UNIVERSIDADE FEDERAL DE OURO PRETO
Departamento de Direito

Luana Assunção Fernandes Teixeira

O AVANÇO DO TECNOAUTORITARISMO NO BRASIL: repensando a autodeterminação informacional na era do capitalismo de vigilância

Ouro Preto
2024

Luana Assunção Fernandes Teixeira

O AVANÇO DO TECNOAUTORITARISMO NO BRASIL: repensando a autodeterminação informacional na era do capitalismo de vigilância

Monografia apresentada ao curso de Graduação em Direito da Universidade Federal de Ouro Preto, como requisito parcial para obtenção do título de bacharel em Direito Área de concentração: Direito Civil

Orientadora: Juliana Evangelista de Almeida

Ouro Preto

2024

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Luana Assunção Fernandes Teixeira

O AVANÇO DO TECNOAUTORITARISMO NO BRASIL:
Repensando a Autodeterminação Informacional na Era do Capitalismo de Vigilância

Monografia apresentada ao Curso de Direito da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 15 de outubro de 2024

Membros da banca

Doutora - Juliana Evangelista de Almeida- Orientador(a) Universidade Federal de Ouro Preto
Doutor - Federico Nunes de Matos- Universidade Federal de Ouro Preto
Mestranda - Bárbara Maria Moreira Pimentel - Universidade Federal de Ouro Preto

[Juliana Evangelista de Almeida, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 15/10/2024

Documento assinado eletronicamente por **Juliana Evangelista de Almeida**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 16/10/2024, às 11:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0795892** e o código CRC **4ECB55DF**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3559-1545 - www.ufop.br

AGRADECIMENTOS

Em primeiro lugar, agradeço minha família por todo apoio durante minha trajetória universitária e por sempre me orientarem para o caminho da educação e do conhecimento. Em especial, meus avós, Lourdinha e João, e minha mãe, Ana.

Agradeço à Monica e Liza, por me proporcionarem o melhor tratamento e apoio para enfrentar os desafios universitários sem abrir mão do bem mais precioso da vida, que é a saúde.

Agradeço à Líder Aviação e toda a equipe de TI, em especial meus queridos chefes, Celina e Junio, por receberem uma estudante de Direito em um setor de tecnologia e por permitirem que eu aprendesse a prática da proteção de dados pessoais.

Agradeço a professora Juliana, por aceitar me orientar neste trabalho e compartilhar comigo sua experiência e conhecimentos em proteção de dados.

Por fim, agradeço à grandiosa Universidade Federal de Ouro Preto por me capacitar para ser não apenas uma profissional do Direito, mas também por me qualificar como um ser humano mais consciente dos meus privilégios e que se preocupa com questões e problemas sociais. Assim, deixo a UFOP com a certeza de que o conhecimento é a arma mais poderosa para enfrentar a vida pessoal e o mundo profissional.

> *“Olhar para trás após uma longa caminhada pode fazer perder a noção da distância que percorremos, mas se nos detivermos em nossa imagem, quando a iniciamos e ao término, certamente nos lembraremos o quanto nos custou chegar até o ponto final, e hoje temos a impressão de que tudo começou ontem. Não somos os mesmos, mas sabemos mais uns dos outros. E é por esse motivo que dizer adeus se torna complicado! Digamos então que nada se perderá. Pelo menos dentro da gente.”*
>
> *João Guimarães Rosa*

RESUMO

Em razão do desenvolvimento de tecnologias sustentadas pela coleta intensiva de dados pessoais, este trabalho possui o propósito de abordar como o Estado faz o uso de ferramentas que burlam sistemas de segurança para permitir a extração de dados de dispositivos pessoais dos cidadãos. Nesse sentido, busca-se argumentar que a partir do momento em que entidades estatais se apropriam de tecnologias e dispositivos que permitem a coleta de quantidades massivas de dados pessoais dos cidadãos brasileiros sem o devido processo informacional, fomenta-se um ambiente de relativização de direitos personalíssimos como a autodeterminação informacional, ou seja, o direito dos indivíduos compreenderem e controlarem como suas informações são tratadas, o que pode contribuir para o avanço de práticas autoritárias, como vigilância, controle e manipulação. Assim, o objetivo deste trabalho é, a partir do levantamento bibliográfico e documental, compreender o impacto do tecnoautoritarismo no contexto brasileiro ao investigar as intricadas relações entre tecnologia, autoritarismo e violações dos direitos à privacidade e à personalidade. Para tanto, almeja-se documentar a extensão dessas práticas diante da Lei Geral de Proteção de Dados e também questionar os fundamentos legais que sustentam a utilização de dispositivos tecnológicos por autoridades estatais

Palavras-chave: Tecnoautoritarismo. Autodeterminação informacional. Proteção de Dados. Privacidade.

ABSTRACT

Due to the development of technologies sustained by the intensive collection of personal data, this work aims to address how the State uses tools that bypass security systems to enable the extraction of data from citizens' personal devices. In this context, the aim is to argue that from the moment state entities appropriate technologies and devices that allow the collection of massive amounts of personal data from Brazilian citizens without the due informational process, an environment is fostered where personal rights such as informational self-determination are relativized, that is, the fundamental right of individuals to understand and control how their information is handled, which can contribute to the advancement of authoritarian practices such as surveillance, control, and manipulation.. Therefore, this paper seeks to understand the impact of Techno-Authoritarianism in the Brazilian context by examining the complex interactions between technology, authoritarianism, and the violation of privacy and personality rights through bibliographic and documentary research. Additionally, it aims to document the extent of these practices in relation to the General Data Protection Law and to question the legal basis for the use of technological devices by state authorities.

Keywords: Techno-Authoritarianism. Informational Self-Determination. Data Protection. Privacy.

SUMÁRIO

1 INTRODUÇÃO

A evolução de dispositivos tecnológicos é responsável por proporcionar diversas facilidades para as pessoas e empresas, desde a automação de tarefas cotidianas até a otimização de processos industriais complexos. Essa constante inovação impulsiona a eficiência e a produtividade e transforma a maneira como se vive e trabalha. Com a utilização de dispositivos tecnológicos, a comunicação se torna mais instantânea, o acesso à informação se torna mais amplo e as oportunidades de negócio se expandem. Esses avanços têm um impacto significativo na sociedade e promovem mudanças em diversas áreas, como educação, saúde, transporte e entretenimento.

Como consequência, as empresas mais valiosas da atualidade são do setor de tecnologia, como as *big techs*, *Alphabet*, *Amazon*, *Apple*, *Meta* e *Microsoft*[1]. Essas empresas lideram essa revolução tecnológica com inovações que vão desde assistentes virtuais com sistemas de inteligência artificial, logística avançada e dispositivos inteligentes até plataformas de comércio eletrônico e redes sociais que conectam bilhões de pessoas.

Além do aspecto tecnológico, um elemento central que une todas essas empresas é a coleta intensiva de dados pessoais. Ao acumularem e analisarem vastas quantidades de dados sobre seus usuários, essas empresas conseguem personalizar serviços e produtos, e também influenciar comportamentos, prever tendências e direcionar campanhas publicitárias com precisão. Essa capacidade de manipulação de dados confere às *big techs* um poder sem precedentes, o que permite que elas moldem não só o mercado, mas também aspectos culturais e até políticos em escala global.

Não obstante, a utilização de dispositivos tecnológicos sustentados pela coleta massiva de dados pessoais não são práticas apenas de empresas privadas sedentas por proporcionar experiências ditas personalizadas para seus clientes, uma vez que existem também órgãos governamentais interessados nos benefícios oferecidos pela tecnologia para conseguir acessar informações pessoais que até alguns anos atrás

[1] THE WORLD'S MOST VALUABLE RESOURCE IS NO LONGER OIL, BUT DATA. The Economist. 6 de maio de 2017. Disponível em https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em 10 de maio de 2024.

não seria possível em razão da inexistência de ferramentas que permitem o monitoramento constante das pessoas.

Nesse sentido, esta pesquisa justifica-se principalmente por pretender aprofundar os estudos sobre como o Estado brasileiro investe em tecnologias que permitem a coleta intensiva de dados pessoais. Assim, a relevância da pesquisa é justamente deslocar um pouco o foco de que apenas empresas privadas de tecnologia se apropriam de dados pessoais e argumentar, por meio de evidências, que autoridades governamentais corroboram para que um estado de eterna vigilância dos cidadãos seja fomentado.

Assim, o objetivo principal deste trabalho é compreender como entidades estatais brasileiras se apropriam de tecnologias e dispositivos que permitem a coleta massiva de dados pessoais. Nesse sentido, busca-se entender como essas práticas se aproximam de um autoritarismo governamental visto que não possuem autorização legal para acessar de maneira indiscriminada informações pessoais dos cidadãos brasileiros.

Para tanto, será feito o levantamento de alguns casos que evidenciam a adoção de tecnologias e sistemas para a coleta de dados pessoais pelo Estado em larga escala. Assim, será possível fazer ponderações entre tais práticas e suas consequências para os direitos de privacidade e autodeterminação informacional, utilizando as diretrizes e os princípios que da Lei Geral de Proteção de Dados (LGPD) como norte para compreender tais direitos. Além disso, será avaliado como essas tecnologias podem ser instrumentalizadas para legitimar práticas autoritárias, como vigilância indiscriminada e controle excessivo.

Isto posto, para a construção de análise crítica sobre o tema, esta pesquisa será orientada em um primeiro momento pela modalidade bibliográfica, com o uso de fontes como a doutrina para explorar e examinar as principais teorias relacionadas ao tema, e em seguida, será orientada pela pesquisa documental qualitativa com o uso da análise de conteúdo, em que serão utilizadas principalmente fontes de notícias de jornais, pesquisas e denúncias feitas por associações e organizações não governamentais sobre alguns casos de entidades estatais brasileiras que se apropriaram de tecnologias que permitem a coleta de dados pessoais em massa.

Ademais, para a elaboração deste trabalho, foi utilizada a divisão em quatro capítulos, com o intuito de criar uma organização que contemple introdução, desenvolvimento e conclusão de forma coesa.

Nesse sentido, o primeiro capítulo possui como objetivo introduzir os conceitos de capitalismo de vigilância e tecnoautoritarismo para contextualizar e fundamentar como o uso intensivo de tecnologias contribuem e influenciam novas dinâmicas sociais e políticas.

O segundo capítulo, contempla os significados da Lei Geral de Proteção de Dados (LGPD) e do direito à autodeterminação informacional com o propósito de compreender o papel dessa legislação no contexto de crescente monitoramento de dados pessoais dos cidadãos brasileiros por órgãos governamentais. Além disso, será feita ponderação sobre o artigo 4º da LGPD que determina a não aplicação dessa legislação quando o tratamento de dados tiver como finalidade a segurança pública.

Já no terceiro capítulo, será feito o levantamento de pesquisas, notícias e denúncias sobre a coleta indiscriminada e o monitoramento intensivo de dados pessoais pelo Estado Brasileiro com o objetivo de fundamentar que práticas como essas contribuem para a perda progressiva do direito fundamental de proteção de dados.

Em conclusão, o último capítulo visa demonstrar como o uso de tecnologias e sistemas que permitem a coleta massiva de dados pessoais dos cidadãos pelo Estado Brasileiro corrobora para o aumento de práticas autoritárias, como repressão política, perseguição de opositores e discriminação de minorias.

2 A ASCENSÃO DO TECNOAUTORITARISMO NA ERA DO CAPITALISMO DE VIGILÂNCIA: CONCEITOS E CARACTERÍSTICAS

O termo capitalismo de vigilância, desenvolvido por Shoshana Zuboff[2], refere-se a uma nova estrutura social em que dados comportamentais tornaram-se o principal recurso explorado por empresas e governos. Este modelo capitalista, impulsionado por avanços tecnológicos, é sustentado pela coleta e processamento massivo de informações pessoais, que visam moldar, influenciar e até mesmo direcionar comportamentos em diversas esferas da vida. Assim, este capítulo busca descrever a concepção do conceito de capitalismo de vigilância, analisar suas implicações para a autonomia individual e a privacidade, além de destacar as assimetrias de poder e conhecimento que emergem desse contexto que coloca em risco os pilares das sociedades democráticas e os direitos fundamentais dos cidadãos.

Além disso, o capítulo abordará o conceito de tecnoautoritarismo[3], que busca explicar o uso de tecnologias por parte do Estado para monitorar e controlar a população. Este fenômeno, que pode ocorrer tanto em regimes autoritários quanto em democracias, envolve a vigilância em larga escala e o uso de algoritmos para prever e influenciar comportamentos, muitas vezes à custa de direitos como a privacidade e a proteção de dados pessoais. No contexto brasileiro, serão apresentadas evidências de como o governo tem utilizado essas tecnologias, com destaque para os riscos que essas práticas representam para os direitos individuais e para as instituições democráticas.

2.1 Conceito de capitalismo de vigilância

O capitalismo de vigilância é um conceito introduzido por Shoshana Zuboff[4] para descrever uma nova forma de organização social em que dados comportamentais são a principal matéria prima para entidades privadas e públicas. Assim, essa forma de capitalismo apresenta, dentre outros, um componente essencial

[2] ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: A Luta por um Futuro Humano na Nova Fronteira do Poder. 1ª Edição. Rio de Janeiro. Editora Intrínseca, 2020. p. 231-376

[3] DEFENDENDO O BRASIL DO TECNOAUTORITARISMO. Data Privacy Brasil. Disponível em: https://www.dataprivacybr.org/projeto/defendend_o_brasil_do_tecnoautoritarismo/. Acesso em 23 de novembro de 2023.

[4] ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: A Luta por um Futuro Humano na Nova Fronteira do Poder. 1ª Edição. Rio de Janeiro. Editora Intrínseca, 2020. p. 231-376

intitulado *big data*, que possui como algumas de suas propriedades a extração, a análise e a acumulação de dados pessoais.

A autora explica que a evolução de tecnologias que permitem o acúmulo de informações que descrevem os hábitos e os costumes das pessoas colabora para o avanço de uma estrutura social em que poucas entidades possuem vastas quantidades de dados sobre muitas pessoas, ao passo que estas não possuem conhecimento sobre como suas informações estão sendo tratadas[5].

Nesse sentido, quem possui acesso às informações detém o poder de tentar incentivar, manipular e persuadir o comportamento em prol de seus próprios interesses. Isso é possível em razão da crescente introdução de dispositivos tecnológicos que coletam dados nos espaços privados e públicos com o objetivo de conhecer, moldar e influenciar o comportamento humano em aspectos sociais, políticos e econômicos.

Assim, dispositivos digitais com a capacidade de coletar dados em shoppings, bares, restaurantes, lojas e lanchonetes possuem o objetivo de obter informações sobre as pessoas para influenciar o consumo de seus produtos. Enquanto a criação de perfis em redes pode contribuir para a persuasão política de seus usuários, como exemplos, o papel do Google na campanha eleitoral de Barack Obama que analisava e buscava influenciar o perfil de mais de 250 milhões de americanos[6], e também o caso do Facebook e Cambridge Analytica que buscavam rastrear candidatos indecisos para incentivá-los a votar no candidato Donald Trump[7].

Não obstante, não são apenas empresas privadas que estão interessadas no acúmulo e monitoramento massivo de dados pessoais. Como denunciado pelo ex-funcionário da Agência de Segurança Nacional dos Estados Unidos, Edward Snowden, o governo americano investe em sistemas e ferramentas que permitem o acesso a milhares de dispositivos pessoais em claro desvio à Quarta Emenda Constitucional que proíbe a busca e apreensão arbitrárias dos cidadãos e seus bens, isto é, não permite que pessoas e objetos sejam perseguidos e monitorados sem devida ordem judicial[8].

---

[5] *Ibidem*
[6] *Ibidem*
[7] REVEALED: 50 MILLION FACEBOOK PROFILES HARVESTED FOR CAMBRIDGE ANALYTICA IN MAJOR DATA BREACH. The Guardian. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em 05 de maio de 2024.
[8] SNOWDEN, Edward; **Eterna Vigilância**. São Paulo. Editora Planeta do Brasil Ltda, 2019. 288p.

No Brasil, igualmente existem denúncias sobre o governo possuir contratos com empresas que fornecem tecnologias que exploram as vulnerabilidades de segurança para permitir o acesso a dispositivos pessoais sem o devido processo legal e em clara violação aos direitos fundamentais à privacidade e à personalidade dos cidadãos brasileiros[9]. Isso envolve gastos de até 31 milhões de reais pela administração pública em vigilância e espionagem sem licitação[10].

Esse conjunto de técnicas e soluções que permitem a apropriação de dados pessoais rompe com o tradicional contrato social em que o Estado e organizações privadas não podem adentrar a vida privada das pessoas sem autorização e motivações legais e inaugura uma nova fase do capitalismo em que concepções essenciais aos sistemas democráticos como liberdade, privacidade e autodeterminação passaram a ser relativizados e substituídos pela constante vigilância de todas as experiências humanas[11].

Nesse sentido, é necessário entender que o capitalismo de vigilância não é a tecnologia em si, e sim a lógica que permeia a tecnologia e a conduz na direção de quem a detém. Assim, quem está na posse de milhares de informações consegue concentrar conhecimentos suficientes para moldar opiniões e determinar ações que convergem com os seus interesses[12].

Além disso, cabe ressaltar que essa nova forma de organização social possui como principal objetivo captar costumes, hábitos e experiências humanas em todos os seus aspectos com o propósito de transformá-los em dados estatísticos que possam fornecer lucro e influência. Algo inimaginável até poucos anos atrás, visto que empresas privadas e o próprio Estado não tinham meios para adentrar a vida privada das pessoas sem os atuais aparatos e dispositivos tecnológicos[13].

---

[9] MERCADORES DA INSEGURANÇA: CONJUNTURA E RISCOS DO HACKING GOVERNAMENTAL NO BRASIL. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 29 de abril de 2024

[10] ABIN DE RAMAGEM GASTOU R$31 MILHÕES COM FERRAMENTAS DE VIGILÂNCIA SECRETAS E SEM LICITAÇÃO. A Pública. 25 de abril de 2023. Disponível em: https://apublica.org/2023/04/abin-de-ramagem-gastou-r-31-milhoes-com-ferramentas-de-vigilancia-secretas-e-sem-licitacao/

[11] ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: A Luta por um Futuro Humano na Nova Fronteira do Poder. 1ª Edição. Rio de Janeiro. Editora Intrínseca, 2020. p. 231-376.

[12] *Ibidem*

[13] *Ibidem*

2.1.1 Assimetrias de conhecimento e poder

O capitalismo de vigilância opera fundamentalmente por meio de assimetrias de conhecimento e poder, isso significa que enquanto os detentores das tecnologias sustentadas pela apropriação constante de dados pessoais acumulam vastas quantidades de informações sobre as pessoas, estas não possuem conhecimento das operações que envolvem os seus dados.

Dessa forma, as assimetrias de conhecimento e poder se intensificam quando entidades privadas e públicas rompem com o comprometimento de não invadir determinados aspectos da vida privada das pessoas e utilizam tecnologias de ponta para obter informações pessoais sem o devido processo legal e informacional.

Isso acontece, por exemplo, quando os carros do Street Views da empresa Google excedem a sua função de mapear ruas e coletam dados de redes de Wi-Fi privadas, como foi apurado em 2010 pela Comissão Federal Alemã de Proteção de Dados. A investigação revelou que os carros do Google eram capazes de coletar nomes, números de telefone, dados sobre crédito, senhas, mensagens, e-mails, transcrições de bate papo, material pornográfico, histórico de navegação, dados médicos, localização, fotografias, áudios e vídeos[14].

Outro exemplo de assimetrias de conhecimento e de poder é a utilização de métodos ilegais, como a interceptação de sistemas de telefonia, por órgãos estatais brasileiros que não possuem autorização para acessar dados pessoais de dispositivos privados. Neste caso, a Agência Brasileira de Inteligência (ABIN) foi investigada pela Polícia Federal por contratar um software israelense para monitorar a localização de jornalistas, parlamentares e até mesmo Ministros do Supremo Tribunal Federal (STF)[15].

Nesse sentido, as assimetrias de conhecimento e poder representam um desequilíbrio significativo nas relações entre indivíduos e as entidades que detêm os dados a partir do momento em que estas excedem a vigilância e monitoram indiscriminadamente as pessoas, o que contribui para a progressiva desvalorização de direitos como autodeterminação e privacidade, uma vez que os cidadãos já não

---

[14] *Ibidem p. 171.*

[15] QUAIS SÃO OS LIMITES? MAIOR ESCÂNDALO DA ABIN REABRE DISCUSSÃO SOBRE AS ATIVIDADES DE INTELIGÊNCIA. O Globo. 04 de fevereiro de 2024. Disponível em: https://oglobo.globo.com/politica/noticia/2024/02/04/quais-sao-os-limites-maior-escandalo-da-abin-reabre-discussao-sobre-as-atividades-de-inteligencia.ghtml. Acesso em 16 de maio de 2024.

possuem o poder de escolha sobre quais aspectos de sua vida serão públicos ou privados.

Como consequência da falta de autonomia e participação da maioria da população sobre como empresas privadas e entidades públicas podem utilizar da inovação tecnológica para coletar indiscriminadamente dados pessoais, há o risco de abusos por parte dos setores que detêm esses dados, posto que sem supervisão adequada e mecanismos de prestação de contas essas entidades podem utilizar as informações de maneiras que violem os direitos de privacidade e personalidade, o que inclui a manipulação de opiniões, a discriminação de minorias e até mesmo a perseguição política.

Além disso, a falta de transparência sobre como os dados são utilizados dificulta a capacidade dos indivíduos de exercerem controle sobre sua própria informação, o que contribui para enfraquecer os fundamentos do Estado de Direito, onde existe limites sobre como entidades privadas e estatais podem acessar determinados aspectos da vida pessoal dos cidadãos e onde a prestação de contas e a transparência são essenciais para esclarecer como os dados pessoais são acessados e tratados[16].

[16] ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: A Luta por um Futuro Humano na Nova Fronteira do Poder. 1ª Edição. Rio de Janeiro. Editora Intrínseca, 2020. p. 171.

2.2 O que é o tecnoautoritarismo e como ele avança no Brasil?

O tecnoautoritarismo é um conceito desenvolvido pela organização *Data Privacy* Brasil que busca descrever a crescente expansão do poder do Estado para monitorar a população por meio de sofisticadas tecnologias. Este termo foi cunhado para explicar os processos nos quais o governo aumenta suas capacidades de vigilância e controle, muitas vezes, à custa de direitos como a privacidade e a autodeterminação informacional dos cidadãos. Nesse sentido, o tecnoautoritarismo investiga como a interseção entre tecnologia e autoritarismo emerge por meio da violação de direitos como a privacidade e a personalidade a partir do momento em que o Estado abusa de seus poderes de investigação e vigilância[17].

Essas práticas tecno-autoritárias não necessariamente transformam regimes democráticos em regimes de exceção, mas ameaçam a integridade das instituições democráticas ao corroer gradualmente os pilares que as sustentam. Isso é feito por meio da criação de estruturas e sistemas que facilitam a vigilância em massa e a repressão e a supressão do direito à privacidade, o que contribui para minar a liberdade e a autonomia dos cidadãos[18].

Nesse sentido, para entender o tecnoautoritarismo é importante esclarecer que ele não se limita a regimes autoritários, mas também pode ocorrer em democracias. Muitas vezes, ele se aproveita das capacidades específicas das tecnologias de informação e de dados pessoais para consolidar o controle do Estado sobre a sociedade, isso pode incluir a coleta em larga escala de dados pessoais, a vigilância eletrônica indiscriminada e o uso de algoritmos para monitorar e prever o comportamento dos cidadãos[19].

Assim, é fundamental compreender que o Estado Moderno sempre utilizou meios para monitorar e controlar a população, em conformidade com o pacto social estabelecido. Nesse sentido, o tecnoautoritarismo atual representa a adaptação dessas práticas de vigilância de acordo com o avanço de inovações tecnológicas, o que permite a vigilância em larga escala que antes não era possível[20].

---

[17] DEFENDENDO O BRASIL DO TECNOAUTORITARISMO. Data Privacy Brasil. Disponível em: https://www.dataprivacybr.org/projeto/defendend_o_brasil_do_tecnoautoritarismo/. Acesso em 23 de novembro de 2023.
[18] *Ibidem*
[19] *Ibidem*
[20] *Ibidem*

No Brasil, existe um movimento de pesquisas, denúncias e investigações de que o governo investe em sistemas e tecnologias para acessar dispositivos privados em larga escala, isso envolve a capacidade de obter os dados dos dispositivos que estão na posse de agentes governamentais e também o acesso remoto.

Essas evidências serão apresentadas ao longo deste trabalho com o objetivo de fundamentar como o Estado Brasileiro utiliza tais tecnologias e quais os riscos para os direitos de personalidade, em especial aos direitos de privacidade e autodeterminação, quando o governo utiliza novos métodos para vigiar a população sem que esta tenha compreensão e conhecimento da extensão do poder de monitoramento que o Estado possui, o que contribui para o avanço de práticas tecno-autoritárias, como vigilância em excesso e monitoramento indiscriminado da população.

3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E O DIREITO À AUTODETERMINAÇÃO INFORMACIONAL

A partir dos conceitos de capitalismo de vigilância e tecnoautoritarismo, é possível compreender o surgimento de uma nova dinâmica social permeada pela tecnologia em que dados pessoais são valiosos ativos para empresas privadas e para o setor público. Nesse sentido, informações pessoais tornaram-se o centro de um novo modelo econômico e de governança, onde o controle e a manipulação desses dados geram poder e influência sem precedentes.

Diante desse contexto, este capítulo buscará abordar a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018 - LGPD), legislação que surgiu como resposta aos desafios que envolvem tecnologias pautadas na coleta intensiva de dados pessoais e estabeleceu um marco regulatório para o tratamento de dados pessoais no Brasil. A LGPD tem como objetivo principal proteger os direitos de personalidade e privacidade dos indivíduos e assegurar que suas informações sejam tratadas de maneira transparente, segura e em conformidade com a legislação.

Além de apresentar os conceitos centrais da LGPD, este capítulo discutirá o direito à autodeterminação informacional, um dos temas centrais deste trabalho, e que confere aos cidadãos o poder de controlar como seus dados são coletados, usados e compartilhados. Ademais, será explorado o papel regulatório e fiscalizatório da Autoridade Nacional de Proteção de Dados (ANPD) e as implicações da não aplicação da LGPD em casos específicos, como na segurança pública. Por meio dessa análise, busca-se compreender como a proteção de dados deve servir como um instrumento essencial para garantir a proteção dos direitos fundamentais em um cenário cada vez mais dominado pela vigilância tecnológica.

3.1 Conceitos

Diante do contexto apresentado de constante evolução dos dispositivos que permitem a vigilância de dados pessoais, surgiu no Brasil a Lei Geral de Proteção de Dados (Lei 13.709/2018 - LGPD), que está em vigor desde 2020, e marcou mudança significativa no cenário legal brasileiro ao estabelecer regras e diretrizes para o tratamento de dados pessoais para o setor público e privado. Assim, a LGPD visa

proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, em um mundo cada vez mais digitalizado, onde os dados se tornaram uma das principais matérias prima para o mercado.

Outro passo importante para a legislação brasileira foi a inclusão da proteção de dados pessoais no artigo 5º, inciso LXXIX, da Constituição Federal, em 2022, que determina “o direito à proteção dos dados pessoais, inclusive nos meios digitais”. Com isso, a proteção de dados pessoais assumiu a posição de direito fundamental e tornou-se uma “cláusula pétrea da matriz constitucional, inerente aos indivíduos - portanto irrenunciável, inalienável e inviolável - e essencial a uma vida digna, fazendo com que essa proteção se torne um dever do Estado”[21].

Além disso, é importante ressaltar que a LGPD é fundamentada em diversos princípios que orientam o tratamento adequado dos dados pessoais. Entre esses princípios, destacam-se a boa-fé, a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e prestação de contas. Esses princípios estabelecem parâmetros para o uso responsável e transparente dos dados e busca garantir que sejam tratados de maneira legal em todas as etapas do processo.

O princípio da boa-fé estabelece que as atividades de tratamento de dados devem ser conduzidas de acordo com a legislação e levem em consideração que os direitos dos titulares sejam respeitados em todas as etapas do processo. O princípio da finalidade determina que os dados pessoais devem ser coletados e utilizados para fins específicos e legítimos para evitar qualquer forma de uso abusivo ou discriminação[22].

Já o princípio da adequação exige que o tratamento dos dados seja compatível com o contexto e com as finalidades informadas aos titulares. Além disso, o princípio da necessidade estabelece que deve haver justificativa legal e proporcional para a

---

[21] MARTINS, Ricardo Maffeis; GUARIENTO, Daniel Bittencourt. Emenda Constitucional torna a proteção de dados pessoais um direito fundamental. 18 de fevereiro de 2022. Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/359941/ec-torna-a-protecao-de-dados-pessoais-um-direito-fundamental. Acesso em 01 de maio de 2024.

[22] LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. *E-book.* ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 01 mai. 2024. P. 124 – 138.

coleta e o processamento dos dados para assegurar que apenas as informações estritamente necessárias sejam utilizadas para atingir os objetivos pretendidos[23].

O princípio do livre acesso determina a garantia, aos titulares dos dados, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Já o princípio da qualidade dos dados assegura aos titulares a garantia de que suas informações sejam precisas, claras, relevantes e atualizadas de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. E o princípio da prevenção estabelece a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais[24].

O princípio da transparência determina que os titulares dos dados sejam informados de maneira clara e acessível sobre como suas informações serão tratadas e que possam exercer seus direitos de forma consciente e informada. O princípio da segurança, por sua vez, exige a implementação de medidas adequadas para proteger os dados pessoais contra acesso não autorizado, uso indevido, alteração, destruição ou divulgação não autorizada[25].

Por fim, o princípio da responsabilização e prestação de contas estabelece que as organizações que lidam com dados pessoais devem ser responsáveis por garantir o cumprimento dos princípios estabelecidos pela LGPD e que estarão sujeitas a sanções em caso de descumprimento. Esses princípios fornecem um norte legal sólido para o tratamento responsável e transparente dos dados pessoais e promove assim a proteção dos direitos dos titulares e a regulamentação da coleta de dados.

Outro ponto importante estabelecido pela LGPD em seu artigo 2º, inciso II, é em relação ao direito à autodeterminação informacional. Esse conceito refere-se à capacidade dos indivíduos de compreenderem e controlarem como suas próprias informações pessoais são tratadas, e que possam decidir de forma autônoma sobre sua coleta, uso, armazenamento e compartilhamento. Em outras palavras, a autodeterminação informacional confere aos titulares dos dados o poder de escolha

---

[23] LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. *E-book.* ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 01 mai. 2024. P. 124 – 138.

[24] *Ibidem*

[25] *Ibidem*

para determinar o destino de suas próprias informações e exercer um controle efetivo sobre sua privacidade e autonomia[26].

Esse direito foi reconhecido em 1983, pelo Tribunal Constitucional Alemão, após um longo debate jurídico sobre o recenseamento da população, em que foi decidido a proibição do tratamento não transparente de dados pessoais, com fundamento na dignidade humana e no livre desenvolvimento da personalidade. O tribunal alertou para o risco de que o recenseamento da população, devido à sua extensão, poderia comprometer a autonomia das pessoas ao permitir a criação de perfis detalhados dos cidadãos. Portanto, enfatizou a necessidade de que o tratamento de dados seja justificado legalmente e tenha uma finalidade específica[27].

Além disso, conforme explica Laura Schertel[28], a formulação do direito à autodeterminação informacional parte do princípio de que, nas condições atuais de processamento automatizado de dados em larga escala em que informações pessoais tornaram-se valiosos ativos para o mercado, não há mais dados considerados como inúteis e que os riscos atrelados ao tratamento de dados estão mais na finalidade e nas capacidades de processamento do que na natureza dos dados processados. Isso implica que a proteção dos dados deve considerar não apenas o tipo de informação coletada, mas também o contexto em que é utilizada. Dessa maneira, é essencial que os cidadãos sejam informados sobre como suas informações estão sendo processadas com transparência e respeito aos seus direitos de privacidade.

Dessa maneira, a autodeterminação informacional desempenha um papel fundamental na preservação da privacidade e da liberdade individual dos usuários no ambiente digital. Ao garantir que os titulares dos dados tenham controle sobre suas próprias informações, esse princípio busca garantir a transparência para o tratamento de dados pessoas e que eles não sejam utilizados de forma abusiva para violar a privacidade e a intimidade das pessoas.

---

[26] BIONI, Bruno R. **Proteção de Dados Pessoais** - A Função e os Limites do Consentimento. Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 29 nov. 2023. p. 97.

[27] AUTODETERMINAÇÃO INFORMATIVA: COMO ESSE DIREITO SURGIU E COMO ELE ME AFETA? Laboratório de Políticas Públicas e Internet – LAPIN. 27 de abril de 2021. Disponível em: https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/. Acesso em 18 de maio de 2024.

[28] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Revista de Ciência Jurídicas Pensar. e-ISSN:2317-2150. v. 25, n. 4, p. 1-18, out./dez. 2020

Como decorrência do direito à autodeterminação informacional, surgem os direitos elencados pelo artigo 18 da LGPD[29], como a confirmação da existência de tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial, a eliminação dos dados pessoais tratados com o consentimento do titular, a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e a revogação do consentimento[30].

Esses direitos decorrem fundamentalmente da autodeterminação informacional uma vez que buscam conferir aos indivíduos o controle de suas próprias informações por meio da concreta tutela de seus dados[31]. Nesse sentido, a LGPD, ao garantir a autodeterminação informacional, determina que os indivíduos possam exercer autonomia efetiva sobre suas informações e atuar como agentes ativos na gestão e proteção de sua privacidade.

Por fim, percebe-se que a Lei Geral de Proteção de Dados (LGPD) emergiu como um marco essencial na proteção da privacidade e dos direitos fundamentais dos cidadãos no Brasil. Ao estabelecer diretrizes claras e rigorosas para o tratamento de dados pessoais, essa legislação não apenas protege os indivíduos contra o uso abusivo e indiscriminado de suas informações, mas também promove um ambiente de transparência e responsabilidade no manejo dos dados.

---

[29] GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. São Paulo: SRV Editora LTDA, 2023. *E-book.* ISBN 9786555599480. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599480/. P. 47. Acesso em: 30 mai. 2024.

[30] Brasil. LEI Nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Brasília, DF: Diário Oficial da União, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 30 de maio de 2024.

[31] LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. *E-book.* ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 01 mai. 2024. P. 124 – 251.

3.2 Papel regulatório e fiscalizatório

Para orientar, regulamentar e fiscalizar o cumprimento da LGPD no Brasil pelo setor público e privado, foi criada a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública. Assim, a ANPD possui um papel fundamental no monitoramento das atividades de tratamento de dados realizadas por organizações estatais e privadas.

Entre as diversas atribuições da ANPD, está a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar e aplicar sanções em casos de descumprimento da legislação, promover o conhecimento da população sobre normas de proteção de dados, estimular a adoção de padrões para facilitar o controle dos titulares sobre seus dados , editar regulamentos sobre proteção de dados e relatórios de impacto, ouvir agentes de tratamento e a sociedade, interpretar a LGPD, articular-se com autoridades reguladoras setoriais e implementar mecanismos simplificados para registro de reclamações sobre tratamento inadequado de dados pessoais[32].

Em relação ao tratamento de dados pessoais realizado pelo poder público especificamente, a LGPD, em seu artigo 55-J, incisos XI e XVI, determina que a ANPD poderá requerer às entidades do poder público que realizam tratamento de dados pessoais “informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei” e também “realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público”.

Nesse sentido, para regular o tratamento de dados pessoais realizado pelo poder público a ANPD desempenha um papel central, uma vez que como órgão responsável pela aplicação da LGPD possui competência para monitorar e fiscalizar as atividades de tratamento de dados realizadas por entidades governamentais, isso inclui o poder de solicitar informações detalhadas sobre o tratamento de dados

[32] Brasil. LEI Nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Brasília, DF: Diário Oficial da União, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 10 de maio de 2024.

pessoais realizado pelo setor público para garantir a transparência e a conformidade com a legislação. Além disso, a ANPD tem o poder de realizar auditorias e investigações para verificar se as práticas de tratamento de dados pelo poder público estão em conformidade com os princípios e diretrizes estabelecidos pela LGPD.

3.3 Segurança pública e a não aplicação da LGPD

O tecnoautoritarismo avança principalmente por meio do discurso de que a utilização de ferramentas tecnológicas sustentadas pela coleta intensiva de dados pessoais faz parte do processo de modernização dos aparatos de investigação e inteligência do Estado. Não obstante, a prática de burlar sistemas de segurança de dispositivos pessoais por agentes mal intencionados é configurada como crime, mas quando o Estado faz o uso de tais práticas, recebe o respaldo de legalidade pois o faz, muitas vezes, em nome da segurança pública[33].

Nesse sentido, de acordo com o artigo 4º, inciso III, da LGPD, esta não será aplicada para fins exclusivos de segurança pública latu sensu, isto é, segurança pública *stricto sensu*, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. Isso significa que quando a finalidade do tratamento de dados pessoais pelo Estado estiver dentro do escopo do referido artigo, não haverá aplicação dos requisitos da LGPD[34].

Ainda que não seja o objetivo deste trabalho destrinchar o significado de todos os itens do artigo 4º, inciso III, da LGPD, que abarca a segurança pública *latu sensu*, cabe algumas definições de suas atividades. No tocante à segurança pública *stricto sensu*, pode-se entender como uma de suas atribuições a atuação da polícia administrativa, que se concentra na prevenção de atividades criminosas, como o policiamento ostensivo, e outras atividades de vigilância geral que fazem parte de políticas públicas de segurança. Isso inclui, por exemplo, atividades da Unidade de Inteligência Financeira, que visa impedir a lavagem de dinheiro e combater o financiamento do terrorismo[35].

Já em relação à defesa nacional, pode-se compreender como o conjunto de iniciativas e ações governamentais, com foco na expressão militar, visando proteger o território, a soberania e os interesses nacionais contra ameaças externas, sejam elas potenciais ou reais. No que se refere à segurança de estado, trata-se das ações

---

[33] MERCADORES DA INSEGURANÇA: CONJUNTURA E RISCOS DO HACKING GOVERNAMENTAL NO BRASIL. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 04 de maio de 2024. P. 07.

[34] ALVES, Fabrício; VALADÃO, Rodrigo. Proteção de Dados Pessoais na Segurança Pública - Breves considerações acerca do art. 4º, inciso III e §1º da LGPD. Migalhas, 23 de dezembro de 2022. Disponível em: https://www.migalhas.com.br/coluna/dados-publicos/379087/protecao-de-dados-pessoais-na-seguranca-publica. Acesso em 04 de maio de 2024.

[35] *Ibidem*

de inteligência, que envolvem a execução contínua de atividades especializadas para produzir e disseminar informações e auxiliar autoridades governamentais no planejamento, execução, acompanhamento e avaliação das políticas de Estado. E por último, no tocante às atividades de investigação e repressão de infrações penais, trata-se das ações repressivas das forças policiais, como as atividades da polícia judiciária relacionadas à investigação de crimes, com o objetivo de conduzir inquéritos policiais e processos penais, bem como cumprir ordens do Poder Judiciário[36].

Outro ponto importante em relação à segurança pública e a LGPD, é que conforme dispõe o § 1º do artigo 4º, o tratamento de dados pessoais para atividades de segurança pública *latu sensu* será determinado por legislação própria e que deverá levar em consideração medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD. Assim, é determinado um modelo regulatório específico para definir o tratamento de dados pessoais para fins de segurança pública, sendo que já existe um anteprojeto de "LGPD para Segurança Pública" (Projeto de Lei N.º 1.515, DE 2022), para avaliação do Congresso Nacional[37].

Não obstante, enquanto o Congresso Nacional não define métricas para o tratamento de dados pessoais pelo setor público para garantir a segurança pública, é importante entender que a Constituição Federal ao assegurar que a proteção de dados pessoais é um direito fundamental, determina que a privacidade e a proteção de dados sejam levadas em consideração mesmo nos casos de segurança pública pelo Estado. Nesse sentido, mesmo com um déficit legislativo sobre o assunto, os dados pessoais alvos de investigação não estão desprotegidos e não podem ser utilizados pelo Estado de maneira arbitrária[38].

Assim, as práticas e métodos adotados por órgãos governamentais para praticar a vigilância em massa da população por meio de soluções e ferramentas que conseguem burlar a segurança de dispositivos pessoais não podem deixar de levar em consideração o devido processo legal e o direito fundamental de proteção de dados. Isso significa que, mesmo em situações de segurança pública, a privacidade e

[36] *Ibidem*
[37] *Ibidem*
[38] *Ibidem*

a proteção de dados devem ser consideradas, e que as informações pessoais não sejam utilizadas de maneira abusiva pela máquina estatal.

4 ALGUNS CASOS DE VIOLAÇÃO À AUTODETERMINAÇÃO INFORMACIONAL NO BRASIL

Com o objetivo de fundamentar como tecnoautoritarismo avança no Brasil, isto é, como a interseção entre tecnologia e autoritarismo emerge por meio da violação de direitos como a privacidade e a personalidade, este capítulo possui o objetivo de apresentar algumas pesquisas, denúncias e investigações de contratações realizadas entre o Estado Brasileiro e empresas que fornecem ferramentas para a coleta intensiva de dados pessoais, sendo essas parcerias muitas vezes sem ordem judicial ou licitação.

4.1 Levantamento de pesquisas, denúncias e investigações de tecnologias e sistemas de informação empregados por órgãos estatais para a coleta de dados pessoais em larga escala

Para esclarecer como o Estado brasileiro adota ferramentas sofisticadas que permitem a extração de dados pessoais sem o conhecimento da população, este capítulo busca fornecer informações sobre pesquisas, denúncias e investigações sobre contratos entre o governo brasileiro e empresas que oferecem soluções para coletar dados pessoais de forma intensiva.

A principal pesquisa utilizada como fonte para este trabalho é denominada “Mercadores da insegurança: conjuntura e riscos do *hacking* governamental no Brasil[39]”, realizada pelo Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Este estudo analisou que, durante o período de 2015 a 2021, 209 documentos contratuais em nível estadual e federal evidenciam que certas ferramentas de *hacking* estiveram em uso no país durante esse período com o respaldo de que são necessárias para a segurança pública.

A maioria dos documentos foi obtida por meio dos Portais de Transparência e do Serviços de Informação ao Cidadão (SIC) dos Estados, da União e dos Ministérios Públicos Estaduais e Federal, com fundamento na Lei de Acesso à Informação. Não obstante, as solicitações de acesso à informação dos contratos pelo IP.rec. tendiam à

[39] MERCADORES DA INSEGURANÇA: CONJUNTURA E RISCOS DO HACKING GOVERNAMENTAL NO BRASIL. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 02 de maio de 2024.

negativa na maioria dos casos com a justificativa de que são documentos sigilosos e até mesmo de que esses contratos não existiam[40].

Ainda conforme explicado pelo IP.rec., o conceito de soluções *hacking* é analisado em duas perspectivas: técnica e comportamental. Tecnicamente, refere-se à exploração de vulnerabilidades, sejam elas conhecidas ou não pelo fabricante, que resultem em acesso não autorizado a informações, sejam elas em trânsito ou armazenadas. Comportamentalmente, implica na intenção deliberada de alcançar essas informações ao contornar os mecanismos de segurança estabelecidos[41].

Além disso, para compreender o *hacking* governamental, foram criadas duas categorias: A primeira diz respeito ao acesso de dados e comunicações por meio do controle físico do dispositivo, como um celular confiscado, que possibilita a extração de dados do aparelho, inclusive a quebra de criptografias ou o contorno de sistemas de segurança, como senhas ou autenticação biométrica. A segunda, se refere ao acesso remoto de dispositivos, geralmente pela exploração de vulnerabilidades desconhecidas pelos fabricantes, o que permite o acesso total ou parcial ao dispositivo. Nesse último caso, inclui-se também o uso de ferramentas para interceptar o tráfego de informações em redes móveis a partir de proximidade relativa do dispositivo alvo[42].

Nesse sentido, o estudo revela que as autoridades brasileiras estão amplamente familiarizadas e proficientes no uso de ferramentas de *hacking* e conseguem ultrapassar com facilidade os recursos de segurança e acessar dispositivos pessoais e, consequentemente, todas as informações que estão contidas neles. Essa situação é preocupante para a proteção dos direitos fundamentais relacionados à privacidade dos dados e à confidencialidade das comunicações. Além disso, levanta questionamentos sobre a presença e aceitação da indústria de ferramentas de *hacking* no Brasil, muitas vezes respaldada pelas solicitações do governo por tecnologias forenses.

Ainda conforme levantado pelo IP.rec, duas empresas, *Cellebrite* e *Verint*, chamaram a atenção dos pesquisadores, uma vez que ambas estão relacionadas com fatores políticos nacionais e internacionais, principalmente em relações que sugerem

[40] *Ibidem*
[41] *Ibidem*
[42] *Ibidem*

danos aos direitos humanos pelo uso de ferramentas de *hacking*, vazamento de informações confidenciais e perseguição à sociedade civil[43].

É importante ressaltar que ambas empresas trabalham com a exploração de vulnerabilidades de sistemas. Assim, enquanto *big techs* como *Apple* e *Alphabet* chegam a pagar cerca de U$1.000.000 para quem delatar brechas em seus sistemas, empresas como *Cellebrite* e *Verint* buscam por vulnerabilidades sem o objetivo de relatar seus achados, uma vez que utilizam justamente dessas falhas para continuar a ter acesso e monitorar dispositivos pessoais. Em razão disso, será abordado com mais detalhes nos próximos tópicos a relação de ambas as empresas com o Estado Brasileiro[44].

Outra fonte importante para esse trabalho são as pesquisas e divulgações do *Data Privacy* Brasil, organização que atua na promoção, divulgação e pesquisa de informações sobre a proteção de dados pessoais no Brasil, que serão essenciais para fundamentar os efeitos da vigilância em excesso do Estado Brasileiro, principalmente para análise do caso envolvendo a ABIN e o *software First Mile*.

[43] *Ibidem*
[44] *Ibidem p.16*

4.1.1 Caso *Cellebrite* e *Techbiz Forense Digital*

O maior representante comercial de ferramentas de *hacking* para o mercado brasileiro é a empresa *TechBiz Forense Digital*, principal representante da *Cellebritte*, fabricante israelense de soluções de extração de dados, ferramentas essas que foram contratadas pelo Ministério da Justiça, Ministérios Públicos e Secretarias de Segurança Estaduais, em mais de cem contratos com a administração pública estadual e federal, com custos de mais de 100 milhões, desde 2018[45].

As soluções da *Cellebritte* possibilitam o acesso a qualquer dispositivo, aplicativo ou sistema de segurança, seja por meio de códigos PIN, senhas, biometria ou criptografia. Isso implica que um único acesso por meio dessas ferramentas a um dispositivo pessoal pode fornecer quantidades sem precedentes de informações pessoais e comunicações, o que permite a criação de perfis detalhados dos cidadãos por meio da combinação de diversos tipos de dados, como localização, interações registradas, histórico de buscas, conteúdo de comunicações, preferências, fotos, vídeos, dados cadastrais e muito mais[46].

Há alguns aspectos dignos de nota em relação à salvaguarda de informações pessoais dos usuários cujos dados são obtidos por meio dessas soluções. O primeiro ponto diz respeito à capacidade das empresas fabricantes de acessar dados de investigações. Apesar da *Techbiz* declarar que a *Cellebrite* não possui acesso a informações sobre operações policiais, ao mesmo tempo a "*Cellebrite Advanced Servic*es" oferta a extração e a decodificação de dados para seus clientes[47] ".

Assim, é notável que os dados das investigações inevitavelmente são compartilhados com a *Cellebrite*, o que levanta questões sobre a privacidade dos supostos investigados e dos usuários relacionados. Além disso, há relatos internacionais de que as ferramentas da *Cellebrite* são comercializadas em mercados clandestinos, isso inclui informações confidenciais de investigações, o que levanta preocupações sobre a segurança e a confidencialidade dos dados extraídos.[48]

Nesse sentido, a utilização de ferramentas da *Cellebritte* que permitem o acesso total aos dados que estão em dispositivos privados mostra-se preocupante uma vez que existe a possível transferência internacional de informações pessoais

---

[45] *Ibidem p. 48-50*
[46] *Ibidem*
[47] *Ibidem*
[48] *Ibidem*.

entre o estado brasileiro e empresas privadas estrangeiras sem levar em consideração a proteção e a segurança desses dados. Ademais, significa que existe uma parceria entre órgãos públicos e empresas privadas para coletar dados pessoais sem a utilização de métricas que visem a proteção dessas informações, que coloque limites no que será extraído e que garanta que esses dados serão utilizados apenas para os fins necessários e não abusivos.

4.1.1.1 Projeto *Excel*

O Projeto *Excel* é uma iniciativa do Ministério da Justiça e Segurança Pública para criar um banco de dados formado por informações obtidas por meio de ferramentas fabricadas pela *Cellebrite* e fornecidas pela *TechBiz Forense Digital LTDA*, ambas com notoriedade em programas forenses e de espionagem. Ao todo, foram adquiridas 30 licenças que permitem a extração, processamento e análise de dados e informações de dispositivos móveis[49].

As soluções utilizadas pelo projeto incluem acessar dispositivos que estejam bloqueados ou protegidos por criptografia, além de obter informações como histórico de localização, registros de chamadas, mensagens de aplicativos, dados apagados, informações de redes privadas (como VPN) e até mesmo dados de jogos, como Pokémon Go[50].

Uma das preocupações centrais do Projeto *Excel*, é o acesso sem restrições ao vasto banco de dados que já teve autorização para extrair dados de 8.741 dispositivos até 2021. Tal questão torna-se problemática também pelo fato de que os crimes investigados são aqueles que afetam desproporcionalmente a população negra, visto que os crimes mais investigados, até 2021, foram o tráfico de drogas, homicídio e roubo. Sendo que crimes econômicos, como lavagem de dinheiro, estelionato e peculato, são minoritários[51].

Assim, não há transparência sobre como o Ministério da Justiça utiliza os dados que as soluções da *Cellebrite* permitem e nem com qual finalidade essas informações estão sendo tratadas. Isso pode contribuir para o excesso de vigilância nas investigações, uma vez que ao obter acesso, por exemplo, a um dispositivo celular, existe a possibilidade de acessar diversas informações do alvo das investigações e de outras pessoas, o que pode ultrapassar os limites da investigação em andamento

---

[49] MERCADORES DA INSEGURANÇA: CONJUNTURA E RISCOS DO HACKING GOVERNAMENTAL NO BRASIL. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 29 de abril de 2024

[50] MINISTÉRIO DA JUSTIÇA EQUIPA POLÍCIAS PARA VASCULHAR CELULARES EM TROCA DE DADOS. The Intercept. 21 de maço de 2022. Disponível em https://www.intercept.com.br/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados/: Acesso em 10 de maio de 2024.

[51] MERCADORES DA INSEGURANÇA: CONJUNTURA E RISCOS DO HACKING GOVERNAMENTAL NO BRASIL. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 29 de abril de 2024

e afastar a proporcionalidade e a necessidade que justifiquem a utilização dessas ferramentas[52].

[52] MINISTÉRIO DA JUSTIÇA EQUIPA POLÍCIAS PARA VASCULHAR CELULARES EM TROCA DE DADOS. The Intercept. 21 de maço de 2022. Disponível em https://www.intercept.com.br/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados/: Acesso em 10 de maio de 2024.

4.1.2 Caso *Verint Systems* (*Cognyte*/*Suntech*)

A relação comercial com a *Verint* e a administração pública brasileira é outro caso que merece atenção, visto que segundo o Portal da Transparência a empresa figura entre uma das mais favorecidas pelo fornecimento de ferramentas de espionagem, com custos superiores a 40 milhões. A partir da subsidiária *Cognyte* Brasil (ex-*Suntech*), foram levantadas contratações das soluções de *hacking* com a Polícia Civil do Distrito Federal, com o Departamento de Operações Policiais Estratégicas do Estado de São Paulo, com o Fundo Penitenciário do Estado de Alagoas e com a Polícia Civil do Pará[53].

No caso da Polícia Civil do Pará, foi constatado que a contratação das ferramentas de *hacking*, no valor de R$5 milhões, foi feita sem licitação pelo então governador do Pará, Helder Barbalho, com o propósito de espionar os responsáveis pela investigação sobre corrupção na compra de respiradores durante a pandemia da Covid-19 da qual o governador foi alvo, sendo comprovado que a solução podia acessar informações de dispositivos móveis, interceptar conversas criptografadas e gravar áudios do ambiente, tudo sem a necessidade de ordem judicial e com poucos vestígios de sua utilização. Em outra investigação, um dos sócios da *Cognyte* foi preso pela Polícia Federal por estar envolvido em vazamento de informações confidenciais sobre investigações criminais em troca de produtos da *Cognyte*[54].

Além disso, a *Verint*, junto com suas filiais internacionais, tem sido alvo de acusações globais por oferecer tecnologias de espionagem de comunicações em locais onde regimes autoritários estão presentes e em países com histórico de repressão política, como Cazaquistão e Usbequistão, de acordo com a organização *Privacy International*. Investigação da Anistia Internacional revelou que a *Verint Systems Ltd*, subsidiária da *Verint Systems Inc*., forneceu equipamentos de interceptação de comunicações ao governo do Sudão do Sul, onde o governo tem usado tais tecnologias para monitorar e prender jornalistas e ativistas de direitos humanos com base em informações interceptadas[55].

---

[53] MERCADORES DA INSEGURANÇA: CONJUNTURA E RISCOS DO HACKING GOVERNAMENTAL NO BRASIL. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 29 de abril de 2024

[54] *Ibidem*

[55] *Ibidem*

Assim, a situação representa um sério problema para o tratamento de dados pessoais, pois demonstra que o fornecimento dessas ferramentas para entidades governamentais, sem a devida transparência e controle, abre caminho para abusos de poder, violações de privacidade e potencial perseguição de indivíduos com base em suas atividades políticas, jornalísticas ou de defesa dos direitos humanos. Ademais, compromete a integridade dos dados pessoais e pode interferir e prejudicar investigações.

4.1.2.1 ABIN e o *Software First Mile*

Em outubro de 2023, a Polícia Federal relatou que, desde o fim de 2018, a Agência Brasileira de Inteligência (ABIN) fez o uso sem licitação de um sistema de monitoramento denominado *First Mile*, desenvolvido pela empresa israelense *Cognyte*. Este sistema tem a capacidade de rastrear indivíduos com base na localização de dispositivos que operam nas redes 2G, 3G e 4G. Para localizar um alvo, basta inserir o número do telefone da pessoa no programa e visualizar em um mapa a última posição registrada[56].

Assim, conforme esclarecido por Rafael Zanatta, diretor da ONG *Data Privacy* Brasil, o *software* utiliza métodos que violam e ludibriam as redes de operadoras de telefonia para realizar o rastreamento do alvo e acessar informações sigilosas, uma vez que elas apenas poderiam ter sido fornecidas por meio de autorização judicial[57].

Ainda conforme investigação da Polícia Federal, a ABIN realizou cerca de 33 mil monitoramentos ilegais por meio de *softwares* de monitoramento. Destes, aproximadamente 1.800 usos foram direcionados para espionagem de políticos, jornalistas, advogados e ministros do Supremo Tribunal Federal (STF). Entre os alvos estava o jornalista Glenn Greenwald, fundador do site *The Intercept* Brasil e conhecido por publicar reportagens baseadas nos arquivos do ex-funcionário da Agência de Segurança Nacional dos Estados Unidos, Edward Snowden, que denunciou atividades de espionagem ilegal do governo americano[58].

Assim, o caso da ABIN demonstra como a banalização da utilização de tecnologias de vigilância representa grave violação da proteção de dados pessoais e da privacidade dos cidadãos brasileiros, que ficam sob suspeita por motivos políticos e ideológicos[59]. O acesso não autorizado a informações pessoais, como a localização

---

[56] SISTEMA DE ESPIONAGEM USADO ILEGALMENTE PELA ABIN PODE MOSTRAR LOCALIZAÇÃO DE QUALQUER CELULAR - DATA PRIVACY BRASIL RESEARCH. Data Privacy Brasil. Disponível em: Sistema de espionagem usado ilegalmente pela Abin pode mostrar localização de qualquer celular - Data Privacy Brasil Research. Acesso em 10 de maio de 2024.

[57] O QUE É O FIRSTMILE, SOFTWARE QUE TERIA SIDO USADO PELA ABIN PARA MONITORAR JORNALISTAS E MINISTROS DO STF. BBC News. 23 de outubro de 2023. Disponível em: https://www.bbc.com/portuguese/articles/c3g32mz1dzdo. Acesso em 13 de maio de 2023.

[58] COMO O BRASIL VIROU O PARAÍSO DA ESPIONAGEM ILEGAL. The Intercept Brasil. 28 de outubro de 2023. Disponível em: https://www.intercept.com.br/2023/10/28/brasil-virou-paraiso-da-espionagem-ilegal-com-michel-temer-jair-bolsonaro/. Acesso em 13 de maio de 2023.

[59] GOMES, Ana. Espionagem governamental – nem papo futurista, nem coisa da sua cabeça. Instituto de Referência em Internet e Sociedade, 31 de outubro de 2023. Disponível em: https://irisbh.com.br/espionagem-governamental-nem-papo-futurista-nem-coisa-da-sua-cabeca/. Acesso em 04 de maio de 2024.

de dispositivos e comunicações pessoais, sem o devido respaldo legal, compromete os direitos de personalidade e privacidade e abre espaço para abusos por parte das autoridades. Além disso, a utilização de métodos que burlam as redes de telecomunicações para realizar esse tipo de vigilância aumenta os riscos de violações de segurança cibernética e exposição de dados a terceiros não autorizados.

4.2 Impacto dos casos de violação da autodeterminação informacional pelo Estado Brasileiro

A partir dos casos apresentados é possível perceber que o Estado possui acesso a sofisticados aparatos tecnológicos que buscam explorar vulnerabilidades de sistemas de dispositivos pessoais para monitorar dados dos cidadãos brasileiros. Essas ferramentas, ao permitirem que diversos aspectos da vida privada de indivíduos sejam acessados demonstra que atualmente é possível a vigilância em massa da população para além do contrato social, uma vez que os indivíduos já não possuem compreensão e controle de quais aspectos de suas vidas estão sob monitoramento do Estado[60].

Nesse cenário, a autodeterminação informacional, que deveria garantir aos indivíduos o poder de determinar o destino de suas próprias informações e exercer um controle efetivo sobre sua privacidade e intimidade, passa a ser relativizada, muitas vezes, em razão da segurança pública. Como consequência, cria-se um ambiente que se distancia do Estado Democrático de Direito em que a população possui participação ativa sobre como informações pessoais são compartilhadas com o Estado e que considera a privacidade um elemento fundamental da própria vida em sociedade[61].

Assim, a partir do momento que os cidadãos já não possuem o direito de escolha sobre quais aspectos de sua vida serão públicos ou privados, fomenta-se a progressiva desvalorização da autodeterminação informacional. Isso tem impactos significativos na esfera individual e social, posto que rompe com a ideia dos direitos fundamentais de privacidade, personalidade e liberdade em prol de um sistema capaz de monitorar constantemente todos os aspectos da vida das pessoas.

É importante destacar que a ideia de separação entre o que é público e o que é privado em regimes democráticos possui como objetivo proteger o indivíduo contra o poder do Estado. Dessa forma, ao estabelecer um limite à interferência estatal na vida privada, fica determinado que o Estado não pode invadir o espaço protegido que

---

[60] DEFENDENDO O BRASIL DO TECNOAUTORITARISMO. Data Privacy Brasil. Disponível em: https://www.dataprivacybr.org/projeto/defendend_o_brasil_do_tecnoautoritarismo/. Acesso em 23 de novembro de 2023.

[61] BIONI, Bruno R. **Proteção de Dados Pessoais** - A Função e os Limites do Consentimento. Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 15 de maio de 2024. P. 207.

esse direito cria ao redor da pessoa. Ao mesmo tempo, esse direito confere ao indivíduo o poder de exigir, perante a autoridade pública, proteção contra a violação de sua privacidade por terceiros ou pelo próprio Estado[62].

Nesse sentido, a relação do governo brasileiro com empresas capazes de burlar camadas de segurança de dispositivos pessoais e envolvidas na espionagem de opositores políticos, jornalistas, minorias sub representadas e membros do STF, evidencia que a população já não possui autonomia e controle sobre qualquer informação que esteja em seus apetrechos digitais e como ela poderá ser utilizada.

Dessa maneira, percebe-se que ao fomentar a vigilância abusiva e o controle excessivo da população, o governo contribui para a criação de um ambiente propício para o abuso de poder e a violação dos direitos, uma vez que já existem evidências de que o acesso indiscriminado aos dados pessoais dos cidadãos pode ser utilizado para monitorar e reprimir dissidências políticas, perseguir opositores e silenciar vozes críticas, o que enfraquece os pilares da democracia e do Estado de Direito.

[62] ANÁLISE COMPARATIVA ENTRE DIREITO À PRIVACIDADE E DIREITO À PROTEÇÃO DE DADOS PESSOAIS E RELAÇÃO COM O REGIME DE DADOS PÚBLICOS PREVISTO NA LEI GERAL DE PROTEÇÃO DE DADOS. Data Privacy Brasil. 18 de setembro de 2019. Disponível em: https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados-2/. Acesso em 15 de maio de 2024.

5 INSTRUMENTALIZAÇÃO DAS TECNOLOGIAS DE COLETA MASSIVA DE DADOS PARA LEGITIMAÇÃO DE PRÁTICAS ESTATAIS AUTORITÁRIAS

Os progressos obtidos em razão da tecnologia têm sido vantajosos para a sociedade ao simplificar a obtenção de informações, aprimorar procedimentos e impulsionar o crescimento econômico e social. Não obstante, junto com esses avanços, surgiram também novos desafios e preocupações, especialmente no que diz respeito à privacidade e à proteção de dados dos cidadãos.

Nesse sentido, percebe-se que o desenvolvimento de tecnologias e sistemas de segurança são acompanhados também do crescimento de métodos para burlar essas proteções, o que levanta preocupações sobre a vulnerabilidade dos dados pessoais e a possibilidade de abusos por parte das autoridades ou de agentes maliciosos que fazem o uso dessas ferramentas.

Assim, os casos levantados no último capítulo ilustram como as tecnologias de coleta massiva de dados estão sendo instrumentalizadas para legitimar práticas estatais autoritárias no Brasil. A falta de transparência, o uso indiscriminado dessas tecnologias e a ausência de salvaguardas eficazes para a proteção de dados dos cidadãos ameaçam a integridade das instituições democráticas.

O caso que envolve a contratação dos serviços da *TechBiz Forense Digital* e *Cellebrite* pela administração pública para o fornecimento de soluções de acesso e extração de dados de qualquer dispositivo, aplicativo ou sistema de segurança, e que possibilita a criação de perfis detalhados dos cidadãos com base em ampla gama de dados pessoais demonstram que milhares de cidadãos estão sob vigilância sem garantias adequadas de proteção e segurança dessas informações. Além disso, a falta de transparência sobre o uso dessas tecnologias que conseguem burlar as camadas de segurança de dispositivos privados e o compartilhamento dessas informações entre o governo e empresas privadas estrangeiras levanta sérias preocupações sobre possíveis abusos e violações da privacidade dos cidadãos[63].

Já em relação ao Projeto *Excel*, que visa criar um banco de dados formado por informações obtidas por meio das soluções da *Cellebrite* que ultrapassam medidas de

[63] MERCADORES DA INSEGURANÇA: CONJUNTURA E RISCOS DO HACKING GOVERNAMENTAL NO BRASIL. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 02 de maio de 2024. P. 48-50.

segurança de aparelhos privados, levanta sérias suspeitas sobre o enviesamento sobre quais crimes serão objeto do monitoramento, visto que os crimes que afetam prioritariamente a população negra estão mais sujeitos ao monitoramento indiscriminado em relação aos crimes considerados de ordem econômica[64].

A contratação das empresas *Verint Systems* e *Cognyte* é outro caso que demonstra como o Estado brasileiro está familiarizado com refinadas tecnologias e sistemas de monitoramento indiscriminado e espionagem em larga escala sem métricas de proteção de dados, visto que membros do governo utilizam ferramentas para vigiar investigadores de corrupção, como é a situação do governador do Pará envolvido na espionagem dos responsáveis por apurar o desvio de dinheiro para a compra de respiradores durante a pandemia do Covid 19[65].

Além disso, a *Verint Systems* mantém contratos com países com históricos autoritários, como o Sudão do Sul, onde o governo utiliza tecnologias de vigilância em massa para monitorar e repreender jornalistas e ativistas de direitos humanos com base nas informações que foram coletadas de seus dispositivos pessoais[66].

Ainda sobre a empresas *Verint Systems* e *Cognyte*, a contratação sem licitação do software *First Mile* que permite o monitoramento da localização de celulares pessoais pela Agência Brasileira de Inteligência (ABIN) demonstra a falta de finalidades legítimas que justifiquem a motivação para a vigilância constante de mais de 1.800 dispositivos privados de políticos, jornalistas, advogados e ministros do Supremo Tribunal Federal (STF). Nesse sentido, fica expressa a ausência de parâmetros transparentes e legalmente justificáveis para a utilização dessas ferramentas, uma vez que não foram estabelecidos critérios claros sobre quem pode ser alvo de vigilância e com base em quais justificativas legítimas[67].

Assim, a associação entre o Estado Brasileiro e as empresas *Verint Systems* e *Cellebrite* levanta sérios questionamentos sobre a utilização de dispositivos de monitoramento e sobre a proporcionalidade da sua utilização, posto que tais tecnologias estão sendo instrumentalizadas para legitimar práticas abusivas e perseguir indivíduos por meio da coleta intensiva de seus dados pessoais sem a

---

[64] *Ibidem p. 65-67*
[65] Ibidem p. 50-51
[66] Ibidem
[67] COMO O BRASIL VIROU O PARAÍSO DA ESPIONAGEM ILEGAL. The Intercept Brasil. 28 de outubro de 2023. Disponível em: https://www.intercept.com.br/2023/10/28/brasil-virou-paraiso-da-espionagem-ilegal-com-michel-temer-jair-bolsonaro/. Acesso em 13 de maio de 2023.

devida garantia de seus direitos fundamentais à proteção de dados e à autodeterminação informacional.

Dessa maneira, a partir dos exemplos supracitados sobre o uso de tecnologias de vigilância de dados pessoais em massa, fica nítida a fragilidade da proteção dados no Brasil, principalmente no tocante à utilização dessas ferramentas e sistemas pelo Estado. A falta de transparência e parâmetros legais que justifiquem a coleta indiscriminada e a vigilância em excesso de dados pessoais rompe com a ideia democrática de que os indivíduos possuem o direito de manter determinados aspectos da sua vida privada distante do controle estatal.

Nesse sentido, ao contratar empresas especializadas em achar brechas de segurança que permitam acessar dispositivos pessoais, o Estado Brasileiro se aproxima de um autoritarismo tecnológico que permite a vigilância constante de todas as experiências, os costumes e hábitos das pessoas. Assim, com o respaldo de que a Lei Geral de Proteção de Dados não se aplica para situações de segurança pública, o governo faz a contratação de sofisticados softwares para monitorar indiscriminadamente dados pessoais dos cidadãos que não possuem conhecimento de que estão sob vigilância constante e também pouco sabem como suas informações serão tratadas.

Soma-se ao problema, a dificuldade de encontrar como são feitas as contratações do governo com essas empresas, que muitas vezes aparecem como contratação sigilosa, o que dificulta a obtenção de mais informações sobre quais entidades estão investindo em ferramentas de vigilância em massa[68]. Como consequência, direitos como a liberdade, a privacidade e a autodeterminação passam a ser frequentemente relativizados, uma vez que o Estado investe em meios de obter informações pessoais de seus cidadãos ao passo que estes não possuem conhecimento das operações que essas tecnologias estão envolvidas e muito menos como seus dados estão sendo tratados e a motivação para tanto.

[68] MERCADORES DA INSEGURANÇA: CONJUNTURA E RISCOS DO HACKING GOVERNAMENTAL NO BRASIL. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 02 de maio de 2024.

6 CONSIDERAÇÕES FINAIS

A partir do que foi exposto ao longo deste trabalho, é possível perceber que a utilização de tecnologias e sistemas de vigilância com acesso a dispositivos privados pelo Estado brasileiro corrobora para uma nova forma de estrutura social em que direitos como a privacidade e a autodeterminação informacional são relativizados em prol do constante monitoramento dos cidadãos brasileiros.

Nesse sentido, ficou evidente que a associação do estado brasileiro com empresas privadas que burlam camadas de segurança de dispositivos pessoais amplia a capacidade de vigilância estatal, o que permite o acesso irrestrito a uma vasta gama de informações pessoais sem salvaguardas necessárias para proteger os dados dos cidadãos brasileiros que não possuem conhecimento ou controle sobre como seus dados serão tratados.

Assim, a análise dos casos apresentados demonstrou que a falta de transparência e a ausência de critérios claros para o uso dessas ferramentas de vigilância resultam em abusos que comprometem a integridade dos direitos fundamentais. O monitoramento indiscriminado, sem justificativas legais adequadas, evidencia práticas de espionagem generalizadas que violam a privacidade dos cidadãos e os expõe a possíveis perseguições políticas e ideológicas, discriminação racial e outras formas de injustiças.

Além disso, utilização de softwares avançados para monitorar e coletar dados sem a devida regulamentação e supervisão judicial levanta sérias preocupações sobre o futuro da privacidade e da liberdade no país, posto que a contratação de empresas conhecidas por fornecer tecnologias de vigilância reforça a percepção de que o Estado brasileiro se aproxima de práticas autoritárias por retirar da população o direito de escolha sobre como suas informações serão tratadas pelo poder público e por comprometer o Estado de Direito ao afastar a participação popular sobre o uso dessas ferramentas.

Dessa maneira, os resultados dessa pesquisa foram satisfatórios, de modo que foi possível atingir os objetivos propostos e responder os questionamentos introdutórios que orientaram o desenvolvimento do tema. Isto posto, o presente trabalho pretende contribuir e fomentar a discussão sobre o avanço de tecnologias e dispositivos que permitem a vigilância e o monitoramento de dados pessoais em larga

escala pelo Estado Brasileiro e seus efeitos para os direitos de privacidade e autodeterminação informacional.

Portanto, é imperativo que se estabeleçam mecanismos rigorosos de controle e fiscalização sobre o uso dessas tecnologias pelo Estado. A criação de legislação específica que garanta a proteção dos dados pessoais, aliada a uma maior transparência nas contratações e operações realizadas com empresas de vigilância, são medidas essenciais para resguardar os direitos dos cidadãos e prevenir abusos.

Ademais, é crucial promover um debate público amplo e inclusivo sobre o uso de tecnologias de vigilância e suas implicações para a sociedade. A conscientização e a participação da população sobre os riscos associados à coleta massiva de dados e a importância da proteção da privacidade são passos fundamentais para fortalecer a democracia e garantir que os avanços tecnológicos sejam utilizados de forma legal e responsável.

Em conclusão, há muito o que se discutir ainda sobre a utilização de dispositivos e tecnologias de vigilância pelo Estado e é necessário um esforço conjunto de todos os setores da sociedade para garantir que essas ferramentas sejam utilizadas de maneira transparente e de acordo com princípios democráticos que determinam limites entre o público e o privado. Somente assim será possível assegurar um equilíbrio entre o avanço tecnológico e a proteção dos direitos à privacidade e à autodeterminação informacional.

REFERÊNCIAS

Abin de Ramagem gastou R$31 milhões com ferramentas de vigilância secretas e sem licitação. A Pública. 25 de abril de 2023. Disponível em: https://apublica.org/2023/04/abin-de-ramagem-gastou-r-31-milhoes-com-ferramentas-de-vigilancia-secretas-e-sem-licitacao/

ALVES, Fabrício; VALADÃO, Rodrigo. Proteção de Dados Pessoais na Segurança Pública - Breves considerações acerca do art. 4º, inciso III e §1º da LGPD. Migalhas, 23 de dezembro de 2022. Disponível em: https://www.migalhas.com.br/coluna/dados-publicos/379087/protecao-de-dados-pessoais-na-seguranca-publica. Acesso em 04 de maio de 2024.

Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados. Data Privacy Brasil. 18 de setembro de 2019. Disponível em: https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados-2/. Acesso em 15 de maio de 2024.

AUTODETERMINAÇÃO INFORMATIVA: COMO ESSE DIREITO SURGIU E COMO ELE ME AFETA? Laboratório de Políticas Públicas e Internet – LAPIN. 27 de abril de 2021. Disponível em: https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/. Acesso em 18 de maio de 2024.

BIONI, Bruno R. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 29 nov. 2023.

Brasil. LEI Nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Brasília, DF: Diário Oficial da União, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 10 de maio de 2024.

Brasil. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6387 MC-REF / DF. MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. Relatora Ministra Rosa Weber, 07 de maio de 2020. P.55.

Como o Brasil virou o paraíso da espionagem ilegal. The Intercept Brasil. 28 de outubro de 2023. Disponível em: https://www.intercept.com.br/2023/10/28/brasil-virou-paraiso-da-espionagem-ilegal-com-michel-temer-jair-bolsonaro/. Acesso em 13 de maio de 2023.

Decreto nº 5.484, de 30 de junho de 2005 (Política de Defesa Nacional - PDN)
https://www.migalhas.com.br/coluna/dados-publicos/379087/protecao-de-dados-pessoais-na-seguranca-publica

Defendendo o Brasil do Tecnoautoritarismo. Data Privacy Brasil. Disponível em: https://www.dataprivacybr.org/projeto/defendend_o_brasil_do_tecnoautoritarismo/. Acesso em 23 de novembro de 2023.

GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. São Paulo: SRV Editora LTDA, 2023. *E-book.* ISBN 9786555599480. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599480/. P. 47. Acesso em: 30 mai. 2024.

GOMES, Ana. Espionagem governamental – nem papo futurista, nem coisa da sua cabeça. Instituto de Referência em Internet e Sociedade, 31 de outubro de 2023. Disponível em: https://irisbh.com.br/espionagem-governamental-nem-papo-futurista-nem-coisa-da-sua-cabeca/. Acesso em 04 de maio de 2024.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina, 2020. *E-book.* ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 01 mai. 2024.

LUIZ, Gil Mendes. Guerra às drogas, guerra aos negros. Ponte Jornalismo, 2021. Disponível em https://ponte.org/guerra--as-drogas-guerra-aos-negros/. Acesso em 30 de abril de 2024.

MARTINS, Ricardo Maffeis; GUARIENTO, Daniel Bittencourt. Emenda Constitucional torna a proteção de dados pessoais um direito fundamental. 18 de fevereiro de 2022. Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/359941/ec-torna-a-protecao-de-dados-pessoais-um-direito-fundamental. Acesso em 01 de maio de 2024.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Revista de Ciência Jurídicas Pensar. e-ISSN:2317-2150. v. 25, n. 4, p. 1-18, out./dez. 2020.

Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). Novembro de 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 29 de abril de 2024

Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados. The Intercept. 21 de maço de 2022. Disponível em https://www.intercept.com.br/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados/: Acesso em 10 de maio de 2024.

O que é o FirstMile, software que teria sido usado pela Abin para monitorar jornalistas e ministros do STF. BBC News. 23 de outubro de 2023. Disponível em: https://www.bbc.com/portuguese/articles/c3g32mz1dzdo. Acesso em 13 de maio de 2023.

PORTO, Douglas. Negros representam 78% das pessoas mortas por armas de fogo no Brasil. CNN Brasil, 2021. Disponível em https://www.cnnbrasil.com.br/nacional/negros-representam-78-das-pessoas-mortas-por-armas-de-fogo-no-brasil/. Acesso em 30 de abril de 2024.

Quais são os limites? Maior escândalo da Abin reabre discussão sobre as atividades de inteligência. O Globo. 04 de fevereiro de 2024. Disponível em: https://oglobo.globo.com/politica/noticia/2024/02/04/quais-sao-os-limites-maior-escandalo-da-abin-reabre-discussao-sobre-as-atividades-de-inteligencia.ghtml. Acesso em 16 de maio de 2024.

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em 05 de maio de 2024.

Sistema de espionagem usado ilegalmente pela Abin pode mostrar localização de qualquer celular - Data Privacy Brasil Research. Data Privacy Brasil. Disponível em: https://www.dataprivacybr.org/documentos/sistema-de-espionagem-usado-ilegalmente-pela-abin-pode-mostrar-localizacao-de-qualquer-celular/?idProject=125 Acesso em 10 de maio de 2024.

SNOWDEN, Edward; Eterna Vigilância. São Paulo. Editora Planeta do Brasil Ltda, 2019. 288p.

The world's most valuable resource is no longer oil, but data. The Economist. 6 de maio de 2017. Disponível em https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em 10 de maio de 2024.

ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano na Nova Fronteira do Poder. 1ª Edição. Rio de Janeiro. Editora Intrínseca, 2020.