



CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO EM DIREITO

BRUNA EVELLYN LEÃO
LARISSA MYLLENA MENDONÇA DA SILVA
LUCIANO BARBOSA DA SILVA

**Monitoramento digital: uma análise constitucional da inviolabilidade
das comunicações na internet por empresas de tecnologia**

RECIFE/2024



BRUNA EVELLYN LEÃO
LARISSA MYLLENA MENDONÇA DA SILVA
LUCIANO BARBOSA DA SILVA

**Monitoramento digital: uma análise constitucional da inviolabilidade
das comunicações na internet por empresas de tecnologia**

Trabalho de conclusão de curso
apresentado à Disciplina TCC II do
Curso de Bacharelado em Direito do
Centro Universitário Brasileiro –
UNIBRA, como parte dos requisitos
para conclusão do curso.

Orientadora: Prof^ª. Patrícia Alves da
Silva.

RECIFE/2024



BRUNA EVELLYN LEÃO
LARISSA MYLLENA MENDONÇA DA SILVA
LUCIANO BARBOSA DA SILVA

**Monitoramento digital: uma análise constitucional da inviolabilidade
das comunicações na internet por empresas de tecnologia**

Trabalho de conclusão de curso apresentado à Disciplina TCC II do Curso de Direito do
Centro Universitário Brasileiro - UNIBRA, como parte dos requisitos para conclusão do curso.

Examinadores:

Orientador – Titulação

Examinador 1 – Titulação

Examinador 2 - Titulação

Nota: _____

Data: ____/____/____

RESUMO

O presente trabalho tem como tema - “Monitoramento digital: uma análise constitucional da inviolabilidade das comunicações na internet por empresas de tecnologia”. O monitoramento digital refere-se às práticas de coleta, análise e armazenamento de dados e informações de usuários, realizadas por empresas de tecnologia, com o objetivo de rastrear comportamentos, preferências e atividades online. Tais práticas são geralmente utilizadas para fins de comercialização de produtos, com personalização de anúncios e vendas de acordo com o perfil do usuário, no entanto, essa prática levanta preocupações quanto à invasão de privacidade e à conformidade com os direitos fundamentais à privacidade e a inviolabilidade das comunicações. Diante disso, o objetivo geral do estudo foi analisar a prática de monitoramento digital na internet à luz do direito fundamental da privacidade e da inviolabilidade das comunicações. Os objetivos específicos, consistiram em avaliar a eficácia das medidas legais e regulatórias em garantir o direito à privacidade no ambiente digital, baseando-se no posicionamento jurisprudencial relacionado à proteção da privacidade e à inviolabilidade das comunicações no contexto da internet. Posto isso, conclui-se que as práticas de monitoramento digital, embora justificadas por interesses comerciais, apresentam desafios à proteção dos direitos fundamentais. A necessidade de aprofundamento do debate quanto à eficácia das regulamentações existentes, sendo necessária uma fiscalização mais rigorosa por parte do Estado enquanto legitimado para tal ofício, conforme a emenda à constituição 115, de 2022. Para isto, o estudo utilizou como métodos de pesquisa uma abordagem qualitativa, por meio de análises bibliográficas, como doutrinas e artigos científicos e pesquisa documental utilizando-se de legislações e jurisprudências.

Palavras-Chaves: Direito fundamental. Monitoramento. Privacidade. Tecnologia.

ABSTRACT

The theme of this paper is “Digital monitoring: a constitutional analysis of the inviolability of internet communications by technology companies”. Digital monitoring refers to the practices of collecting, analyzing and storing user data and information, carried out by technology companies, with the aim of tracking behaviors, preferences and online activities. Such practices are generally used for the purpose of marketing products, with personalized advertisements and sales according to the user's profile. However, this practice raises concerns regarding the invasion of privacy and compliance with the fundamental rights to privacy and the inviolability of communications. In view of this, the general objective of the study was to analyze the practice of digital monitoring on the internet in light of the fundamental right to privacy and the inviolability of communications. The specific objectives consisted of evaluating the effectiveness of legal and regulatory measures in guaranteeing the right to privacy in the digital environment, based on the jurisprudential positioning related to the protection of privacy and the inviolability of communications in the context of the internet. Therefore, it is concluded that digital monitoring practices, although justified by commercial interests, present challenges to the protection of fundamental rights. The need to deepen the debate regarding the effectiveness of existing regulations, requiring more rigorous supervision by the State as it is authorized to do so, in accordance with constitutional amendment 115, of 2022. For this, the study used a qualitative approach as research methods, through bibliographical analysis, such as doctrines and scientific articles and documentary research using legislation and jurisprudence..

Keywords: Fundamental rights. Monitoring. Privacy. Technology.

¹ Graduando em direito pelo Centro Universitário Brasileiro - UNIBRA - brunaaleao@gmail.com

² Graduando em direito pelo Centro Universitário Brasileiro - UNIBRA - larissa99019@gmail.com

³ Graduando em direito pelo Centro Universitário Brasileiro - UNIBRA - lucyanosilva94@gmail.com

⁴ Mestra em Direito pela Universidade Católica de Pernambuco. Jornalista, Advogada e Professora do Centro Universitário Brasileiro – UNIBRA – patricia.silva@grupounibra.com

LISTA DE SIGLAS E ABREVIATURAS

ANPD	Autoridade Nacional de Proteção de Dados
BIG TECH	Grande Tecnologia
BIG DATA	Grandes dados
CCPA	Califórnia Consumer Privacy Act
COOKIES	Small Text Files - Pequenos Arquivos de Texto
EC	Emenda Constitucional
GDPR	Regulamento Geral de Proteção de Dados
GPS	Sistema de Posicionamento Global
HTML	Linguagem de marcação de hipertexto
IA	Inteligência Artificial
LGPD	Lei Geral de Proteção de Dados
STJ	Superior Tribunal de Justiça
STF	Superior Tribunal Federal
TIC	Tecnologias de Informação e Comunicação
Tracking Pixel	Pixel de Rastreamento

SUMÁRIO

1. Introdução.....	7
<i>1.1 Conceituação da Vigilância Digital.....</i>	<i>9</i>
<i>1.2 Proteção jurídica no contexto da evolução legislativa.....</i>	<i>10</i>
2. Direito à Inviolabilidade das Comunicações.....	11
<i>2.1 Direito à Privacidade.....</i>	<i>12</i>
<i>2.2 Direito à Intimidade.....</i>	<i>12</i>
<i>2.2.1 Princípio da Dignidade da Pessoa Humana.....</i>	<i>13</i>
3. Sistemas operacionais voltados para o monitoramento.....	14
<i>3.1 A Influência das Empresas de Tecnologia na Economia e no Comportamento do Consumidor.....</i>	<i>14</i>
<i>3.2 O Papel da TICs e Big data no monitoramento digital</i>	<i>16</i>
<i>3.2.1 Capitalismo de Vigilância Digital.....</i>	<i>17</i>
<i>3.2.2 Jurisprudências correlatas ao contexto do compartilhamento de dados.....</i>	<i>18</i>
4. Considerações Finais.....	21
5. Referências.....	22

1. Introdução

Este artigo empreende uma análise do direito constitucional à inviolabilidade das comunicações frente ao monitoramento das medidas de vigilância digital na internet perpetrado pelas empresas de tecnologia.

No contexto contemporâneo, a rápida evolução da tecnologia digital tem criado um ambiente global de interconexão sem precedentes, que embora ofereça oportunidades únicas para comunicação, inovação e desenvolvimento, também apresenta desafios significativos para a proteção dos direitos fundamentais, especialmente no que se refere à privacidade.

Diante disso, o objetivo geral do estudo foi analisar a prática de monitoramento digital na internet à luz do direito fundamental da privacidade e da inviolabilidade das comunicações, explorando os desafios, dilemas e implicações legais desse contexto.

Através do método hipotético dedutivo, constatou-se a necessidade de aprofundamento do debate quanto à eficácia das regulamentações existentes, sendo necessária uma fiscalização mais rigorosa por parte do Estado enquanto legitimado para tal ofício, conforme a emenda à constituição 115 de 2022. Para isto, foram utilizados métodos de abordagem qualitativa, com o estudo e análise bibliográfica, publicações acadêmicas, legislações e jurisprudências.

Ao examinar as bases teóricas e os fundamentos que orientam a coleta, armazenamento, tratamento e compartilhamento de dados, conforme dispõe a Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709/2018, bem como, casos práticos que ilustram sua aplicação e seus desafios, este artigo contribuirá para o debate acadêmico sobre a proteção dos direitos fundamentais no contexto digital.

Ademais, buscará fornecer percepções relevantes para a formulação e aprimoramento de meios regulatórios que equilibrem efetivamente a necessidade de segurança com o respeito aos direitos fundamentais em um mundo cada vez mais interconectado e digital. Posto isso, conclui-se que as práticas de monitoramento digital, embora justificadas por interesses comerciais, apresentam desafios à proteção dos direitos fundamentais.

Os objetivos específicos, consistiram em avaliar a eficácia das medidas legais e regulatórias em garantir o direito à privacidade no ambiente digital, baseando-se no posicionamento jurisprudencial relacionado à proteção da privacidade e à inviolabilidade das comunicações no contexto da internet.

A vigilância digital tem raízes profundas que remontam aos primórdios da internet. No início, a rede mundial de computadores foi projetada como um espaço de liberdade e descentralização, permitindo uma comunicação aberta e rápida entre pessoas e instituições.

Contudo, à medida que a internet crescia e se tornava indispensável para a sociedade moderna, os interesses econômicos e políticos também aumentaram, empresas de tecnologia, inicialmente focadas em fornecer serviços, passaram a acumular grandes quantidades de dados pessoais, alimentando uma verdadeira revolução no campo da vigilância.

Na década de 1990, com o surgimento das empresas de tecnologia, como *Google*, *Facebook* e *Amazon*, a vigilância digital tomou outra proporção, essas empresas perceberam o valor econômico dos dados pessoais e desenvolveram mecanismos sofisticados para monitorar e prever o comportamento dos usuários.

A internet deixou de ser apenas uma ferramenta de comunicação e se transformou em um vasto campo de coleta de dados, onde cada ação online passou a ser registrada e analisada para fins comerciais.

Com o avanço da tecnologia e o crescimento do Big Data, o poder das empresas de tecnologia na coleta e análise de informações se intensificou, a coleta de dados, antes limitada a cadastros básicos, passou a incluir detalhes íntimos sobre a vida dos usuários, como suas preferências, localização, hábitos de consumo e até questões de saúde.

A partir de algoritmos complexos, essas informações são utilizadas para criar perfis detalhados, permitindo uma vigilância em massa que antes era impensável. De forma assertiva, Wolfgang Hoffmann-riem afirma que:

O termo Big Data refere-se a situações em que as tecnologias digitais são utilizadas para lidar com grandes e diversas quantidades de dados e às várias possibilidades de combinação, avaliação e processamento desses dados por autoridades privadas e públicas em diferentes contextos. Os métodos de análise permitem um uso muito amplo de Big Data, tanto por atores estatais quanto privados. Isso envolve tanto oportunidades quanto riscos. O desenvolvimento posterior de aplicações de Big Data permite um potencial enorme aumento de conhecimento, pois agora é possível ler e classificar bases de dados confusas com comparativamente pouco esforço. Por outro lado, o uso de tecnologias digitais utilizando Big Data e IA também pode criar riscos consideráveis para relevantes bens jurídicos individuais e coletivos.¹

A partir dos anos 2000, as revelações feitas por figuras como Edward Snowden sobre a colaboração entre empresas de tecnologia e governos aumentaram as preocupações em torno da vigilância digital.

O caso trouxe à tona o debate sobre a privacidade na era digital, mostrando como a vigilância realizada por empresas pode servir a interesses governamentais, principalmente em questões de segurança nacional, a integração entre Estado e corporações no monitoramento digital revelou a fragilidade da privacidade individual.

Do ponto de vista constitucional, o monitoramento digital desafia diretamente direitos fundamentais, como o direito à privacidade e à inviolabilidade das comunicações. A Constituição Federal de 1988, em seu artigo 5º, garante a inviolabilidade da vida privada e da intimidade, bem como o sigilo das comunicações, no entanto, as práticas de vigilância digital massiva colocam em risco essas garantias, ao permitir que empresas acessem e manipulem informações pessoais sem o consentimento adequado dos indivíduos.

Em resposta a essas ameaças, diversas legislações foram implementadas ao redor do mundo, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia e, no Brasil, a Lei Geral de Proteção de Dados (LGPD), essas legislações buscam estabelecer limites para a coleta e uso de dados pessoais.

Nessa esteira, vem colocando o indivíduo no centro das decisões sobre suas informações, todavia, o desafio permanece, uma vez que as empresas de tecnologia continuam a desenvolver novas formas de monitoramento, muitas vezes à margem da regulamentação. Além disso, Tarcísio Teixeira sana dúvidas dizendo que:

O envio de mensagens eletrônicas, a princípio, reflete o direito à liberdade de expressão, não sendo razoável o exercício da censura, sob pena de infração do disposto no inc. IX do art. 5º, considerando-se que o e-mail é uma espécie de correspondência, apesar da forma eletrônica, ele teria, antes de tudo, a mesma natureza jurídica da correspondência convencional ou epistolar, cuja inviolabilidade e sigilo estão assegurados no inc. XII, do art. 5º da Constituição Federal. Por sua vez, o envio indiscriminado de mensagens - spams (a partir da captação dos dados pelos cookies e sua comercialização) à caixa de correio de uma determinada pessoa - pode ser considerado violação do direito à privacidade, amoldando-se à previsão constitucional, art. 5º, inc. X. Da mesma maneira, a clandestina captação de dados dos usuários, pessoas físicas e jurídicas, bem como o tráfico desses dados, pode infringir o dispositivo do inc. XII do art. 5º, por se tratar de violação do sigilo de dados. A privacidade é uma questão bastante relevante, tanto que é considerada direito fundamental. Sua violação, inclusive, é vedada pela Constituição Federal de 1988, art. 5º, inc. X. Entretanto, com a chegada da internet, a privacidade pode ter encontrado uma grande vilã nessa avançada rede de comunicação.²

Assim, a análise das medidas de vigilância digital pelas empresas de tecnologia sob a óptica constitucional revela um cenário complexo, onde os avanços tecnológicos e os direitos fundamentais muitas vezes colidem. A questão que se coloca é como equilibrar o desenvolvimento tecnológico e a inovação com a proteção dos direitos dos cidadãos, garantindo que a vigilância digital não se transforme em uma ferramenta de opressão.

1.1 Conceituação da Vigilância Digital

A vigilância digital pode ser entendida como acompanhamento das atividades das pessoas na internet, feito através da coleta e análise de dados gerados por elas. "A vigilância consiste em um processo contínuo de coleta, categorização e avaliação de dados, controle, direcionamento, disciplinar ou acompanhamento do comportamento das pessoas" (Duarte DE, Nunes P, Lima TGL, 2023).³

Empresas e governos usam essas informações para diferentes propósitos, como segurança ou publicidade, mas isso também traz preocupações sobre a privacidade e até onde é certo usar esses dados sem afetar a privacidade e nem violar o sigilo das comunicações.

Portanto, a vigilância digital é um fenômeno que se refere ao monitoramento e à coleta sistemática de informações sobre indivíduos ou grupos por meio de tecnologias digitais, este tipo de vigilância, realizado principalmente por governos e corporações, ocorre em plataformas online, dispositivos móveis e redes sociais, coletando dados pessoais, históricos de navegação, interações sociais e comportamentos de consumo.

A partir desses dados, são criados perfis detalhados que podem ser utilizados para diversos fins, desde a personalização de serviços até o controle social, no mundo contemporâneo, essa prática tornou-se central para o modelo de negócios de grandes empresas de tecnologia, ao mesmo tempo em que levanta sérias questões sobre privacidade e direitos fundamentais. No mais Tarcísio Teixeira afirma:

No que diz respeito à proteção da privacidade (direito inerente à inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa, nos termos da Constituição Federal, art. 5º, inc. X), a lei garante o sigilo dos dados pessoais do usuário, do que ele acessa na rede e do conteúdo de suas comunicações. Assim, não é permitido monitorar e fiscalizar os pacotes de dados (conteúdos) transmitidos pelos usuários na internet, sendo que o acesso a esses dados necessita de ordem judicial.²

Historicamente, a vigilância sempre foi uma ferramenta poderosa para governos, mas a era digital trouxe novos métodos de coleta e processamento de dados em uma escala sem precedentes. A internet, que foi inicialmente vista como uma ferramenta de liberdade e autonomia, rapidamente se transformou em um espaço de coleta massiva de dados.

Empresas de tecnologia em conjunto governos autoritários utilizam essas tecnologias para monitorar/controlar a sociedade, enquanto empresas de tecnologia extraem dados de seus usuários para fins de lucro, traçando perfis precisos para campanhas de marketing direcionadas, o impacto disso não se limita à violação da privacidade, mas também influencia comportamentos sociais e até mesmo resultados eleitorais.

Na perspectiva jurídica, a vigilância/monitoramento digital desafia diretamente os direitos garantidos pela constituição no que tange à confidencialidade. Na maioria das democracias, a constituição garante que as comunicações privadas não podem ser interceptadas sem o devido processo legal.

No entanto, a crescente capacidade das empresas de tecnologia de monitorar quase todas as interações digitais sem o consentimento explícito dos indivíduos cria uma tensão entre as garantias

essenciais e as interações financeiras, a falta de transparência sobre como e onde os dados são coletados agrava essa situação, tornando difícil para os cidadãos controlarem o uso de suas próprias informações.

1.2 Proteção jurídica no contexto da evolução legislativa

O avanço da tecnologia nas últimas décadas trouxe uma nova dimensão à vigilância/monitoramento digital, e com ela, a necessidade urgente de regulamentação para proteger os direitos dos cidadãos no que tange à privacidade. A coleta massiva de dados por empresas desafia fronteiras legais, exigindo uma resposta legislativa à altura.

Na Europa, Estados Unidos e Brasil, diferentes abordagens jurídicas emergiram, refletindo as particularidades econômicas, culturais e políticas de cada região, no entanto, todas essas legislações buscam, de algum modo, equilibrar o progresso tecnológico com a preservação da privacidade e dos direitos básicos. Além disso, Tarcísio Teixeira dispõe que:

A violação da privacidade dá à vítima o direito de buscar a reparação do dano junto ao agente causador, que, demonstrado o dano e nexo causal, responderá, patrimonialmente, pelo ato praticado. A lesão à vida privada pode ser de ordem patrimonial ou moral, sendo assegurada à vítima uma indenização proporcional ao dano causado.²

Nesse contexto, a Europa pontilhou o marco mais significativo para a proteção contra a vigilância digital através do “Regulamento Geral de Proteção de Dados” (GDPR)⁴, implementado em 2018. O GDPR é pioneiro em estabelecer um controle rigoroso sobre a administração de informações pessoais, exigindo que as empresas obtenham consentimento explícito para coletar, processar e armazenar informações dos usuários.

Além disso, o regulamento confere aos cidadãos europeus o direito de solicitar a retirada de suas informações, impondo sanções severas para violações, o GDPR não apenas elevou o padrão de proteção de dados na Europa, mas também inspirou legislações semelhantes em outras partes do mundo, criando uma referência global.

Trazendo esse contexto para as américas, os Estados Unidos adotam a proteção jurídica no contexto da vigilância digital de forma mais fragmentada e menos abrangente do que na Europa, as leis variam de acordo com o estado, com a Califórnia liderando o caminho ao aprovar o California Consumer Privacy Act (Lei de Privacidade do Consumidor da Califórnia)⁵ com a sigla (CCPA) em 2020.

Essa legislação oferece aos residentes da Califórnia direitos como o de saber quais dados estão sendo coletados e o de proibir a venda dessas informações, no entanto, a nível federal, os Estados Unidos ainda carecem de uma lei abrangente semelhante ao GDPR, o que permite que grandes empresas de tecnologia, como *Google* e *Facebook*, continuem a operar com maior liberdade na coleta de dados.

No Brasil, a elaboração da Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, representou um avanço crucial na proteção jurídica dos dados pessoais, inspirada em grande parte no GDPR europeu, a LGPD impõe normas rígidas para o tratamento de dados, exigindo o consentimento informado e a transparência das empresas que manipulam informações pessoais.

A lei também prevê a criação da Autoridade Nacional de Proteção de Dados (ANPD), responsável pela supervisão e execução das regulamentações. A LGPD marca uma evolução no cenário brasileiro, que até então não possuía uma regulamentação consistente em relação ao processamento de dados na esfera digital, e coloca o Brasil em sintonia com as tendências internacionais de proteção à privacidade.

Embora a Europa tenha se consolidado como a região com a legislação mais avançada em relação à vigilância digital, tanto os Estados Unidos quanto o Brasil começam a dar passos significativos em direção a uma proteção mais robusta dos dados dos cidadãos, no entanto, o ritmo acelerado da inovação tecnológica exige que essas legislações estejam em constante revisão e aprimoramento, novos desafios, como o uso de sistemas de inteligência artificial para vigilância e obtenção de informações biométricas, demandam respostas legislativas ágeis para garantir que os direitos individuais não sejam suprimidos pelo poder crescente das grandes corporações.

A proteção jurídica no contexto do monitoramento digital é, portanto, um campo em constante transformação, à medida que novas tecnologias surgem, o direito precisa evoluir para salvaguardar as liberdades civis, o GDPR europeu, o CCPA nos Estados Unidos e a LGPD no Brasil são exemplos de como diferentes países têm buscado enfrentar o desafio da vigilância digital, cada um com suas particularidades e limitações, a tendência, contudo, é que o futuro traga uma convergência dessas legislações em um esforço global para proteger a privacidade em um mundo cada vez mais interconectado.

2. Direito à Inviolabilidade das Comunicações

O direito à inviolabilidade das comunicações está previsto no art. 5º, inciso XII da Constituição Federal de 1988,⁶ garantindo que as comunicações telefônicas, telegráficas, de dados e correspondências sejam protegidas contra interceptações, a não ser em casos extraordinários previstos em lei, este direito é fundamental para preservar a liberdade individual, à proteção da privacidade e à segurança dos dados, sendo de especial relevância no mundo digital, onde dados circulam em alta velocidade a todo momento.

A Lei Geral de Proteção de Dados (LGPD),⁷ ao disciplinar o tratamento de dados pessoais, reafirma o direito à inviolabilidade das comunicações ao estabelecer, em seu art. 6º, a necessidade de medidas de segurança e confidencialidade na manipulação de informações pessoais, a coleta e o uso de dados, por exemplo, precisam respeitar a integridade das comunicações entre os indivíduos, garantindo que informações privadas não sejam violadas ou interceptadas sem autorização legal. De acordo com Tarcísio Teixeira :

O sigilo da correspondência, da comunicação e dos dados são questões bem problemáticas no âmbito da internet, tendo em vista a grande possibilidade de serem devassados. O direito ao sigilo da correspondência, da comunicação e dos dados está relacionado a sua inviolabilidade. Tal inviolabilidade está diretamente ligada ao direito à privacidade, pois este alberga a proteção dos dados e fatos privados de uma pessoa. A correspondência, a comunicação e os dados das pessoas são invioláveis. Isso quer dizer que ninguém pode ter acesso ao seu conteúdo, romper seu sigilo, o conteúdo deve ficar restrito àquele que emite e àquele que recebe.²

No âmbito do Marco Civil da Internet, o art. 7º “assegura a inviolabilidade e o sigilo do fluxo de comunicações por meio da internet”,⁸ reforçando o direito de não ser monitorado indevidamente, o descumprimento dessas garantias pode resultar em responsabilidade civil e penal para os infratores, conforme disposto no Código Penal (art. 151), que “criminaliza a violação de correspondência, incluindo comunicações digitais”.⁹

Assim, as empresas de tecnologia e órgãos estatais precisam atuar com extrema cautela para evitar violações que comprometam as comunicações dos cidadãos, uma vez que o monitoramento não autorizado de dados pode ferir tanto a privacidade quanto a inviolabilidade das comunicações.

Portanto, o direito à inviolabilidade das comunicações, inicialmente proposto na Constituição Federal de 1988, ganha novos contornos e reforços com a LGPD, o Marco Civil da Internet e a EC 115/2022, essas normativas garantem que as comunicações, especialmente no meio digital, sejam protegidas contra qualquer violação indevida, assegurando a proteção da privacidade e a segurança das informações transmitidas.

2.1 Direito à Privacidade

O direito à privacidade está assegurado no art. 5º, inciso X da Constituição Federal, garantindo a todos os cidadãos o respeito à privacidade, à intimidade e à honra. Este direito é essencial para proteger os indivíduos contra interferências indevidas em sua vida pessoal e familiar, bem como para assegurar a livre autodeterminação no ambiente digital, com a era da informação impõe novos desafios, especialmente com o avanço das tecnologias de vigilância e o uso extensivo de informações pessoais. De acordo com José Afonso da Silva que dispõe:

O intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadramento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilitada a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendam a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.¹¹

A LGPD, em seu art. 2º, inciso I, reconhece o respeito à privacidade como princípio fundamental, regulando o processamento de informações pessoais para proteger a privacidade dos usuários no ambiente digital.

Empresas que captam informações pessoais devem garantir que sua utilização respeite os limites estabelecidos, evitando abusos que possam violar a privacidade, como o compartilhamento e coleta de dados sensíveis não autorizados, a coleta, armazenamento e uso de dados devem ser realizados apenas com o consentimento expresso dos titulares, o que evita que a privacidade seja comprometida, qualquer ato que desrespeite essas normas pode gerar responsabilidade civil e penal. Conforme Tarcísio Teixeira:

A violação da privacidade dá à vítima o direito de buscar a reparação do dano junto ao agente causador, que, demonstrado o dano e nexo causal, responde, patrimonialmente, pelo ato praticado. A lesão à vida privada pode ser de ordem patrimonial ou moral, sendo assegurada à vítima uma indenização proporcional ao dano causado.²

O Código Penal, em seu art. 154-A, prevê o crime de invasão de dispositivo informático, uma proteção que visa diretamente a privacidade no recinto digital, punindo a violação de sistemas informáticos ou redes privadas. Assim, o direito à privacidade, garantido pela Constituição, tem sido constantemente fortalecido por legislação brasileira, que regulam o uso de dados pessoais e protegem os indivíduos contra violações.

2.2 Direito à Intimidade

O direito à intimidade é assegurado no art. 5º, com o inciso X da Constituição Federal de 1988, como uma das garantias mais relevantes da vida privada, diferente do direito à privacidade, que protege o controle de informações pessoais em um sentido amplo, o direito à intimidade resguarda aspectos mais íntimos da vida pessoal, incluindo questões que dizem respeito à identidade pessoal, relações familiares e afins.

Visto isso, com o avanço das tecnologias digitais, esse direito ganhou importância ainda maior. Assim, a LGPD oferece salvaguardas para garantir que a intimidade dos indivíduos seja preservada no ambiente digital. A lei estabelece, em seu art. 6º, a necessidade de respeito à autodeterminação informativa, o que implica que o processamento de informações pessoais íntimas deve ser feito com o máximo de cautela, garantindo que não sejam expostos aspectos da vida privada sem o consentimento explícito da pessoa envolvida. Além disso, José Afonso da Silva de acordo com o Constituição Federal dispõe que:

A vida privada, artigo 5, inciso X da CF, é aquela que, em última análise, integra a esfera íntima da pessoa, porque é repositório de segredos e particularidades do foro moral e íntimo do indivíduo. A vida interna que se debruça sobre a mesma pessoa, sobre seus membros de sua família, sobre seus amigos é inviolável nos termos da constituição.¹¹

Nesta seara, o Marco Civil da Internet, em seu art. 7º, também protege a intimidade dos usuários ao garantir o sigilo das informações pessoais e comunicações privadas, esse disposto legal assegura que a intimidade de cada indivíduo será respeitada no ambiente digital, limitando o acesso a informações pessoais e proibindo a disseminação sem autorização, o que pode acarretar obrigação civil e criminal, conforme o direito civil e penal.

Assim, o direito à intimidade, protegido pela Constituição e reforçado pela LGPD, pelo Marco Civil da Internet e pela Emenda Constitucional 115/2022, assegura que os aspectos mais pessoais da vida de cada indivíduo sejam resguardados contra invasões indevidas.

2.2.1 Princípio da Dignidade da Pessoa Humana

O princípio da dignidade da pessoa humana é o pilar central da proteção, direitos e garantias fundamentais na Constituição Federal de 1988, conforme disposto no art. 1º, inciso III, este princípio eleva o indivíduo ao núcleo do sistema jurídico, garantindo-lhe o respeito como ser humano, em sua essência e autonomia.

No contexto digital, a dignidade da pessoa humana adquire novas dimensões, especialmente com o crescimento das tecnologias de vigilância e coleta massiva de dados pessoais, o que impõe novos desafios para a proteção e respeito à individualidade. Conforme Sylvio Motta que sana as dúvidas dizendo que:

De acordo com o artigo 1º, inciso III, da Constituição, a dignidade da pessoa humana é um princípio fundamental que estabelece a supremacia do valor intrínseco do ser humano. Esse preceito basilar reconhece que o indivíduo possui um valor inerente que precede qualquer outra consideração. Em outras palavras, a dignidade humana é um valor absoluto que deve ser respeitado e protegido acima de todos os demais interesses. Isso significa que as leis e políticas devem ser orientadas para preservar e promover a dignidade de cada pessoa, considerando-a como fim em si mesma, e não como meio para alcançar outros objetivos. Assim, a dignidade da pessoa humana se torna um parâmetro ético e jurídico para avaliar a legitimidade das ações estatais e da sociedade.¹²

A Lei Geral de Proteção de Dados (LGPD) foi um marco importante para garantir a preservação da dignidade humana no ambiente digital, ao disciplinar o uso de dados pessoais pelas empresas de tecnologia, no art. 2º, inciso I, da LGPD, destaca-se a valorização da privacidade e do direito de decidir sobre as próprias informações como princípios basilares, refletindo a essência da dignidade humana, nesse contexto, o uso abusivo de dados, como no caso de monitoramento não consentido, fere diretamente esse princípio, reduzindo o indivíduo a um simples objeto de análise, sem consideração pela sua autonomia.

Nesta seara, o Marco Civil da Internet, por sua vez, vem também reforçando o valor da dignidade humana ao garantir direitos como a liberdade de se expressar e o respeito à privacidade, o art. 7º do Marco Civil explicita o direito à proteção das informações privadas, impondo limites à coleta e tratamento de informações digitais, diante disso, a vigilância desmedida e sem critérios legais abala não só a privacidade, mas a própria dignidade, visto que coloca o indivíduo em uma constante posição de vulnerabilidade. De acordo com Adriana Espíndola Corrêa que informa:

A finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção e a não discriminação, permeadas pelo princípio da boa-fé, perfazem a constelação principiológica da LGPD que, por óbvio,

é emoldurada pelos princípios constitucionalmente previstos na Carta de 1988 e se ampara em instrumentos jurídicos previstos em outras searas, para além do direito digital, como a civil, a penal e a consumerista.¹³

Diante dos novos desafios trazidos com a presente revolução tecnológica, o legislador encontrou-se diante da necessidade de elevar a segurança das informações pessoais para incluí-los na categoria de direito e garantias essenciais, colocando sob tutela da União o dever de resguardá-los ao promulgar a Emenda Constitucional 115 de 2022.¹⁰

Reconhece a segurança das informações como um direito primordial no art. 5º, inciso LXXIX da Constituição, a dignidade do indivíduo obteve mais força na esfera digital, essa emenda constitucional incorpora explicitamente a necessidade de proteger a privacidade e a integridade dos dados pessoais, reconhecendo o papel fundamental que essas proteções desempenham na manutenção da dignidade.

Assim, o princípio da dignidade da pessoa humana permeia todo o sistema jurídico, especialmente em tempos de transformação digital, a LGPD, o Marco Civil da Internet e a EC 115/2022 são instrumentos legais que reafirmam esse princípio, buscando equilibrar o progresso tecnológico com o respeito profundo pela dignidade e autonomia de cada cidadão.

3. Sistemas operacionais voltados para o monitoramento

A crescente adesão de sistemas operacionais voltados para o monitoramento tem suscitado preocupações significativas acerca da privacidade dos usuários. A coleta de dados, muitas vezes, visa informações sensíveis, sendo que muitos desses sistemas monitoram dados pessoais como localização, hábitos de uso e preferências.

Tal prática pode resultar em invasões à privacidade, uma vez que, frequentemente, os usuários não têm clareza sobre quais dados estão sendo coletados e como serão utilizados, essa falta de transparência faz com que os direitos dos indivíduos sejam violados de maneira imperceptível, dificultando a identificação das infrações por parte dos afetados.

Ademais, o armazenamento de grandes quantidades de dados aumenta consideravelmente o risco de vazamentos e acessos não autorizados, expondo informações pessoais que deveriam ser resguardadas, essa situação propicia, ainda, o uso indevido de dados, que, uma vez coletados, podem ser utilizados para fins comerciais ou vendidos a terceiros, sem o consentimento explícito dos usuários.

A falta de responsabilidade das empresas por vazamentos de dados, especialmente aqueles monitorados sem a devida autorização dos usuários, é uma questão crítica na era digital, este problema levanta preocupações éticas e jurídicas, refletindo uma falha nas práticas de proteção de dados e na transparência das operações das empresas, essas empresas são responsáveis por garantir a proteção dos dados dos usuários desde a coleta até o descarte.

Todavia, reverberando a realidade dos fatos de como esses dados têm sido tratados, fica evidente a fragilidade no resguardo das informações pessoais dos usuários, deixando claro que a coleta de dados pessoais pelas empresas de tecnologia é uma ameaça à privacidade e à segurança dos cidadãos.

3.1 A Influência das Empresas de Tecnologia na Economia e no Comportamento do Consumidor

As grandes empresas de tecnologia, as famosas big tech, como *Google*, *Facebook*, *Amazon*, *Apple* e *Microsoft*, exercem um domínio considerável no cotidiano da sociedade, influenciando profundamente a maneira como os indivíduos pensam, agem e vivem. Esse monitoramento constante,

realizado pelas redes sociais, ocorre em função do fornecimento contínuo de dados pessoais pelos usuários, essa prática é conhecida como bolha de informação.

A bolha de informação são algoritmos dessas plataformas que são projetados para analisar o comportamento dos usuários, priorizando a exibição de opiniões e conteúdos que correspondem aos seus interesses. Dessa forma, o usuário é exposto a uma seleção limitada de informações, o que pode restringir sua visão de mundo e reforçar crenças pré-existentes.

De acordo com o “Documentário da Plataforma Streaming *NETFLIX* O dilema das redes”¹⁴ as consequências sociais vão além do indivíduo; elas afetam a coesão social e a democracia, a falta de diálogo entre diferentes grupos pode resultar em desconfiança e animosidade, prejudicando o tecido social, a incapacidade de ouvir e compreender perspectivas alternativas pode transformar debates em confrontos, minando a capacidade de resolução pacífica de conflitos. Desta forma é levantada diversas questões jurídicas, especialmente no que tange à violação de direitos fundamentais.

As grandes empresas de tecnologia, comumente denominadas big tech, exercem uma influência significativa sobre a economia global, estas empresas desempenham um papel crucial na formação de tendências relacionadas à inovação, privacidade de dados e comportamento do consumidor, sua atuação não se limita apenas ao desenvolvimento de produtos, mas também à reconfiguração de setores inteiros, estabelecendo novos paradigmas de mercado.

No âmbito da pesquisa e desenvolvimento, as big tech são líderes, impulsionando inovações em diversas áreas, como tecnologia da informação, inteligência artificial, e-commerce e serviços digitais. Este dinamismo inovador não apenas resulta na criação de novos produtos e serviços, mas também redefine a forma como os consumidores interagem com o mercado e entre si.

A interação entre essas empresas e os consumidores é mediada por algoritmos sofisticados, que personalizam experiências e anúncios, tal personalização influencia diretamente as decisões de compra, alterando hábitos de consumo e criando novas dinâmicas de mercado.

Ademais, para Brittany Kaiser as estratégias utilizadas pelas big tech para manipular e direcionar a atenção dos usuários são de natureza complexa e multifacetada, a atenção humana, atualmente, se configurou como uma mercadoria valiosa, suscetível à monetização, as empresas de tecnologia competem intensamente para capturar e monetizar essa atenção, criando um ambiente de mercado em que a atenção do usuário se torna o principal recurso.

A predominância de anúncios direcionados e de estratégias de engajamento evidencia essa dinâmica. A maioria dos serviços digitais gratuitos, como redes sociais, aplicativos e plataformas de vídeos online, é sustentada por modelos de publicidade, em vez de pagarem diretamente pelos serviços oferecidos, os usuários pagam com sua atenção, que, por sua vez, é vendida a anunciantes em busca de maximizar sua visibilidade e impactar o comportamento do consumidor, essa abordagem suscita reflexões profundas sobre a natureza do relacionamento entre os usuários e as plataformas digitais.

A exploração da atenção humana como um recurso comercial levanta questões éticas relevantes, neste contexto, a afirmação do ex-designer do *Google*, e especialista em ética tecnológica, o americano Tristan Harris, no documentário, “O dilema das redes” torna-se pertinente ao falar que, Se você não está pagando pelo produto, então você é o produto.

Esta declaração ressalta a realidade de que, ao utilizar serviços aparentemente gratuitos, os usuários se tornam, de fato, o objeto da transação, servindo como fonte de dados valiosos para as empresas que, em última análise, se beneficiam dessa interação.

A discussão acerca da privacidade de dados também é crucial nesse contexto, a coleta e o uso de dados pessoais pelas big tech demandam uma análise crítica, considerando as implicações éticas e legais. Portanto, a influência das big tech na economia e no comportamento do consumidor é um

fenômeno complexo que requer uma abordagem multidisciplinar. De acordo com Edson Pires, destaca que:

Respeito à privacidade é um dos fundamentos da LGPD (art. 2º, I). Com o advento das redes sociais e a superexposição espontânea a que muitas pessoas se submeteram, parecia que a privacidade tinha perdido a importância. Em 9 de janeiro de 2010, o fundador e CEO do Facebook, Mark Zuckerberg, afirmou que "A era da privacidade chegou ao fim". Essa afirmação foi feita no contexto da popularização das redes sociais, nas quais as pessoas compartilham uma infinidade de informações pessoais.¹⁵

No entanto, esta superexposição ao ambiente virtual é preocupante, as práticas de vigilância a longo prazo entram frequentemente em conflito com os direitos fundamentais existentes na constituição, resultando potencialmente na perda da privacidade e da autonomia individual. Por isso, é fundamental que tanto os legisladores quanto a sociedade civil se mobilizem para entender e regular essa dinâmica, garantindo que a tecnologia sirva ao bem comum e não apenas aos interesses corporativos.

3.2 O Papel da TICs e Big data no monitoramento digital

As Tecnologias da Informação e Comunicação (TICs) desempenham um papel central e estratégico no contexto do monitoramento digital, permitindo a coleta, análise e divulgação de informações de maneira eficiente, automatizada e em tempo real.

Essas tecnologias são incluídas por diversos componentes, tais como hardware, software, sistemas de telecomunicações e redes de comunicação, que em conjunto possibilitam a interconexão de sistemas e pessoas em escala global, o uso das TICs é amplo e diversificado, abrangendo setores como educação, saúde, negócios, governança e entretenimento, proporcionando uma transformação profunda na maneira como os indivíduos se comunicam, acessam informações e realizam transações diárias

O estudioso e especialista Viktor Mayer-Shönberger ao falar da Big Data, explica que é uma tecnologia que processa e armazena grandes quantidades de dados, sendo amplamente utilizada para identificar padrões específicos de comportamento, especialmente em plataformas de redes sociais, como *Facebook*, *Twitter* e *Instagram*.

Por meio de ferramentas avançadas de mineração de dados e algoritmos de Inteligência Artificial (IA), essa tecnologia possibilita o processamento de grandes volumes de informações, os algoritmos referidos são usados para categorizar e classificar os usuários com base em suas interações, comportamentos e mensagens.

Contudo, o uso intensivo das Tecnologias da Informação e Comunicação (TICs), especialmente no campo do Big Data, suscita preocupações críticas no que tange à privacidade, à proteção de dados e à preservação dos direitos fundamentais dos cidadãos.

O Big Data, ao permitir a coleta, armazenamento e análise massiva de informações, possibilita a identificação de padrões de comportamento e a criação de perfis detalhados dos usuários, muitas vezes sem que estes tenham plena ciência da extensão do monitoramento a que estão sujeitos.

Analisando o “Documentário da plataforma Streaming *NETFLIX* O dilema das redes”,¹⁴ vemos como é usada as plataformas digitais, como redes sociais (*Facebook*, *Twitter*, *Instagram*), amplia o volume e a diversidade de dados disponíveis para processamento por meio avançados de mineração de dados e algoritmos de Inteligência Artificial (IA).

Esses mecanismos classifica e categoriza os usuários com base em suas interações, preferências, comportamentos e mensagens, criando um cenário no qual informações pessoais, que podem incluir

hábitos de consumo, localização geográfica e até tendências ideológicas, são capturadas e utilizadas para diferentes fins, como marketing direcionado, controle social ou mesmo decisões automatizadas.

Embora essas tecnologias tragam benefícios inegáveis, como a personalização de serviços e a eficiência operacional em diversos setores, seu uso também impõe desafios éticos e legais, a coleta e o processamento de dados em larga escala podem comprometer a autonomia individual, uma vez que os cidadãos possam ser rastreados, monitorados e categorizados sem o consentimento devido informado.

É imprescindível que as organizações adotem práticas transparentes e éticas em relação à coleta e ao uso de dados pessoais, respeitando os direitos fundamentais à privacidade. Medidas de proteção, como a implementação de políticas claras de consentimento e a adoção de tecnologias que assegurem a segurança da informação, são essenciais para mitigar os riscos associados. Além disso, a conscientização dos usuários sobre seus direitos e sobre as práticas de coleta de dados é fundamental para a proteção da privacidade em um ambiente cada vez mais digital e monitorado.

Portanto, é vital que se estabeleçam normas e regulamentações robustas que garantam a proteção dos dados pessoais e promovam a responsabilização das empresas em caso de violação dos direitos dos usuários. A privacidade deve ser considerada um direito inalienável, sendo essencial para a dignidade humana e para a preservação da liberdade individual em um mundo interconectado.

3.2.1 Capitalismo de Vigilância Digital

O capitalismo de vigilância digital é um fenômeno cada vez mais debatido em estudos contemporâneos sobre tecnologia e sociedade, ele se refere à prática adotada por grandes empresas de tecnologia que extraem, analisam e utilizam dados pessoais em larga escala para fins comerciais.

Esse modelo econômico, amplamente analisado por estudiosos como Shoshana Zuboff, baseia-se na transformação de dados dos usuários em um recurso valioso, vendendo previsões sobre o comportamento humano para publicidade direcionada, embora pareça inofensivo para muitos usuários, o impacto profundo desse tipo de capitalismo levanta sérias questões sobre privacidade, autonomia e direitos individuais. Além disso, dispõe com Shoshana Zuboff que:

O capitalismo de vigilância como o processo de coleta unilateral e opaca de dados baseado na experiência humana. Esses dados, quando não usados para melhorar produtos e serviços, são considerados "superávit comportamental" e são utilizados para prever comportamentos.¹⁶

Na prática, o capitalismo de vigilância se manifesta por meio de plataformas digitais como *Google*, *Facebook* e *Amazon*, que coletam dados constantemente enquanto os usuários navegam, fazem compras ou interagem online, esses dados vão muito além de preferências explícitas, incluem padrões de comportamento, localizações, contatos, hábitos de consumo e até microexpressões faciais, capturadas por algoritmos.

Os principais sistemas que coletam esses dados estão integrados diretamente nas ferramentas que usamos diariamente, por exemplo, o Sistema de Geolocalização (GPS), presente em smartphones e aplicativos como *Google Maps* e redes sociais, rastreia a localização em tempo real, gerando dados sobre os lugares frequentados pelo usuário.

Navegadores de internet como *Google Chrome* e *Safari*, por sua vez, utilizam *cookies* e *tracking pixels* (pixel de rastreamento) trata-se de um código HTML que pode ser incorporado em sites, e-mails ou comentários para coletar dados sobre os visitantes, como horário de leitura, endereço IP, localização aproximada e tipo de dispositivo, outro exemplo, é o uso de sistemas de reconhecimento facial, como o *Face ID* da *Apple* ou o *DeepFace* do *Facebook*, que coletam dados biométricos dos usuários, podendo até detectar emoções.

Além disso, assistentes virtuais como *Siri*, *Alexa* e *Google Assistant*, amplamente presentes em dispositivos inteligentes, coletam dados de voz e comportamento, ajustando suas recomendações com base nas interações diárias, esses mecanismos, somados ao uso constante de *cookies* e *tracking pixels*, formam um ecossistema onde as empresas monitoram e analisam profundamente a vida digital dos usuários, transformando dados pessoais em commodities altamente lucrativas. Nessa esteira, Guidolini destacam que:

O ramo da tecnologia, altamente monopolizado, tem gerado seus lucros principalmente através da extração dos dados pessoais de usuários para comercialização. Empresas como o Google, Facebook e a Microsoft, utilizam essas informações para alimentar inteligências artificiais capazes de antecipar o comportamento humano e, assim, vender aos anunciantes previsões sobre as ações dos usuários. Dessa forma, para facilitar o aumento da acumulação de capital, tornou-se necessário, não apenas prever, mas modificar o comportamento humano. O capitalismo, em seu infindável processo de valorização, passou a mercantilizar a própria experiência humana, utilizando-a como matéria-prima para processos comerciais, com o objetivo de aumentar exponencialmente a massa de lucro.¹⁷

Esse intrincado sistema de vigilância digital cria um ambiente onde a privacidade individual está constantemente sendo invadida e monetizada, a coleta de dados, realizada sem transparência ou verdadeiro consentimento, coloca em xeque a autonomia dos usuários sobre suas informações. O desafio, tanto para os governos quanto para os indivíduos, é compreender a profundidade dessa vigilância e adotar medidas eficazes para limitar o controle das corporações sobre a vida digital.

Ainda assim, o que torna esse modelo mais preocupante é o fato de que a maioria das legislações ainda não estão totalmente preparadas para lidar com o alcance dessa coleta massiva de dados, mesmo com a aprovação de leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia.

Os mecanismos de controle muitas vezes não são suficientes para conter os abusos, as empresas tecnológicas se valem de termos de uso complexos, que raramente são lidos ou compreendidos pelos usuários, legitimando o acesso a uma vasta quantidade de dados sensíveis, muitas vezes sem consentimento totalmente informado.

Em última análise, o capitalismo de vigilância digital representa uma mudança paradigmática nas relações de poder entre empresas e indivíduos. Para Koerner (2021), “o capitalismo de vigilância viola a privacidade e invade os domínios de existência, porque essa é a dinâmica de acumulação do seu setor dominante, o capital de plataforma, que necessita extrair dados para os seus negócios”.¹⁸

Enquanto o usuário pensa estar apenas navegando ou utilizando serviços gratuitos, na verdade está sendo monitorado, categorizado e transformado em um produto, o desafio de combater esse modelo reside na criação de uma regulamentação mais robusta e na conscientização do público sobre como suas informações são utilizadas.

3.2.2 Jurisprudências correlatas ao contexto do compartilhamento de dados

O julgamento realizado pelo STJ avalia a privacidade, com base no Marco Civil da Internet (Lei n. 12.965/2014). No caso específico, determinada empresa alegou que um vídeo difamatório foi postado anonimamente nas redes sociais, prejudicando sua imagem, e pediu tanto a remoção do vídeo quanto a identificação dos usuários que o compartilharam.

Todavia, o relator do processo destacou que, embora a lei permita a solicitação de dados mediante autorização judicial, é necessário que a parte interessada faculte concretos de ilicitude, justificativa da utilidade dos registros e a delimitação do período a ser investigado.

O ministro relator Luis Felipe Salomão, em seu voto, reforçou que a proteção à privacidade dos usuários não pode ser desconsiderada, mesmo em casos de postagens difamatórias. O direito à

privacidade deve prevalecer sobre pedidos genéricos de quebra de sigilo, especialmente quando não há provas suficientes que comprovem a ilicitude da conduta dos usuários que apenas compartilharam o conteúdo.

Assim, a decisão evita a quebra indiscriminada do sigilo dos usuários, protegendo seus dados e informações pessoais, salvo nos casos devidamente justificados e especificados.

RECURSO ESPECIAL. OBRIGAÇÃO DE FAZER C/C EXIBIÇÃO DE DOCUMENTOS. POSTAGEM DE VÍDEO CONTENDO INFORMAÇÕES ALEGADAMENTE FALSAS, PREJUDICIAIS À IMAGEM DA SOCIEDADE EMPRESÁRIA AUTORA, EM REDE SOCIAL. QUEBRA DO SIGILO DE TODOS OS USUÁRIOS QUE COMPARTILHARAM O CONTEÚDO POTENCIALMENTE DIFAMATÓRIO NA PLATAFORMA DO FACEBOOK. IMPOSSIBILIDADE. PLEITO SEM EXPOSIÇÃO DE FUNDADAS RAZÕES PARA A QUEBRA. MARCO CIVIL DA INTERNET (LEI N. 12.965/2014, ART. 22). PRESERVAÇÃO DA PRIVACIDADE E DO DIREITO AO SIGILO DE DADOS. 5. Nos termos da Lei n. 12.965/2014 (art. 22), a parte interessada poderá pleitear ao juízo, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Para tanto, sob pena de admissibilidade, exige a norma que haja: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros (parágrafo único). 6. É vedado ao provedor de aplicações de internet - em pedido genérico e coletivo, sem a especificação mínima de uma conduta ilícita realizada - fornecer dados, de forma indiscriminada, dos usuários que tenham compartilhado determinada postagem. 7. Na espécie, a recorrida não trouxe nenhum elemento, nem sequer descreveu indícios de ilicitude da conduta dos usuários que, por qualquer motivo, acabaram por apenas compartilhar o vídeo com conteúdo difamador, limitando-se a identificar a página do autor da postagem e de um ex-funcionário que também teria publicado o vídeo em seu perfil. 8. Assim, sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, deve prevalecer a privacidade dos usuários. Não se pode subjugar o direito à privacidade a ponto de permitir a quebra indiscriminada do sigilo dos registros, com informações de foro íntimo dos usuários, tão somente pelo fato de terem compartilhado determinado vídeo que, depois se soube, era falso. (Processo nº 0304874-38.2016.8.24.0005 - Tribunal de Justiça de Santa Catarina) (STJ - REsp n. 1.859.665/SC, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 9/3/2021, DJe de 20/4/2021).¹⁹

Evidencia-se que a proteção à privacidade dos dados é um direito fundamental que deve ser rigorosamente defendido, especialmente no contexto digital. A relativização desse direito, sem a devida justificativa e controle judicial, pode comprometer a dignidade, a liberdade e a segurança dos indivíduos.

Ainda assim, o combate aos crimes e a preservação da ordem são públicos legítimos, qualquer medida que envolve a quebra de sigilo deve ser proporcional, limitada e embasada em prejuízos concretos de ilícitos, a fim de evitar abusos e garantir que a privacidade permaneça um valor essencial na sociedade democrática.

Nessa esteira, em que há a necessidade de acessar determinados dados de caráter privado respaldado na necessidade, a jurisprudência ornamentada a partir do agravo regimental no recurso em mandado de segurança, o qual a medida se apresentava adequada, necessária e proporcional, uma vez que serve como instrumento para a elucidação de delito grave, conforme a decisão do juízo da 5ª Vara Criminal de São José do Rio Preto - SP abaixo.

AGRAVO REGIMENTAL NO RECURSO EM MANDADO DE SEGURANÇA. QUEBRA DE SIGILO TELEFÔNICO E REQUISIÇÃO DE REGISTROS DE GEOLOCALIZAÇÃO. INVESTIGAÇÃO CRIMINAL. IDENTIFICAÇÃO DE

USUÁRIOS. DELIMITAÇÃO TEMPORAL E ESPACIAL. PROPORCIONALIDADE DA MEDIDA. AGRAVO REGIMENTAL DESPROVIDO. 4. Medida que está respaldada no art. 22 do Marco Civil da Internet, e em consonância com a jurisprudência da Terceira Seção desta Corte que reconheceu "a legalidade da ordem judicial que determina quebra de sigilo de dados informáticos estáticos relativos a dados pessoais e registros de conexão ou acesso a servidores, navegadores ou aplicativos de internet, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, desde que, presentes circunstâncias que denotem a existência de interesse público relevante, a decisão seja proferida por autoridade judicial competente, com fundamentação suficiente, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios mínimos que indiquem a configuração de suposta ocorrência de crime sujeito à ação penal pública." (AgRg no RMS n. 66.791/CE, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 7/12/2021, DJe de 13/12/2021) 7. In casu, a medida se apresenta adequada, necessária e proporcional, uma vez que serve como instrumento para a elucidação de delito grave - homicídio qualificado - cuja autoria delitiva dificilmente poderá ser identificada por outros meios. Ademais, não se trata de pedido de alcance indeterminado de pessoas ou genérico, eis que se limita apenas aos telefones móveis e contas GOOGLE, APPLE e FACEBOOK acessados nos dias, horas e locais mencionados nas coordenadas geográficas elencadas pela Autoridade Policial, o que será útil para trazer segurança ao juízo no momento do julgamento futuro. Além disso, o fornecimento dos dados de localização não causará gravame aos indivíduos eventualmente afetados que não tenham conexão com o delito, posto que não serão publicados e, ao final, serão descartados. (Processo nº 1507478-37.2022.8.26.0576 - Tribunal de Justiça de São Paulo) (STJ - AgRg no RMS n. 72.137/SP, relator Ministro Ribeiro Dantas, Quinta Turma, julgado em 20/2/2024, DJe de 27/2/2024).²⁰

Nessa esteira, o STF assentou o entendimento na Ação Direta de Inconstitucionalidade - 5527 ajuizada pelo partido político PR - Partido da República objetivando tornar inconstitucional as decisões em instâncias inferiores de suspensão de atividades decorrentes descumprimento de decisões judiciais voltadas ao fornecimento de dados necessários à instrução processual.

Na recente decisão do Supremo Tribunal Federal, ao interpretar o Marco Civil da Internet, este reafirma a centralidade do direito à privacidade no ordenamento jurídico brasileiro, resguardado pelo art. 5º, XII, da Constituição Federal, o tribunal foi claro ao estabelecer que, ainda que a era digital tenha ampliado as possibilidades de comunicação e interação, o conteúdo das comunicações privadas só pode ser acessado mediante ordem judicial, e restrito para fins de investigação criminal ou instrução penal.

Este representa um avanço na proteção dos direitos fundamentais em tempos de vigilância tecnológica, evitando que o sigilo das comunicações seja violado sem as devidas garantias legais, a proteção à privacidade não é apenas uma proteção individual, mas um pilar essencial da dignidade humana.

AÇÃO DIRETA INCONSTITUCIONALIDADE. LEI Nº 12.965/2014 (MARCO CIVIL DA INTERNET). SUSPENSÃO OU INTERRUÇÃO DOS SERVIÇOS FORNECIDOS POR PROVEDORES DE CONEXÃO OU APLICAÇÕES DE INTERNET DETERMINADA POR ORDEM JUDICIAL. ; (iv) julgava parcialmente procedente o pedido sucessivo de interpretação conforme a Constituição do art. 12, III e IV, da Lei nº 12.965/2014 apenas para (a) assentar que autorizada a imposição das penalidades de suspensão temporária das atividades e de proibição de exercício das atividades, aos provedores de conexão e de aplicações de internet, nos casos de descumprimento da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, inclusive em face do descumprimento, no âmbito de investigação criminal ou de instrução processual penal, de (a.1) ordem judicial para disponibilização de registro de conexão e de acesso a aplicações de internet e dados pessoais, ou (a.2) ordem judicial para

disponibilização do conteúdo de comunicações privadas específicas, quando materialmente possível o seu cumprimento, nas hipóteses e na forma de lei que estabeleça prévio leque de infrações definidas como especialmente graves, a ponto de justificar a natureza da medida; (b) ficando afastada, todavia, qualquer exegese que – isoladamente ou em combinação com o art. 7º, II e III, da Lei nº 12.965/2014 – estenda a sua hipótese de incidência de modo a abarcar o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação, o processo foi destacado pelo Ministro Alexandre de Moraes. Plenário, Sessão Virtual de 22.9.2023 a 29.9.2023. (Processo nº4000753-38.2016.1.000000 - DF - DISTRITO FEDERAL) (STF - AÇÃO DIRETA DE INCONSTITUCIONALIDADE 5.527 PROCED. : DISTRITO FEDERAL RELATORA : MIN. ROSA WEBER).²¹

Ao definir que as deliberações dos provedores de internet só podem ser aplicadas em casos específicos e mediante a preservação da segurança dos dados pessoais, o STF reitera que a privacidade digital é inviolável. A decisão vai além, ao proibir qualquer exegese que exija a fragilização dos mecanismos de criptografia como forma de cumprimento de ordens judiciais.

Esse cuidado garante que a arquitetura de proteção à privacidade na era digital continue robusta, impedindo abusos e vigilância indiscriminada. Assim, o tribunal equilibra a necessidade de investigação com o respeito aos direitos constitucionais, destacando que o avanço da tecnologia não pode significar um retrocesso na proteção dos direitos fundamentais dos cidadãos.

4. Considerações Finais

Conforme evidenciado na pesquisa, a vigilância digital é um fenômeno complexo e desafiador, particularmente no que diz respeito à proteção dos direitos essenciais. A capacidade das grandes corporações de tecnologia de inovar e moldar comportamentos de consumo por meio da coleta e análise massiva de dados não apenas redefine a interação entre consumidores e mercados, mas também levanta questões éticas e jurídicas significativas, esse cenário coloca em xeque o equilíbrio entre a inovação tecnológica e a segurança dos direitos pessoais.

A exploração da atenção humana como um recurso comercial, aliada à coleta de dados pessoais, suscita reflexões profundas sobre a ética dessas práticas e a necessidade de uma proteção legal adequada, essa superexposição dos indivíduos na esfera digital, juntamente com a vigilância intrusiva, ameaça a autonomia e a dignidade humana, destacando a urgência de um marco regulatório robusto que proteja os direitos dos cidadãos

O fortalecimento das legislações nacionais, aliado à criação de um marco regulatório internacional, constitui um conjunto de medidas essenciais para abordar o complexo problema da vigilância digital, um fenômeno que, atualmente, coloca em risco a proteção dos direitos fundamentais e a privacidade dos indivíduos.

Tais iniciativas não apenas garantiriam a conformidade das empresas com regras claras e objetivas, mas também estabeleceriam um ambiente normativo que prioriza a transparência e o consentimento informado no uso de dados pessoais. Nesse sentido, é imprescindível que tanto empresas quanto governos estejam vinculados a normas que estabeleçam diretrizes rigorosas sobre como os dados são coletados, tratados e compartilhados.

No que tange ao âmbito internacional a proposta de um tratado sobre privacidade e a segurança das informações pessoais, inspirado em legislações consolidadas, como o Regulamento Geral sobre a Proteção de Dados (GDPR) adotado na União Europeia e a Lei Geral de Proteção de Dados (LGPD) implementada no Brasil, surge como uma solução viável e necessária para em escala global.

Todavia, delimitando a problemática no âmbito nacional, o desempenho da Autoridade Nacional de Proteção de Dados (ANPD) poderia estabelecer padrões mínimos vinculada a LGPD para a captação, tratamento e armazenamento de dados, promovendo uma harmonização normativa que permita um controle mais eficaz sobre as atividades de processamento de dados pessoais.

Além disso, a regulamentação deve prever a imposição de sanções rigorosas por violações, como multas significativas, bem como a grupos interdisciplinares encarregados pela supervisão e aplicação dessas normas, com isso, é imprescindível garantir total transparência e controle ao usuário no que diz respeito ao manejo de suas informações pessoais.

Para tanto, as empresas devem ser obrigadas a fornecer informações claras, detalhadas e de fácil compreensão sobre os dados que coletam, a forma como esses dados são utilizados e com quem eles são compartilhados, essa obrigação de transparência é fundamental para que os usuários possam fazer escolhas conscientes sobre a utilização de suas informações pessoais e, conseqüentemente, exercer efetivamente seu direito à privacidade.

Nesse contexto, a implementação de soluções tecnológicas, como painéis de controle de privacidade, que sejam acessíveis aos usuários, torna-se essencial, esses painéis devem permitir que os usuários visualizem e gerencie suas informações de forma intuitiva e direta, oferecendo uma interface amigável que facilite a navegação e a compreensão das opções disponíveis.

A adoção de mecanismos que garantam a efetividade desse controle, como a possibilidade de reclamações e consultas em caso de dúvidas ou questões associadas ao manejo de dados, é igualmente essencial. As empresas devem estabelecer canais de comunicação diretos e acessíveis que permitam aos usuários exercerem seus direitos de forma prática e efetiva.

Por fim, a pesquisa evidenciou a necessidade urgente de um marco regulatório robusto que possa equilibrar o avanço tecnológico com a proteção dos direitos essenciais dos indivíduos, especialmente no que tange à privacidade, à inviolabilidade das comunicações e à dignidade humana.

As empresas de tecnologia, que dominam o cenário de vigilância digital, devem ser submetidas a regras mais claras e rigorosas, no âmbito nacional, para garantir que a coleta, o tratamento e o compartilhamento de dados ocorram de forma transparente e com o consentimento informado dos usuários. O fortalecimento das medidas de proteção à privacidade não é apenas uma questão legal, mas também uma questão de ética e respeito à autonomia individual em um universo cada vez mais conectado.

5. Referências

1- HOFFMANN-REIM, Wolfgang. **Teoria geral do direito digital**: transformação digital desafios para o direito, Editora Forense, Rio de Janeiro, 2020.

2- TEIXEIRA, Tarcisio. **Direito Digital e Processo eletrônico**. 5º Edição. Brasil. Saraiva, 2021.

3- Duarte DE, Nunes P, Lima TGL. Estudos de vigilância [livro eletrônico]. 1ª ed. Rio de Janeiro: CESeC; 2023 [citado em 5 de nov 2024]. Disponível em: https://nev.prp.usp.br/wp-content/uploads/2023/10/PANOPT_panorama_estudos-vigilancia_FINAL_1707.pdf.

4- EUR. Bruxelas. [GDPR (2016)]. **Regulamento geral da União Europeia (GDPR)**. ed. atual. 27 de abril de 2016: Parlamento Europeu, 2018. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 17 out. 2024.

- 5- EUA. Califórnia. [CCPA (2018)]. **Lei de Privacidade do Consumidor da Califórnia (CCPA)**. ed. atual. 13 de março de 2024: California State Assembly, 2018. Disponível em: <https://oag.ca.gov/privacy/ccpa>. Acesso em: 17 out. 2024.

- 6- BRASIL. [Constituição (1988)] **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 15 set. 2024.

- 7- BRASIL. [LGPD (2018)] **Lei Geral de Proteção de Dados**. Brasília, DF: Senado Federal. 2018 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm . Acesso em 25 nov. 2024.

- 8- BRASIL. **Marco Civil da Internet**. Brasília, DF: Senado Federal, 2014. Disponível em: <https://corpus927.enfam.jus.br/legislacao/INTER-14>. Acesso em: 05 out. 2024.

- 9- BRASIL. [Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940] **Código Penal**. Brasília, DF: Senado Federal, 1940 Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 set. 2024.

- 10- BRASIL. **Emenda Constitucional Nº 115**, de 10 de fevereiro de 2022, DF: Senado Federal, 2022 Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pe ssoais. Acesso em: 10 ago. 2024.

- 11- DA SILVA, José Afonso . **Curso de Direito Constitucional Positivo**. 45 ° Edição. Salvador. Editora JusPodivm, 2024.

- 12- MOTTA, Sylvio. **Direito Constitucional: teoria, jurisprudência e questões**. 29º Edição. Rio de janeiro: Forense, 2021.

- 13- ESPINDOLA, Adriana. **Tratado de proteção de dados pessoais**. 2º Edição, Editora forense, Rio de Janeiro, 2023.

- 14- **O DILEMA DAS REDES**. Direção: Jeff Orlowski. Estados Unidos, 2020. 1 vídeo 1h 34m. Disponível em: www.netflix.com.br. Acesso em: 19 de Set. 2024.

- 15- PIRES, Edson. **Lei Geral de Proteção de Dados Pessoais: LGPD**. 2º Edição. São Paulo: Editora Juspodivm, 2022.

- 16- ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2020.

- 17- GUIDOLINI, et. al. **Capitalismo, neoliberalismo e contemporaneidade: a sociedade em meio à pandemia**, in: Pet ufes economia, Brasil, 2020.

18- KOERNER, A. **Capitalismo e vigilância digital na sociedade democrática**. Revista Brasileira de Ciências Sociais, Disponível em: <https://www.scielo.br/j/rbcsoc/a/3RSTj7mCYh6YcHRnM8QZcYD/> Acesso em 25 out. 2024.

19- BRASIL. Superior Tribunal de Justiça. **Recurso Especial**. Preservação da privacidade e do direito ao sigilo de dados. Brasília, DF: Superior Tribunal de Justiça, [2021]. Disponível em: <https://processo.stj.jus.br/SCON/>. Acesso em: 10 out. 2024.

20- BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Mandado de Segurança**. quebra de sigilo telefônico e requisição de registros de geolocalização. Investigação criminal. Identificação de usuário. Brasília, DF: Superior Tribunal de Justiça, [2024]. Disponível em: <https://processo.stj.jus.br/SCON/>. Acesso em: 12 out. 2024.

21- BRASIL. Superior Tribunal Federal. **Ação Direta Inconstitucionalidade**. Suspensão ou interrupção dos serviços fornecidos por provedores de conexão ou aplicação de internet determinada por ordem judicial. Brasília, DF: Superior Tribunal Federal, [2023]. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>. Acesso em: 12 out. 2024.

22- SOUZA, Lucas; AUGUSTO, Olavo; EDUARDO, Paulo. **Monografia Jurídica**; guia prático para elaboração do trabalho científico e orientação metodológica. 2º Edição, São Paulo: Editora Método, 2015.