



ESCOLA DA MAGISTRATURA DO ESTADO DO RIO DE JANEIRO

OS RISCOS E OS LIMITES DE FERRAMENTAS DE MONITORAMENTO SECRETO DE
DISPOSITIVOS ELETRÔNICOS

Matteus Rodriguez Camarinha Loureiro

Rio de Janeiro
2025

MATTEUS RODRIGUEZ CAMARINHA LOUREIRO

OS RISCOS E OS LIMITES DE FERRAMENTAS DE MONITORAMENTO SECRETO DE
DISPOSITIVOS ELETRÔNICOS

Artigo Científico apresentado como exigência de
conclusão de Curso de Pós-Graduação *Lato Sensu*
da Escola da Magistratura do Estado do Rio de
Janeiro. Professores Orientadores:

Monica C. F. Areal

Nelson C. Tavares Junior

Ubirajara da Fonseca Neto

Rafael Mario Iorio Filho

Rio de Janeiro
2025

OS RISCOS E OS LIMITES DE FERRAMENTAS DE MONITORAMENTO SECRETO DE DISPOSITIVOS ELETRÔNICOS

Matteus Rodriguez Camarinha Loureiro

Graduado pelo Instituto Brasileiro de Mercados e Capitais (IBMEC). Advogado.

Resumo- o avanço tecnológico trouxe inúmeras mudanças no contexto social, fazendo com que o Estado se utilize de novos mecanismos que auxiliam na busca de potenciais ameaças à sociedade, bem como nas investigações criminais. As ferramentas de monitoramento secreto aparecem no ordenamento jurídico levantando debates acerca de sua admissibilidade, isso porque seu caráter invasivo ultrapassa limites constitucionais. O presente trabalho irá analisar as normas vigentes capazes de regulamentar o uso dessas ferramentas, assim como a violação de direitos constitucionais, defendendo, portanto, a necessidade de uma nova legislação.

Palavras-chave – Direito Constitucional; Princípios Fundamentais; Direito à Privacidade; monitoramento secreto.

Sumário – Introdução. 1. Análise sobre as Leis que regem o universo virtual e as funções das ferramentas de monitoramento secreto. 2. As ferramentas e seus riscos, bem como o embate entre a segurança pública e os direitos constitucionais. 3. Da necessidade de criação de uma regulamentação específica. Conclusão. Referências.

INTRODUÇÃO

O presente artigo irá abordar a introdução das ferramentas de monitoramento secreto no universo virtual, que são utilizadas para monitorar e investigar atividades suspeitas. A utilização dessas ferramentas continua aumentando ao redor do mundo e a falta de uma regulamentação poderá gerar riscos a sociedade.

O trabalho visa ao debate sobre a utilização de ferramentas de monitoramento secreto, por parte de serviços de inteligência de órgãos e agentes públicos, de dispositivos eletrônicos, que possuem acesso a dados e informações pessoais em uma busca preventiva de ameaças a sociedade. Evidente que tal liberdade nessas ferramentas podem gerar um risco aos direitos constitucionais, que será analisado ao longo da pesquisa.

A tecnologia tomou conta da vida moderna e sem ela grande parte da população teria dificuldade no seu dia a dia. É possível ter acesso a qualquer tipo de informação, trabalho e manter conexões com outros cidadãos a partir do uso de aparelhos eletrônicos como tablets, celulares e outros, além de registrar momentos em família e utilizar aplicativos de banco.

Entretanto, como todo e qualquer avanço social é preciso que o Estado regularize e regulamente os limites de atuação dos novos programas. Para isso, algumas leis foram criadas visando a atuação virtual, assim como a proteção de dados. Apesar da criação das leis, devido

a rápida evolução tecnológica, órgãos e agentes públicos começaram a utilizar ferramentas e softwares aptos a monitorar e ter acesso a dados pessoais na busca por informações capazes de antecipar fatos que gerem risco à sociedade.

Essas ferramentas estão sendo utilizadas de forma deliberada, porque as leis ainda não possuem regulamentação atualizada, gerando assim um eminente risco de violação dos preceitos fundamentais, como o direito à privacidade, direito a informação e a proteção de dados pessoais.

Sendo assim, o primeiro capítulo terá como objetivo o debate acerca das Leis que regem o universo virtual, bem como explicar como as ferramentas de monitoramento secreto atuam, pois são capazes de monitorar a vida pessoal do cidadão sem o seu consentimento, na busca por informações que possam gerar risco à sociedade. Em contrapartida, é neste ponto que é possível verificar um risco aos direitos fundamentais.

Nesse sentido, o segundo capítulo terá como foco o questionamento no embate entre a segurança pública e os direitos fundamentais, pois qual seria o limite de atuação dessas ferramentas, tendo em vista que podem fornecer acesso total aos dados pessoais. O capítulo também irá pontuar quais princípios constitucionais estão em risco com a utilização dessas ferramentas, fazendo uma ponderação normativa entre eles.

Por fim, tendo analisado todos os conflitos, o terceiro capítulo irá demonstrar a necessidade de reformulação ou de criação de novas Leis, capazes de delimitar a atuação de órgãos e agentes públicos na utilização desses softwares, de modo que possam ser utilizados de uma maneira mais eficiente, ajudando tanto nas investigações criminais, como no combate a ameaças de forma preventiva, porém sem que haja um risco de violação à Constituição.

O artigo é desenvolvido através de uma pesquisa qualitativa, bem como explicativa, visto que busca uma melhor compreensão sobre o tema. Para isso, o pesquisador irá se utilizar de pesquisas bibliográficas que se relacionam com o tema, sites da internet, legislações, jurisprudências, entre outros.

1. ANÁLISE SOBRE AS LEIS QUE REGEM O UNIVERSO VIRTUAL E AS FUNÇÕES DAS FERRAMENTAS DE MONITORAMENTO SECRETO

O tema que abrange a utilização das ferramentas de monitoramento secreto é complexo, e, portanto, se faz necessário um melhor entendimento sobre sua atuação. Essas ferramentas, também conhecidas como *spywares*, são utilizadas para registrar e monitorar todas as atividades do usuário.

Os *spywares* são *softwares* maliciosos que possuem como principal função a coleta de dados e podem ser capazes de invadir qualquer tipo de sistema, repassando aos titulares do software todos os dados coletados sem que o usuário consiga perceber a invasão, podendo dizer que são quase invisíveis¹. Uma vez dentro do sistema, a ferramenta será capaz de rastrear a localização do aparelho, comandar ações, como a utilização da câmera, o uso do microfone que pode ser utilizado como escuta, o acesso a dados pessoais, entre outros.

A inteligência por trás das ferramentas de monitoramento parte de uma premissa de vulnerabilidade no sistema de informação, que uma vez descoberta é atacada e explorada para que as informações sejam extraídas. O uso desse mecanismo por parte do Estado fomenta e ajuda na criação de vulnerabilidade no sistema de comunicação.

Existem diversos tipos de *spywares* que possuem funções variadas, sendo cada um deles específico para determinado fim². Entre eles é possível destacar o *infostealer* que irá ter acesso aos dados de um computador como usuário, e-mail e senha, o *keylogger* que será capaz de registrar tudo o que o usuário digita e o mais recente entre eles, o *tryout*, que foi desenvolvido com a intenção de espionar dispositivos móveis.

Um ponto importante a se destacar é a pesquisa realizada pela Fundação Getúlio Vargas³, que constatou em 2024, que existem 2,2 dispositivos eletrônicos para cada habitante no Brasil.

Esse dado é muito relevante no contexto da utilização dessas ferramentas, pois torna seu alcance praticamente nacional, ainda que certa parte da população não tenha acesso a esses dispositivos eletrônicos, a maioria está conectada, fazendo com que a coleta de dados seja cada vez maior.

Com isso, alguns Estados começaram a utilizar essas ferramentas com a justificativa de prevenir potenciais ameaças. O monitoramento realizado por órgãos estatais teve início com o objetivo de coletar dados a fim de identificar riscos como terrorismo, tráfico, e combatê-los antes que pudessem ser executados visando a segurança pública.

Todavia, o imenso universo de informações produzido por essas ferramentas liga um sinal de alerta a sociedade, isso porque o cidadão, polo mais fraco na relação, não conseguirá

¹ STARTI. **Spyware:** sorria, você está sendo espionado. Starti, 2021. Disponível em: <https://blog.starti.com.br/spyware/>. Acesso em: 10 jun. 2025.

² YOUTUBE. **O que é spyware?** Descubra como se proteger. Brasília, 26 de out. de 2021. 1 vídeo (4 min) Publicado pelo canal Starti. Disponível em: https://www.youtube.com/watch?v=vJWn_xvOSNs&t=68s. Acesso em: 10 jun. 2025.

³ BRASIL tem mais smartphones do que habitantes, aponta levantamento. **Veja**, São Paulo, 27 de abr.2023. Disponível em: <https://veja.abril.com.br/tecnologia/brasil-tem-mais-smartphones-do-que-habitantes-aponta-levantamento>. Acesso em: 11 mar. 2025.

se defender de tais invasões. Ainda que o objetivo do governo seja prevenir ataques, ou até mesmo investigações criminais, tal liberdade de acesso aos dados pessoais poderia violar princípios fundamentais.

Esse fato não está voltado apenas para cada cidadão, mas também a coletividade, uma vez que essa espionagem pode alcançar jornalistas e profissionais da comunicação, fazendo com que a informação seja passível de controle e colocando em xeque a própria democracia e a liberdade de expressão.

Em breve análise sobre o tema, é possível destacar alguns pontos em que a utilização dessas ferramentas se encontra em lacunas legislativas e sua admissibilidade ainda é discutida, seja na fiscalização por parte de agentes públicos, ou em investigações criminais.

No ordenamento jurídico duas leis foram de suma importância no combate a proteção de dados, sendo elas o Marco Civil da Internet (Lei nº 12.965/14⁴), que estabeleceu direitos e garantias no meio digital como a liberdade de expressão, além de trazer a inviolabilidade e o sigilo das comunicações, e a Lei Geral de Proteção de Dados (Lei nº 13.709/18⁵), que resguardou a segurança e a privacidade dos dados pessoais, sendo possível dizer que essas leis revolucionaram o mundo cibernético trazendo inovações e limites de atuações virtuais.

Entretanto, o mundo virtual possui avanços significativos e de maneira contínua, onde de um dia para o outro, tudo pode mudar. Apesar das leis supracitadas serem “recentes” algumas normas não acompanham a velocidade da internet, criando lacunas e demonstrando a necessidade de mudanças legislativas.

Sobre o tema, deve-se destacar a arguição de descumprimento de preceito fundamental 1.143⁶, que foi proposta pela Procuradoria-Geral da República e possui como relator o Ministro Cristiano Zanin, que visa discutir as lacunas existentes na utilização dos programas invasivos.

⁴ BRASIL. **Lei nº 12.965/14, de 23 de abril de 2023.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Presidente da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 11 mar. 2025.

⁵ BRASIL. **Lei nº 13.709/18, de 14 de agosto de 2018.** Estabelece a Lei Geral de Proteção de dados pessoais. Brasília, DF: Presidente da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 11 mar. 2025.

⁶ BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental 1.143.** Utilização de ferramentas de monitoramento secreto. Relator: Min. Cristiano Zanin, 14 de maio de 2021. Disponível em: <https://portal.stf.jus.br/jurisprudencia/>. Acesso em: 14 mar. 2025.

Atualmente, existem duas leis que devem ser observadas para que os *spywares* possam ser aplicados, sendo a Lei nº 9.296/96⁷, Lei das Interceptações Eletrônicas e a Lei nº 12.850/2013⁸, Lei das Organizações Criminosas que citam os agentes virtuais infiltrados.

Segundo Alisson Alexandro Possa⁹, da Comissão de Direito Digital da OAB, nenhuma dessas leis prevê medidas em que esses malwares possam ser aplicados, devido ao seu caráter invasivo e, conseqüentemente, a possibilidade de acesso a uma grande quantidade de dados. Esse caráter torna praticamente impossível filtrar o que efetivamente o órgão ou agente fiscalizador terá acesso.

Acrescenta, portanto, em conformidade ao princípio da reserva legal, a necessidade de uma legislação que autorize a instalação desses *softwares*, bem como a determinação de limites que prevejam garantidas para evitar abusos.

Outro fator importante, já citado anteriormente, são os riscos trazidos a coletividade e aos meios de comunicação que podem atingir o direito à informação. A imprensa, que se faz através dos jornalistas é responsável por levar as notícias à público, é através dela que se torna possível o acesso às informações.

Os jornalistas, para publicarem uma matéria necessitam de fontes, e muitas vezes ficam em situações que não é possível expor a origem da informação. A divulgação da fonte nem sempre é uma tarefa simples, pois em grande parte dos casos, a pessoa que compartilha a informação pede o anonimato, tendo em vista que ela poderá correr risco de vida ou de ser perseguida.

A invasão e a espionagem nos aparelhos telefônicos dos profissionais de comunicação trazem inúmeros malefícios a democracia. Isso porque, o Estado poderia controlar as matérias atacando no princípio, antes de se tornarem públicas, e esse controle não é apenas sinônimo de ditadura, com tamanho acesso a dados confidenciais o monitoramento dessas informações poderia crescer significativamente, o que já ocorreu em outros países, trazendo prejuízos a sociedade.

⁷ BRASIL. **Lei nº 9.296/96, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, DF: Presidente da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19296.htm. Acesso em: 11 mar. 2025.

⁸ BRASIL. **Lei nº 12.850/2013, de 2 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal. Brasília, DF: Presidente da República, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm. Acesso em: 12 mar. 2025.

⁹ BRASIL. Supremo Tribunal Federal. **Audiência Pública sobre o uso de ferramentas de monitoramento secreto.** Brasília, 11 de jun. de 2024. 1 vídeo (149 min.) Publicado pelo canal STF. Disponível em: <https://www.youtube.com/watch?v=ufyNUW0BEvY>. Acesso em: 14 mar. 2025.

Deve-se então destacar o parágrafo primeiro do artigo 220 da Constituição Federal¹⁰, que dispõe, “[...] Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.”

Logo, é possível afirmar que o artigo supracitado garante explicitamente que nenhuma lei poderá conter dispositivo que restrinja a plena liberdade de informação jornalística. Ademais, o Supremo Tribunal Federal¹¹ entendeu pela impossibilidade de o Estado fixar quaisquer restrições a atividade jornalística, incluindo o direito constitucional do sigilo das fontes.

Sendo assim, tendo como base o que foi exposto anteriormente, é possível dizer que os limites de atuação das ferramentas de monitoramento secreto ainda não estão previstos em lei específica, sendo necessário o estudo de leis diversas para justificar sua aplicabilidade, ainda que não seja uma unanimidade na doutrina.

A existência de lacunas legislativas, faz com que o uso de tais ferramentas sem uma regulamentação direta coloque em risco princípios constitucionais, que serão analisados a seguir. Conclui-se, então, que as leis do ordenamento jurídico que regem o universo cibernético não conseguem abranger toda a atuação desses *spywares*, o que demonstra mais uma vez a necessidade de uma nova legislação a fim de impor limites de atuação respeitando os direitos e garantias de cada cidadão e assim, evitando abusos, bem como seu uso indevido.

2. AS FERRAMENTAS E SEUS RISCOS, BEM COMO O EMBATE ENTRE A SEGURANÇA PÚBLICA E OS DIREITOS CONSTITUCIONAIS

Devido a rápida evolução tecnológica, as ferramentas de monitoramento secreto se tornaram uma forte aliada da segurança pública, sendo utilizadas por órgãos de inteligência do Estado e agentes públicos, em investigações de potenciais riscos à sociedade e até mesmo em investigações criminais.

Contudo, como abordado no capítulo anterior, as legislações do ordenamento jurídico tiveram dificuldade de acompanhar esses avanços tecnológicos, fazendo com que o uso dessas

¹⁰ BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 mar. 2025.

¹¹ FUX, Luiz. Supremo Tribunal Federal. **Restrições à imprensa tornam a democracia uma mentira e a Constituição uma mera folha de papel**. Disponível em: <https://noticias.stf.jus.br/postsnoticias/restricoes-a-imprensa-tornam-a-democracia-uma-mentira-e-a-constituicao-uma-mera-folha-de-papel-afirma-presidente-do-stf/>. Acesso em: 10 jun. 2025.

ferramentas se tornasse algo perigoso a coletividade, tendo em vista não haver limites, impostos por lei, para regulamentar suas atividades.

É incontroverso que a utilização desses *softwares* conflita diretamente com princípios constitucionais, uma vez que são verdadeiros espões cibernéticos e possuem acesso a uma infinidade de dados. É preciso destacar então, quais são esses princípios e em que ponto eles entram em conflito.

Inicialmente, deve-se destacar o direito à privacidade, previsto no artigo 5º, X, da Constituição Federal¹². Este princípio garante a cada cidadão a inviolabilidade de sua intimidade, de sua vida privada, de sua honra e sua imagem, prevendo inclusive direito a indenização em caso de violação. É preciso enfatizar que com os avanços da tecnologia e das redes sociais, a grande maioria das pessoas carrega suas intimidades literalmente na palma da mão, com o massivo uso de aparelhos eletrônicos, onde é possível encontrar desde fotos até aplicativos de banco, por isso a privacidade não se limita as relações físicas, mas também a todo o universo cibernético e aquilo que nele é divulgado.

Outro direito constitucional de extrema relevância ao tema é a inviolabilidade das comunicações, previsto no artigo 5º, XII, da Constituição Federal¹³, esse inciso foi inserido pela Lei nº 9.296/96, garantindo o sigilo das comunicações telegráficas, de dados e das comunicações telefônicas. Todavia, esse artigo também prevê a possibilidade de quebra desse sigilo em casos em que houver ordem judicial, obedecendo as hipóteses e na forma que a lei estabelecer.

Nesse sentido, ainda há uma controvérsia, que será mais a frente analisada, sobre a possibilidade de utilização dos *softwares* em casos de investigações criminais ou em instruções processuais penais quando houver a quebra desse sigilo, tendo em vista que ainda não estão regulamentados por lei específica que determine os limites de acesso aos dados, o que torna essa busca invasiva.

Outrossim, o direito à informação, também entra em rota de colisão com as ferramentas de monitoramento secreto, e neste caso é a coletividade que está ameaçada. Tendo previsão legal no artigo 5º, IX, da Constituição Federal¹⁴, esse princípio garante a livre expressão dos meios de comunicação. É através deste que a sociedade tem acesso as notícias de um modo geral, portanto, um controle do Estado sobre as informações que circulam na

¹² BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 mar. 2025.

¹³ *Ibid.*

¹⁴ *Ibid.*

imprensa não afeta somente a classe jornalística, mas também se torna uma afronta a própria democracia.

Samara Castro¹⁵, diretora da Secretaria de Políticas Digitais e representante da Secom, sinaliza sobre os riscos do uso das ferramentas de monitoramento secreto, cita que em 2017, o Relator Especial da ONU sobre liberdade de expressão, destaca alguns efeitos negativos sobre o tema, abordando o *software* “Pegasus” que foi utilizado no México espionando cerca de 180 jornalistas ao redor do mundo.

Apesar dos riscos de violação aos preceitos fundamentais, ainda existe uma divergência doutrinária sobre o tema em relação ao seu uso. Isso porque, ainda não é possível determinar a informação que será extraída do sistema, ou seja, uma vez que o *software* invade determinado aparelho ele terá acesso a uma grande quantidade de informações e não somente a uma informação específica, dividindo opiniões entre os autores doutrinários.

Nesse sentido, José Afonso da Silva¹⁶, especialista em direito constitucional, entende que apesar dos riscos apresentados, ainda que o software tenha acesso a essa quantidade de dados, ele ainda pode ser justificado em exceções, como em investigações criminais por exemplo, porém pontua que seu uso deve ser feito observando os direitos e princípios constitucionais.

Em contrapartida, é possível verificar opiniões divergentes com relação ao seu uso, uma vez que pode apresentar riscos a intimidade e a privacidade dos indivíduos. Os Ministros Luís Roberto Barroso e Alexandre de Moraes alertam sobre os riscos apresentados por esses softwares. O primeiro¹⁷, alega que a utilização desses softwares sem limitação vai de encontro aos princípios constitucionais, podendo acarretar uma vigilância massiva, enquanto o segundo¹⁸ defende um controle judicial rígido em relação aos *spywares* a fim de evitar seus abusos.

Sendo assim, é possível perceber o conflito entre a segurança pública e os direitos constitucionais. É bem verdade, que a evolução tecnológica segue em ritmo acelerado e não é somente o cidadão de bem que usufrui de seus avanços, com o passar do tempo a criminalidade também evolui e se utiliza de mecanismos modernos para chegar a seus determinados fins, não atoa os crimes cibernéticos cada vez mais vem aumentando. A era tecnológica proporciona a

¹⁵ BRASIL. Supremo Tribunal Federal. **Audiência Pública sobre o uso de ferramentas de monitoramento secreto**. Brasília, 11 de jun. de 2024. 1 vídeo (149 min.) Publicado pelo canal STF. Disponível em: <https://www.youtube.com/watch?v=ufyNUW0BEvY>. Acesso em: 14 mar. 2025.

¹⁶ SILVA, José Afonso. **Curso de Direito Constitucional Positivo**. 45. ed. Salvador: JusPodivm, 2024.

¹⁷ BARROSO, Luís Roberto. **O Direito Constitucional e a Efetividade de Suas Normas**. Rio de Janeiro: Renovar, 2009.

¹⁸ MORAES, Alexandre de. **Direito Constitucional**. 38. ed. São Paulo: Atlas, 2022.

esses criminosos utilizar mecanismos de criptografia avançada, tornando mais difícil o acesso a esses dados.

Para evitar que criminosos se beneficiem das novas tecnologias, é preciso que o sistema de investigação também caminhe junto a essa evolução, se utilizando dos meios mais modernos para acessar essas informações. As ferramentas de monitoramento, podem ser vistas como um importante avanço nas investigações desses crimes, atuando como aliado do investigador dando todo o suporte necessário para realizar as buscas em mundo digitalizado.

Ademais, em investigações criminais de difícil localização do alvo, os softwares poderão dar acesso a câmeras, escutas e até mesmo espionar o aparelho telefônico do investigado, o que daria acesso a mensagens, fotos e tudo aquilo que estiver no sistema, sem a necessidade de apreensão do aparelho, tudo feito de forma remota, facilitando a produção de prova nesses casos.

Entretanto, é preciso destacar que tal liberdade na utilização desses *softwares*, acarretaria uma invasão total de informação, criando um evidente embate com os princípios constitucionais supracitados. Até que ponto a utilização dos *spywares* poderia ajudar nas buscas criminais, sem se utilizar dessa invasão desenfreada. Esse é exatamente o maior desafio do ordenamento jurídico, encontrar um meio termo para sua utilização.

O uso das ferramentas se torna perigoso, primeiro pela falta de legislação específica que limite sua atuação e pelo tamanho poder invasivo que possui. Quando é utilizado a fim de extrair informações, ele não só dará acesso aquela informação desejada, mas sim a tudo que estiver no sistema, sendo praticamente impossível filtrar os dados que o investigador terá acesso. Portanto, caso uma empresa ou uma pessoa esteja sendo investigada, ela correrá o risco de ter informações confidenciais vazadas.

Dessa forma, havendo lacunas legislativas, e um evidente risco a direitos constitucionais, um controle judicial mais rígido deverá ser feito, evitando que seu uso seja livre, somente sendo aceito em casos específicos, em exceções, quando já utilizado todos os meios para obtenção de prova.

Desse modo, algumas jurisprudências seguiram esse mesmo pensamento, com destaque ao Habeas Corpus 91.867¹⁹, julgado pelo Supremo Tribunal Federal, com repercussão geral, que versou sobre a interceptação telefônica. Neste caso, o Supremo entendeu pela ilicitude da prova produzida em sede de inquérito policial, determinando que a interceptação

¹⁹ BRASIL. Supremo Tribunal Federal (2 Turma). **Habeas Corpus 91.867**. Litude da prova produzida durante o inquérito policial. Relator: Min. Gilmar Mendes, 20 de setembro de 2012. Disponível em: <https://portal.stf.jus.br/jurisprudencia/>. Acesso em: 14 mar. 2025.

telefônica somente poderá ser realizada através de ordem judicial, devendo ser observado os indícios da praticada do crime, para que justifiquem a interceptação.

Outro entendimento que demonstrou defesa aos princípios constitucionais foi o debate acerca da quebra de sigilo de dados pela Receita Federal. Nesse caso, o Supremo Tribunal Federal²⁰ firmou o Tema 990, que permite a Receita Federal encaminhar os dados para o Ministério Público somente quando houver indícios de algum delito e ao mesmo tempo, não permite ao Ministério Público requisitar esses dados sem prévia autorização judicial, que deverá ser fundamentada.

É possível extrair dessas decisões, que os Tribunais Superiores, ainda que haja uma lacuna legislativa sobre o tema de monitoramento secreto, vem direcionando seu posicionamento a proteção dos princípios constitucionais, exigindo critérios mais rigorosos para a utilização dessas ferramentas, bem como a existência de ordem judicial que autorize e justifique seu uso.

Sendo assim, no embate entre a segurança pública, com o uso das ferramentas de monitoramento secreto, e os direitos previstos na Constituição Federal, é possível afirmar que há um viés mais garantista, limitando o uso dessas ferramentas de forma desenfreada e abusiva.

Enquanto não houver uma legislação capaz de limitar e delimitar o uso dos *spywares* e o acesso às informações, é necessário que haja um controle mais rigoroso, evitando uma invasão a vida privada e garantindo o direito à informação, blindando os profissionais da área de comunicação para que não sofram interferência e que seja garantido o sigilo da fonte.

3. DA NECESSIDADE DE CRIAÇÃO DE UMA REGULAMENTAÇÃO ESPECÍFICA

Conforme abordado no presente artigo, o tema é cercado de incertezas que circulam sobre o funcionamento e a utilização das ferramentas, de modo que o uso dos *softwares* desencadeou um embate entre preceitos fundamentais analisado anteriormente. Ainda é discutida sua admissibilidade no âmbito público, por órgãos e agentes estatais, mas também no âmbito privado, visto que não há transparência na destinação das informações extraídas.

É certo, que as ferramentas de monitoramento são as mais intrusivas a disposição do Estado, promovendo uma vigilância remota e invasiva dos dispositivos eletrônicos, permitindo

²⁰ BRASIL. Supremo Tribunal Federal. **Tema 990**. Possibilidade de compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais do contribuinte. Relator: Min. Dias Toffoli, 28 de novembro de 2019. Disponível em: <https://portal.stf.jus.br/jurisprudenciarepercussao/verandamentoprocessos.asp?incidente=5213056&numeroprocesso=1055941&classeprocesso=re&numerotema=990>. Acesso em: 09 de abr. 2025.

acesso a dados pessoais sem limitações. Nesse sentido, tendo em vista seu carácter agressivo na busca por informações, essas ferramentas não podem ser equiparadas a interceptação telefônica, já regulamentada no ordenamento jurídico, pois apresenta maiores riscos à vida privada.

Importante salientar, que o conjunto de normas vigentes na legislação brasileira, garante que toda quebra de sigilo de dados deve ter fundamentação clara e que esteja de acordo com a lei, devendo ser ponderado o interesse público nas investigações criminais e os riscos trazidos pela invasão de dados²¹.

Dessa forma, há o entendimento que tal medida deve estar amparada pela proporcionalidade, ou seja, a quebra no sigilo de informações deve ser proporcional a seu fim no caso concreto, não podendo um órgão ou Estado vigiar de forma massiva a sociedade, visto que tal atitude não atenderia a proporcionalidade do ato.

Portanto, admitindo que seu uso deve ser proporcional ao caso, respeitando o interesse público, abre-se o questionamento sobre o limite dessa proporcionalidade, até onde é possível investigar sem que haja violação aos princípios. É neste ponto, que mais uma zona cinzenta se apresenta, não sendo possível extrair tal resposta das leis que regem o universo cibernético, como a Lei Geral de Proteção de Dados e o Marco Civil da Internet, demonstrando a necessidade de uma nova legislação para que tal limite seja estabelecido.

Deve-se destacar, que a normas vigentes, citadas anteriormente, que determinam uma fundamentação clara para a quebra de sigilo de informação, dizem respeito as investigações criminais e não se confundem com o serviço de inteligência. Nas investigações criminais, a polícia, de forma posterior ao fato, busca identificar os autores do crime, enquanto o serviço de inteligência, busca antecipar fatos e situações que possam gerar risco à sociedade e a instituições.

Sendo assim, com relação ao sistema de inteligência, previsto na Lei nº 9.883/99²², que deu origem a Agência Brasileira de Inteligência, é possível afirmar que não há um mecanismo de controle judicial prévio, que é possível observar em outros países democráticos, como a Espanha, onde a Suprema Corte Espanhola designa um juiz específico para avaliar casos

²¹ BRASIL. Superior Tribunal de Justiça (6 Turma). **Recurso em Habeas Corpus 117.462**. Por falta de fundamentação, Sexta Turma invalida quebra de sigilos telefônico, fiscal e bancário. Relator: Rogerio Schietti Cruz, 2 de setembro de 2019. Disponível em: <https://www.stj.jus.br/sites/porta1p/Paginas/Comunicacao/Noticias/28052021-Por-falta-de-fundamentacao--Sexta-Turma-invalida-quebra-de-sigilos-telefonico--fiscal-e-bancario.aspx>. Acesso em: 10 jun. 2025.

²² BRASIL. **Lei nº 9.883/1999, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN. Brasília, DF: Presidente da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19883.htm. Acesso em: 10 jun. 2025.

de inteligência, evidenciando uma necessidade de atualização da norma visando um controle mais efetivo, visto que a Lei não atua de forma incisiva na fiscalização das ferramentas.

Um dos principais pontos de discussão, sobre a criação de uma nova norma, é a garantia da democracia. Com a evolução da tecnologia, foram criados métodos de investigação que o Estado se utiliza para um melhor desempenho em suas buscas, visto que o sistema de defesa também melhorou, como a utilização da criptografia. Entretanto, tais métodos acabam sendo utilizados para investigações em massa por parte do Estado.

Esse fenômeno, de acordo com Pedro José Nasser Saliba²³, coordenador de assimetria e poder da Data Privacy Brasil, tem o nome de “tecno autoritarismo”, e cita uma passagem de Ingo Wolfgang Sarlet²⁴, que explica o termo:

[...] é a utilização, cada vez mais massiva, em termos quantitativos e qualitativos, dos recursos das tecnologias de comunicação e tecnologias digitais para o controle, por parte do Estado, da sociedade. O tecno autoritarismo não é um fenômeno típico somente de estados ditatoriais, mas é um fenômeno que está minando, de dentro para fora, as democracias.

Aduz também, sobre a tese utilizada pela Data Privacy Brasil acerca do tema, que entende que a utilização de *software* de extração de dados de aparelhos celulares de suspeitos, exigem um conjunto de freios, contrapesos e arranjos institucionais que garantam os princípios da necessidade, legalidade e proporcionalidade.

Em suma, o uso desses mecanismos, sem a correta regulamentação, demonstra mais uma vez riscos à sociedade e neste caso, à democracia. É preciso enfatizar que esse monitoramento é real nos países democráticos e que essa não é uma realidade distante, não se pode relaxar e afrouxar o sistema de fiscalização dessas ferramentas.

Portanto, após análise de todos os embates que cercam o tema, como a falta de legislação, os riscos aos direitos fundamentais e a democracia, é possível verificar a necessidade de criação de uma regulamentação específica, garantindo limites a utilização dos *softwares* e atendendo ao princípio da reserva legal.

O estudo realizado no presente artigo visou debater as falhas apresentadas pela legislação, bem como explicitar as zonas cinzentas do ordenamento jurídico. Evidenciou os

²³ BRASIL. Supremo Tribunal Federal. **Audiência Pública sobre o uso de ferramentas de monitoramento secreto**. Brasília, 11 de jun. de 2024. 1 vídeo (149 min.) Publicado pelo canal STF. Disponível em: <https://www.youtube.com/watch?v=ufyNUW0BEvY>. Acesso em: 14 mar. 2025.

²⁴ SARLET, Ingo Wolfgang. **Tecnoautoritarismo, democracia e direitos fundamentais**. Brasília, 29 de ago. de 2023. 1 vídeo (66min.). Publicado pelo canal A Ciência da CF88. Disponível em: <https://www.youtube.com/watch?v=O3nkLRtsD58>. Acesso em: 09 de abr. de 2025.

riscos aos direitos e garantias constitucionais e a democracia. Sendo necessário então, expor as necessidades e as expectativas que a nova legislação deverá abranger.

Nesse sentido, é preciso que essa nova regulamentação se atente a alguns requisitos, de forma a resguardar os princípios fundamentais. Alisson Alexandro Possa²⁵, da comissão de direito digital da OAB, expõe alguns desses requisitos que são majoritariamente citados pela doutrina.

A necessidade de autorização judicial devidamente fundamentada, com observância dos princípios da adequação, necessidade e proporcionalidade do uso dessas ferramentas no caso concreto, e não de forma abstrata. Em hipóteses fechadas e restritas dos tipos penais que o uso de *malware* deve ser permitido. Deve-se estabelecer procedimentos com tipos e dispositivos maliciosos permitidos, tipos de dados coletados e reversibilidade de medidas, e outros mecanismos voltados a segurança, visto que os *softwares* podem modificar as barreiras de segurança dos aparelhos.

Ademais, é necessário a determinação de um período em que a utilização do software será permitida, bem como delimitar a renovação desse período. A previsão de formas, a fim de garantir a proteção de conteúdos íntimos ou sensíveis encontradas com o uso da ferramenta que não tenham pertinência a investigação, tendo em vista que a invasão realizada pelo software dará acesso a uma infinidade de informações dentro do sistema, sendo difícil determinar a informação específica que se terá acesso. Deverá ser estipulado também um mecanismo de supervisão e controle, seja por autoridade competente ou por parte do acusado/investigado.

É evidente que outras questões precisam ser enfrentadas, a fim de resguardar todos os direitos dos cidadãos, mas os requisitos supracitados são os essenciais, aqueles que deverão estar presentes numa futura legislação.

Sendo assim, enquanto uma nova Lei não é publicada, para prevenir os abusos, é necessário que o cidadão saiba dos seus direitos e seus limites, devendo redobrar a atenção no mundo cibernético. O governo também deve adotar medidas de prevenção, buscando evitar os abusos e garantindo que sua utilização passe por um controle judicial prévio.

Enquanto não houver um controle mais rígido sobre o tema, o perigo de estar sendo espionado sempre existirá, seja por um órgão estatal, ou por uma entidade privada que tenha realizado a contratação do *software*. Uma simples câmera, ou apenas um aparelho telefônico,

²⁵ BRASIL. Supremo Tribunal Federal. **Audiência Pública sobre o uso de ferramentas de monitoramento secreto**. Brasília, 11 de jun. de 2024. 1 vídeo (149 min.) Publicado pelo canal STF. Disponível em: <https://www.youtube.com/watch?v=ufyNUW0BEvY>. Acesso em: 14 mar. 2025.

podem ser suficientes para extração de informações e descobrir que está sendo observado nunca é uma tarefa fácil.

CONCLUSÃO

É incontroverso, que as inovações tecnológicas trouxeram mudanças no contexto social. Para isso, a sociedade como um todo deve estar preparada para receber tais alterações, sendo dever do Estado garantir a proteção de seus cidadãos.

Nesse sentido, as leis precisam acompanhar essas mudanças para que seja possível garantir a devida proteção, blindando os cidadãos de possíveis ataques. Em contrapartida, com a utilização dos *spywares*, ficou evidenciado que as normas vigentes não garantiam plena proteção a sociedade, fato que gerou desconfiança e incerteza. O Marco Civil da Internet e a Lei Geral de Proteção de Dados que seriam as leis capazes de limitar o uso dos softwares, como demonstrado no presente artigo encontram-se desatualizadas e por isso não conseguiram controlar seu uso indevido.

Como exposto em todo o trabalho, a utilização de ferramentas de monitoramento secreto vem sendo utilizada para auxiliar nas buscas e investigações de potenciais ameaças à segurança pública. Todavia, demonstrou ser um mecanismo extremamente invasivo que garante acesso a um universo de informações e por se tratar de um avanço tecnológico não encontrou barreiras dentro do ordenamento jurídico para que seu uso fosse devidamente delimitado. Foi também utilizado por Estados para monitorar e controlar jornalistas.

Dessa forma, sua utilização foi severamente questionada, visto que apresenta uma afronta aos direitos fundamentais, como o direito à privacidade, intimidade, a inviolabilidade das comunicações, entre outros.

Além disso, a classe jornalística foi claramente afetada com o uso dos *spywares*, tendo sido investigada e espionada nessa incansável busca por informação. A utilização desses softwares para retirar informações confidenciais, afrontam diretamente a própria democracia e não só os profissionais que trabalham com informação, é um ataque direto contra a sociedade.

É bem verdade, que com os avanços da tecnologia está cada vez mais difícil o processo de investigação e o Estado necessita de ferramentas novas que sejam efetivas contra essas mudanças, para que assim exerça corretamente sua função de proteger a sociedade.

O grande questionamento não é somente sobre o uso das ferramentas, pois estas podem se tornar um grande aliado do Estado e o auxiliar na prevenção de ameaças, bem como em agilizar as investigações. O centro do problema está na liberdade que esses softwares possuem,

sendo impossível controlar qual informação será extraída do sistema, tudo será exposto. Por esse motivo, seu uso deve ter um melhor controle judicial que delimite sua utilização, a fim de evitar violação aos direitos fundamentais.

Por fim, a utilização dos *softwares* atualmente, evidencia uma necessidade de evolução legislativa, de modo que uma nova regulamentação específica deve ser idealizada, com intuito de proteger os direitos e garantias constitucionais, bem como impor contrapesos a sua utilização. Enquanto houver zonas cinzentas acerca do tema, o risco de violação aos princípios constitucionais não deixará de existir.

REFERÊNCIAS

BARROSO, Luís Roberto. **O Direito Constitucional e a Efetividade de Suas Normas**. Rio de Janeiro: Renovar, 2009.

BRASIL tem mais smartphones do que habitantes, aponta levantamento. **Veja**, São Paulo, 27 de abr.2023. Disponível em: <https://veja.abril.com.br/tecnologia/brasil-tem-mais-smartphones-do-que-habitantes-aponta-levantamento>. Acesso em: 11 mar. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 mar. 2025.

BRASIL. **Lei nº 12.850/2013, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal. Brasília, DF: Presidente da República, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm. Acesso em: 12 mar. 2025.

BRASIL. **Lei nº 9.883/1999, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN. Brasília, DF: Presidente da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19883.htm. Acesso em: 10 jun. 2025.

BRASIL. **Lei nº 12.965/14, de 23 de abril de 2023**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Presidente da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 11 mar. 2025.

BRASIL. **Lei nº 13.709/18, de 14 de agosto de 2018**. Estabelece a Lei Geral de Proteção de dados pessoais. Brasília, DF: Presidente da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 11 mar. 2025.

BRASIL. **Lei nº 9.296/96, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, DF: Presidente da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19296.htm. Acesso em: 11 mar. 2025.

BRASIL. Superior Tribunal de Justiça (6 Turma). **Recurso em Habeas Corpus 117.462**. Por falta de fundamentação, Sexta Turma invalida quebra de sigilos telefônico, fiscal e bancário. Relator: Rogerio Schietti Cruz, 2 de setembro de 2019. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/28052021-Por-falta-de-fundamentacao--Sexta-Turma-invalida-quebra-de-sigilos-telefonico--fiscal-e-bancario.aspx>. Acesso em: 10 jun. 2025.

BRASIL. Supremo Tribunal Federal (2 Turma). **Habeas Corpus 91.867**. Licitude da prova produzida durante o inquérito policial. Relator: Min. Gilmar Mendes, 20 de setembro de 2012. Disponível em: <https://portal.stf.jus.br/jurisprudencia/>. Acesso em: 14 mar. 2025.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental 1.143**. Utilização de ferramentas de monitoramento secreto. Relator: Min. Cristiano Zanin, 14 de maio de 2021. Disponível em: <https://portal.stf.jus.br/jurisprudencia/>. Acesso em: 14 mar. 2025.

BRASIL. Supremo Tribunal Federal. **Audiência Pública sobre o uso de ferramentas de monitoramento secreto**. Brasília, 11 de jun. de 2024. 1 vídeo (149 min.) Publicado pelo canal STF. Disponível em: <https://www.youtube.com/watch?v=ufyNUW0BEvY>. Acesso em: 14 mar. 2025.

BRASIL. Supremo Tribunal Federal. **Tema 990**. Possibilidade de compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais do contribuinte. Relator: Min. Dias Toffoli, 28 de novembro de 2019. Disponível em: <https://portal.stf.jus.br/jurisprudenciarepercussao/veramentoprocesso.asp?incidente=5213056&numeroprocesso=1055941&classeprocesso=re&numerotema=990>. Acesso em: 09 de abr. 2025.

FUX, Luiz. Supremo Tribunal Federal. **Restrições à imprensa tornam a democracia uma mentira e a Constituição uma mera folha de papel**. Disponível em: <https://noticias.stf.jus.br/postsnoticias/restricoes-a-imprensa-tornam-a-democracia-uma-mentira-e-a-constituicao-uma-mera-folha-de-papel-afirma-presidente-do-stf/>. Acesso em: 10 jun. 2025.

MORAES, Alexandre de. **Direito Constitucional**. 38. ed. São Paulo: Atlas, 2022.

SARLET, Ingo Wolfgang. **Tecnoautoritarismo, democracia e direitos fundamentais**. Brasília, 29 de ago. de 2023. 1 vídeo (66min.). Publicado pelo canal A Ciência da CF88. Disponível em: <https://www.youtube.com/watch?v=O3nkLRtsD58>. Acesso em: 09 de abr. de 2025.

SILVA, José Afonso. **Curso de Direito Constitucional Positivo**. 45. ed. Salvador: JusPodivm, 2024.

STARTI. **Spyware: sorria, você está sendo espionado**. Starti, 2021. Disponível em: <https://blog.starti.com.br/spyware/>. Acesso em: 10 jun. 2025.

YOUTUBE. **O que é spyware?** Descubra como se proteger. Brasília, 26 de out. de 2021. 1 vídeo (4 min) Publicado pelo canal Starti. Disponível em: https://www.youtube.com/watch?v=vJWn_xvOSNs&t=68s. Acesso em: 10 jun. 2025.