senso de capacitação para utilizar a tecnologia de maneira eficiente e segura. Isso, por sua vez, permite que aproveitem ao máximo os benefícios da tecnologia, ao mesmo tempo em que minimizam os riscos envolvidos.

Em suma, a importância da conscientização acerca do compartilhamento e divulgação de dados é fundamental para salvaguardar a privacidade individual, fomentar a responsabilidade das empresas e assegurar que a tecnologia seja empregada de maneira ética e benéfica para a sociedade. Isso constitui um pilar crucial da literacia digital na era atual, garantindo, desse modo, a preservação dos direitos fundamentais e humanos das pessoas.

REFERÊNCIAS

Assembleia Geral da ONU. Declaração Universal dos Direitos Humanos. Paris, 1948. Disponível em: <https://declaracao1948.com.br/declaracao-universal/declaracao-direitos-humanos/>. Acesso em: 17 ago. 2023

BASTOS, Celso Ribeiro, Curso de Direito Constitucional/ Celso Ribeiro Bastos – São Paulo: Celso Bastos Editora, 2002.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 05 ago. 2023

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: ago. 2023.

BRASIL. Lei nº. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art.5º da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19296.htm. Acesso em: ago. 2023.

BERGHEL, H. *Malice Domestic: The Cambridge Analytica Dystopia*. Nevada: University of Nevada, 2018

CAMERON, D. AggregateIQ created Cambridge analytica's election software, and here is the proof. Disponível em: <<https://gizmodo.com/aggregateiq-created-cambridge-analyticas-election-softw-1824026565>>. Acesso em: 09 set. 2023.

CONFESSORE, N. Cambridge Analytica and Facebook: The scandal and the fallout so far. The New York times, Disponível em:<<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>>. Acesso em: 4 set. 2023

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. 2000. Disponível em: < http://www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf >. Acesso em: 01 set. 2023.

FERNANDA, D. Conheça as leis de proteção de dados ao redor do mundo. Disponível em: <<https://www.lgpdbrasil.com.br/conheca-as-leis-de-protecao-de-dados-ao-redor-do-mundo/>>. Acesso em: 29 set. 2023.

Gizmodo Media Group, 2018. Disponível em: <https://gizmodo.com/aggregateiq-created-cambridge-analyticas-election-softw-1824026565>. Acesso em: 9 dez. 2019.

KODAMA, R.; TÉCNICO, A.; PEREIRA, A. Guia de boas práticas lei geral de proteção de dados (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-dedados/guias/guia_lgpd.pdf. Acesso em: 25 set. 2023.

KOZLOWSKA, I. *Facebook and Data Privacy in the Age of Cambridge Analytica*. Seattle: Henry M. Jackson School of International Studies; College of Arts and Sciences; University of Washington, 2019.

MATHIAS, Márcio José Barcellos. Distinção conceitual entre Direitos Humanos, Direitos Fundamentais e Direitos Sociais (2006). Disponível em: <http://www.direitonet.com.br/artigos/exibir/2791/Distincao-conceitual-entre-Direitos->

Humanos -Direitos-Fundamentais-e-Direitos-Sociais. Acesso em 29 set. de 2023.

ONU - Pacto Internacional sobre os Direitos Cíveis e políticos. Disponível em: <<https://www.cne.pt/content/onu-pacto-internacional-sobre-os-direitos-civis-e-politicos>>. Acesso em: 04 set. 2023.

PRIVACY TECH, 2021. Apenas três estados americanos têm leis abrangentes de privacidade de dados. Disponível em: < <https://www.privacytech.com.br/protecao-de-dados/apenas-tres-estados-americanos-tem-leis-abrangentes-de-privacidade-de-dados,403686.jhtml>> Acesso em 7 set. 2023.

REDESG / Revista Direitos Emergentes na Sociedade Global – www.ufsm.br/redesg v. 2, n. 2, jul. dez/2013

SARLET, Ingo Wolfgang. Conceito de direitos e garantias fundamentais. 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/67/edicao-1/conceito-de-direitos-e-garantias-fundamentais>

SAMPAIO, José Adércio Leite. Direito à Intimidade e à Vida Privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998

VII CONGRESSO INTERNACIONAL DE DIREITOS HUMANOS DE COIMBRA: UMA VISÃO TRANSDISCIPLINAR. Disponível em: <https://www.cidhcoimbra.com/_files/ugd/8f3de9_232734456abd43bdb2afeeacd7e632.pdf>. Acesso em: 29 set. 2023.

VIEIRA DE LORENZI CANCELIER, M. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. Seqüência estudos jurídicos e políticos, v. 38, n. 76, p. 213, 2017.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, Vol. 4, nº. 5, Dec. 1890, pp. 193-220. Disponível em: <https://www.jstor.org/stable/pdf/->

1321160.pdf?refreqid=excelsior%3A97ece71b995c64e58a3e57a6291f8a77&ab_segments=&origin=&initiator=&acceptTC=1, Acesso em 25 ago. 2023

WONG, J. C. The Cambridge Analytica scandal changed the world – but it did not change Facebook. THE GUARDIAN. Disponível em: <<https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>> Acesso em: 4 set. 2023