LAMPIÃO
revista acadêmica

USO DA CRIPTOGRAFIA EM APLICATIVOS DE MENSAGEM: UMA ANÁLISE DA FALSA DICOTOMIA ENTRE PRIVACIDADE E SEGURANÇA PÚBLICA

[Artigo Científico]

Maria Leal Teixeira Neta
Flávio Augusto de Freitas Câmara Neto
Mariana de Siqueira

Submissão: 09/10/2024
Aprovação: 30/11/2024

SOBRE O AUTOR/A/OS/AS:

- **Maria Leal Teixeira Neta**

Graduanda de Direito pela Universidade Federal do Rio Grande do Norte **(UFRN)**. Estagiária da Defensoria Pública do Rio Grande do Norte e monitora da disciplina de Direito Processual Penal.

- **Flávio Augusto de Freitas Câmara Neto**

Graduando de Direito pela Universidade Federal do Rio Grande do Norte **(UFRN)**. Estagiário da Defensoria Pública do Rio Grande do Norte e monitor da disciplina de Direito Digital.

- **Mariana de Siqueira**

Doutora em Direito pela Universidade Federal do Pernambuco **(UFPE)**. Advogada e **professora** da Universidade Federal do Rio Grande do Norte **(UFRN)**.

USO DA CRIPTOGRAFIA EM APLICATIVOS DE MENSAGEM: UMA ANÁLISE DA FALSA DICOTOMIA ENTRE PRIVACIDADE E SEGURANÇA PÚBLICA

USE OF CRYPTOGRAPHY IN MESSAGING APPS: AN ANALYSIS OF THE FALSE DICHOTOMY BETWEEN PRIVACY AND PUBLIC SECURITY

Maria Leal Teixeira Neta,
Flávio Augusto de Freitas Câmara Neto,
Mariana de Siqueira

RESUMO

Este artigo debate a narrativa existente que opõe os direitos à privacidade e à segurança pública em relação ao uso da criptografia nos aplicativos de mensagens. Persiste, atualmente, uma linha de pensamento que encara a técnica criptográfica como empecilho à investigação criminal. A partir de pesquisa bibliográfica de natureza qualitativa sobre estudos acerca da criptografia, segurança de dados, investigação criminal e decisões proferidas no âmbito do Supremo Tribunal Federal, o presente trabalho argumenta que a referida contraposição é equivocada, por três razões. Primeiro, porque a utilização da criptografia permite o exercício seguro da privacidade no ciberespaço. Segundo, porque a criação de acessos excepcionais a mensagens criptografadas incrementa o risco de acesso de dados por terceiros não autorizados. Terceiro, porque é verificável que a criptografia e a segurança pública são categorias que se complementam. O artigo, portanto, defende que não há uma dicotomia entre privacidade e segurança com o uso da criptografia nos aplicativos de mensagens, mas uma relação necessária na era das tecnologias digitais.

Palavras-chave: ciberespaço; segurança de dados; era das tecnologias digitais.

ABSTRACT

This article debates the existing narrative that opposes the rights to privacy and public security in relation to the use of cryptography in messaging apps. Based on studies on cryptography, data security, criminal investigation, and rulings issued by the Supreme Federal Court, this paper argues that this opposition is misguided for three reasons. First, because the use of cryptography allows for the secure

exercise of privacy in cyberspace. Second, because the creation of exceptional access to encrypted messages increases the risk of unauthorized third-party data access. Third, because it is verifiable that cryptography and public security are complementary categories. Therefore, the article argues that there is no dichotomy between privacy and security with the use of cryptography in messaging apps, but rather a necessary relationship in the era of digital technologies.

Keywords: cyberspace; data security; era of digital technologies.

1. INTRODUÇÃO

A ideia de que a segurança pública e a privacidade são valores incompatíveis ou que estão em constante conflito não é nova, porém, com o avanço das tecnologias digitais, essa questão adquiriu uma nova fase. O avanço tecnológico vem constantemente transformando a forma como nos comunicamos e interagimos, trazendo à tona debates cruciais sobre privacidade e investigações criminais. Em particular, a utilização da criptografia nas comunicações digitais.

Por um lado, a criptografia é defendida como um meio essencial para garantir o exercício de direitos fundamentais, como o direito à privacidade. Por outro lado, autoridades governamentais e órgãos de segurança pública frequentemente apontam para a necessidade de acessar comunicações criptografadas, pautando-se na prevenção e no combate ao crime. Surge, então, o problema central deste estudo: é possível conciliar a proteção à privacidade garantida pela criptografia com as demandas de segurança pública?

A relevância deste tema se evidencia pela crescente dependência da criptografia em plataformas de comunicação digital, como o WhatsApp, e pelo impacto que decisões judiciais, como as proferidas no Brasil na Aguição de Descumprimeto de Preceito Fundamental (ADPF) 403 e na Ação Direta de Inconstitucionalidade (ADI) 5527, têm no equilíbrio entre a privacidade dos indivíduos e a necessidade de acesso a dados para fins de investigação. No caso da ADPF 403, o Supremo Tribunal Federal (STF) debateu a legalidade da suspensão do WhatsApp por descumprimento de ordens judiciais, ao passo que a ADI 5527 tratou da proteção constitucional das comunicações digitais no âmbito do Marco Civil da Internet.

O objetivo geral deste artigo é analisar de que forma a criptografia, enquanto instrumento de proteção à privacidade - exercício de um direito fundamental - pode coexistir e, inclusive, auxiliar com as demandas de segurança pública.

Este artigo tem como abordagem a pesquisa bibliográfica de natureza qualitativa de estudos sobre criptografia, privacidade e decisões proferidas no âmbito do Supremo Tribunal Federal. Na primeira parte, objetiva-se mapear a ligação da criptografia com o direito à privacidade. Na segunda parte, tratamos de situar

o uso da criptografia no que tange às investigações criminais. Na terceira parte, que antecede a conclusão, pretende-se refutar a visão de que a privacidade e a segurança estão em lados opostos, destacando a relevância da criptografia no exercício dos direitos fundamentais no ambiente digital e sua importância para com a segurança pública.

2. INTERFACE ENTRE CRIPTOGRAFIA E PRIVACIDADE

O constante desenvolvimento das tecnologias digitais, assim como a crescente dependência do ambiente digital para realização de atividades pessoais e profissionais, ressalta, cada vez mais, a importância da cibersegurança. Os mecanismos de cibersegurança, além de garantir a confidencialidade dos dados enquanto eles trafegam na Internet, também são essenciais para assegurar a confidencialidade dos dados armazenados nos computadores e em outros dispositivos (Liguori, 2022). É justamente nessa necessidade de dar segurança e proteção aos inúmeros usuários do ambiente digital que se destaca o uso da criptografia.

A criptografia, em conceitos técnicos, consiste na aplicação de algoritmos criptográficos, chamados de cifras, que são capazes de modificar uma mensagem inteligível em uma mensagem cifrada. Essa transformação ocorre por meio da utilização de uma informação secreta, ou melhor dizendo, uma chave criptográfica.

Outro conceito que ajuda na compreensão é que a criptografia é o campo de pesquisa voltado:

> ao estudo, projeto e implementação de técnicas para comunicação segura entre múltiplas partes na presença de atacantes ou adversários. Estes últimos, cujo principal objetivo consiste em impedir que as partes se comuniquem de maneira segura, representam entidades no mundo real como fraudadores, empresas intrusivas e até governos autoritários, capazes de empregar uma variedade de recursos e abordagens para alcançar sua finalidade (Aranha, 2018, p. 27).

É justamente por essa função primordial, que as técnicas criptográficas têm sido amplamente adotadas por uma variedade de autores, com o principal objetivo de assegurar a proteção da comunicação e das informações no âmbito pessoal, comercial e no setor público. Ressalta-se, ainda, que, como bem colocado no relatório da UNESCO, “a encriptação que protege a comunicação entre usuários e serviços de Internet oferece melhorias significativas à privacidade e segurança do usuário perante terceiros maliciosos” (Schulz, de Hert, 2016, p. 18).

Dada essa breve explanação sobre os conceitos da criptografia, iremos abordar agora, especificamente, a criptografia de ponta a ponta, que é o foco de estudo deste trabalho. A criptografia de ponta a ponta, também chamada de “ponto a ponto” ou “fim a fim”, é um método empregado para assegurar a pro-

teção das informações em plataformas de comunicação, como os aplicativos de mensagens instantâneas.

A criptografia de ponta a ponta funciona, em termos práticos, ao criptografar a mensagem no dispositivo do remetente usando a chave pública do destinatário. Somente o destinatário, com sua chave privada, é capaz de descriptografá-la. Assim, mesmo que a mensagem passe por um servidor central que a encaminha para o destinatário, esse servidor não consegue acessar seu conteúdo, pois não possui a chave necessária para descriptografá-la (Liguori, 2022).

É esta criptografia de ponta a ponta, a qual assegura que, mesmo que a mensagem passe por um terceiro ou gerenciador, ela só é decifrada no receptor, ao passo que os próprios gerenciadores da troca de mensagens não possuem acesso às chaves para decifrá-las (Teixeira, 2022).

Superada essa abordagem inicial, entramos no principal tema deste tópico: a contribuição da criptografia para viabilização de direitos fundamentais no ambiente digital. É nesse contexto que a criptografia é frequentemente vinculada ao direito à privacidade. Contudo, ela também desempenha um papel essencial na garantia dos direitos à liberdade de expressão e associação no ambiente online.

Nesse sentido, é que a importância da criptografia para garantir o direito à privacidade e outros direitos fundamentais no ambiente digital já foi reconhecida, inclusive, em diversos documentos e relatórios emitidos por organizações de destaque internacional, como a UNESCO (Schulz, de Hert, 2016, p. 73):

> A proteção da encriptação em instrumentos relevantes de direito e de política, sob a ótica dos direitos humanos, é especialmente importante, visto que a encriptação torna possível proteger informações e comunicações na plataforma de comunicações inseguras que seria a Internet. Inicialmente, a própria Internet não foi projetada para fornecer a segurança das informações e comunicações em geral. Ao longo dos anos, as técnicas criptográficas tornaram-se um componente central da Internet, amparadas por numerosos protocolos e padrões que apoiam a sua implementação na prática. A encriptação torna possível ajudar a garantir confidencialidade, privacidade, autenticidade, disponibilidade, integridade e anonimato em configurações específicas. Isso facilita a proteção dos direitos humanos dos usuários da Internet e a liberdade de expressão e privacidade em particular.

Ao tentar traçar a relação entre o exercício do direito à privacidade e o uso da criptografia, a interseção aparenta ser clara: ao passo que se obstaculiza o acesso não autorizado a informações, documentos e comunicações pessoais, o sistema de criptografia tornaria possível a preservação da privacidade do indivíduo no contexto digital.

Na Constituição Federal do Brasil, o direito à privacidade é previsto no art. 5º, X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente

de sua violação" (Brasil, [2024], 5º, X). Nesse contexto, depreende-se que é uma garantia fundamental que protege o indivíduo contra intromissões indevidas em sua esfera íntima, abrangendo aspectos da intimidade, da vida privada, da honra e da imagem. Ou seja, trata-se de uma proteção essencial à dignidade humana, capaz de promover um ambiente onde as pessoas possam desenvolver suas personalidades.

O que antes dizia respeito ao direito de estar só (*the right to be let alone*), passa a ser um poder de controlar a própria vida, a qual na economia dos dados é a concretização do direito à privacidade (Véliz, 2021). É seguindo por essa linha de pensamento que elegemos a teoria de que a privacidade consiste em um direito de controle sobre informações pessoais (Liguori, 2022).

Neste contexto, o direito à privacidade não é visto apenas como um modo de impedir que terceiros interfiram em questões pessoais. Em vez disso, é compreendida como o poder do indivíduo de decidir como, quando e em quais condições as informações a seu respeito serão tornadas públicas.

Westin (1968) entende que a privacidade refere-se ao desejo de indivíduos, grupos ou instituições de controlarem quando, de que forma e em que medida suas informações serão compartilhadas com terceiros.

É nesse cenário que se destaca a importância da criptografia para o direito à privacidade. Conceder ao indivíduo a capacidade de proteger suas informações e comunicações de terceiros é uma maneira de garantir-lhe controle sobre esses dados, ainda que esse controle se restrinja ao acesso às informações. A encriptação proporciona a possibilidade de que as pessoas protejam a integridade, disponibilidade e confidencialidade de suas comunicações.

Diante do exposto, não poderíamos nos eximir de abordar a tão debatida criptografia de ponta a ponta utilizada por aplicativos de mensageria, em especial o WhatsApp.

Em linhas gerais, a criptografia de ponta a ponta implementada pelo WhatsApp garante que apenas o usuário tenha acesso ao conteúdo das mensagens e dos dados transmitidos pelo aplicativo. Para cada mensagem enviada, é gerada uma nova chave de segurança, o que significa que, mesmo que uma chave seja decifrada, apenas aquela mensagem específica seria exposta, não a conversa completa. Com esse sistema, o WhatsApp não tem a capacidade de interceptar ou ler as conversas ou arquivos trocados na plataforma, uma vez que não possui acesso às chaves privadas dos usuários.

Ou seja, o papel da criptografia seria, aqui, proteger essa comunicação de seu acesso por terceiros e evitar sua divulgação não autorizada por confidentes, promovendo, assim, aspectos fundamentais da vida humana como a proteção à confidencialidade, à autenticidade e à privacidade das mensagens transmitidas.

Portanto, se o sigilo garantido pela criptografia das mensagens não fosse mantido, haveria maior risco de chantagens econômicas, psicológicas ou físicas decorrentes do acesso indevido a informações privadas. Além disso, governos autoritários teriam mais facilidade em monitorar as comunicações, o que permitiria a censura de conteúdos e a repressão de discursos contrários ao regime, enfraquecendo o debate democrático e silenciando vozes dissidentes (Costa, 2021).

Diante de tudo que foi abordado até agora, compreende-se, conforme trecho notável do Ministro Edson Fachin no julgado da ADPF 403, que "a criptografia forte é, de acordo com as principais evidências científicas o mecanismo por excelência de garantia do relevantíssimo direito à privacidade" (Brasil, 2020, p. 75).

3. CRIPTOGRAFIA, INVESTIGAÇÕES CRIMINAIS E BACKDOORS

Compreendida a importância da criptografia para viabilização do direito fundamental à privacidade, faz-se necessário, ainda, analisar outro controverso debate em relação aos impactos da disseminação de sistemas criptográficos para atividades de investigação no país.

A discussão sobre acesso a dados criptografados para fins de instrução criminal, não é nova nem fácil de ser sintetizada. São recorrentes os discursos que ressaltam os desafios enfrentados pelas autoridades de investigação diante da disseminação da criptografia forte. Esses discursos, muitas vezes, apresentam conteúdo similar e com título idêntico: *Going Dark*. Essa expressão é usada para resumir os entraves que a impossibilidade de acessar conteúdos criptografados impõem às autoridades, deixando-as "no escuro" e sem acesso a informações que poderiam ser relevantes para suas investigações (Liguori, 2022).

A grande preocupação argumentada pelas autoridades, que inclusive foi abordada no I Simpósio *Going Dark* Brasil, em 2019, consiste no uso dos diversos sistemas de criptografia forte como medida antiforense. O principal objetivo dessas medidas seria a destruição, a ocultação ou a manipulação da fonte de prova, de modo a inviabilizar o acesso ao seu conteúdo, frustrando, assim, sua utilidade na análise forense.

Ou seja, a criptografia de dados em trânsito, na modalidade ponta a ponta, estaria criando obstáculos para as autoridades que realizam interceptações telemáticas. Até mesmo quando uma comunicação fosse interceptada com sucesso, a criptografia garantiria que seu conteúdo permanecesse inacessível/ilegível a terceiros estranhos.

É nesse exato ponto dos "obstáculos à investigação", que frequentemente são levantadas narrativas contra a "criptografia forte" com a consequente implantação de *backdoors* para as autoridades de investigação. Esse termo, pejora-

tivamente chamado de *backdoors*, remete ao "método de superar ou desviar das formas de autenticação ou outros protocolos de controle de segurança com o objetivo de acessar um sistema computacional ou os dados nele contidos" (Costa, 2021, p. 22).

No Brasil, tivemos casos emblemáticos que impulsionaram as narrativas dos *backdoors* para aqueles aplicativos de mensageria que utilizam a criptografia de ponta a ponta. Nos anos de 2015 e 2016, o WhatsApp, mediante ordens judiciais, foi bloqueado por três vezes no país, sob alegação de descumprimento de determinações judiciais.

A sanção foi imposta devido à incapacidade do provedor de disponibilizar o conteúdo das comunicações em sua plataforma, uma vez que, com a utilização da criptografia de ponta a ponta, apenas o remetente e o destinatário têm acesso às mensagens trocadas. No entanto, as ordens judiciais interpretaram essa impossibilidade como uma recusa.

Nesse contexto, o que se percebe é que esses acontecimentos fizeram emergir, ainda mais, as narrativas "privacidade versus segurança", culminando no fortalecimento de discursos "anti-criptografia". Esses argumentos são, muitas vezes, sustentados por cenários de crise na segurança pública, que projetam uma visão distópica sobre o impacto da criptografia no combate ao crime (Costa, 2021).

Ademais, não é raro que as propostas para flexibilizar o uso da criptografia sejam apresentadas sem a devida fundamentação em dados que comprovem que a ausência dessa tecnologia impediria, de fato, a realização de atividades ilícitas. As iniciativas das agências de investigação carecem de provas concretas que demonstrem que a criptografia é o principal obstáculo para a resolução de ataques e a captura de criminosos. Pelo contrário, há sinais de que o enfraquecimento da criptografia estaria longe de ser uma solução eficaz, revelando-se uma medida ineficiente tanto na prevenção quanto na investigação criminal (Costa, 2021).

Nesse mesmo sentido, defende Liguori, de forma cirúrgica, que "há pouquíssimos dados, relatórios ou qualquer outro tipo de informação que possa ajudar a entender quão profundamente a questão da criptografia impacta a investigação e a resolução de crimes na prática" (Liguori, 2022, p. 32). Acrescenta, ainda, que na pesquisa para sua obra, não foi sequer capaz de encontrar dados empíricos sobre o impacto da criptografia para autoridades de investigação criminal fora dos Estados Unidos da América.

Na verdade, o que se percebe é que sistemas de segurança avançados, equipados com criptografia forte, são essenciais para a realização das investigações. Ou seja, asseguram tanto a confidencialidade das comunicações entre os

agentes quanto a proteção e a integridade de documentos, provas e outras informações cruciais para o processo penal (Liguori, 2022).

4. DESFAZENDO A COLISÃO "PRIVACIDADE X SEGURANÇA" NO USO DA CRIPTOGRAFIA

Para entender a profundidade do debate em torno da criptografia, é essencial desconstruir a simplista oposição entre "privacidade versus segurança" e a ideia de que segurança pública e privacidade estariam em rota de colisão.

Retomando as ideias anteriores, tem-se que a criptografia desempenha um papel fundamental na proteção dos direitos à privacidade, liberdade de expressão e segurança das comunicações no ambiente digital. Ela assegura que indivíduos possam se comunicar e realizar transações de maneira segura, impedindo o acesso indevido a suas informações pessoais. Ao mesmo tempo, argumenta-se que a criptografia pode criar obstáculos às investigações criminais, uma vez que dados criptografados podem se tornar inacessíveis para autoridades de investigação, mesmo com ordens judiciais.

Entretanto, essa percepção de que a vida privada e defesa social estão em constante colisão não é necessariamente verdadeira. Na prática, a criptografia não apenas protege a privacidade individual, mas também fortalece a segurança pública. Assegurar a privacidade por meio da proteção da infraestrutura de dados equivale a promover a segurança pública, já que sistemas seguros previnem a realização de vários crimes no ambiente digital, como invasão de dispositivos, furto de informações financeiras, entre outros.

Ademais, na seara da investigação, a integridade dos sistemas é crucial para o desempenho de suas funções, como a comunicação segura entre agentes e a preservação de dados essenciais para os processos investigativos.

A implementação de sistemas criptográficos robustos é essencial para proteger informações confidenciais, incluindo as utilizadas por governos e instituições públicas para prevenir ataques cibernéticos e proteger infraestruturas críticas. Quando tratamos da segurança no sentido mais amplo, incluindo a cibersegurança, a criptografia aparece como um aliado, e não como um inimigo.

Nesse sentido, vale destacar que Daniel Solove dedicou um livro exclusivamente para tentar desconstruir essa abordagem combativa. Destacamos, a esse respeito, um trecho que sintetiza bem sua análise (Solove, 2011, p. 34):

> O argumento de que a privacidade e a segurança se excluem mutuamente deriva daquilo a que chamo a "falácia do tudo ou nada". Sacrificar a privacidade não nos torna automaticamente mais seguros. Nem todas as medidas de segurança são invasivas da privacidade. Além disso, não foi estabelecida nenhuma correlação entre a eficácia de uma medida de

> segurança e uma correspondente diminuição da liberdade. Por outras palavras, as medidas de segurança mais eficazes não têm de ser as mais prejudiciais para a liberdade. (Tradução nossa).

Além disso, propostas que sugerem a inserção de *backdoors* nos sistemas criptográficos, sob a justificativa de facilitar o acesso para investigações, representam um risco significativo tanto para a privacidade quanto para a segurança.

Ao contrário do que se argumenta, criar portas de acesso para autoridades pode, na verdade, comprometer toda a integridade do sistema, prejudicando não só indivíduos, mas também a própria segurança pública que se busca proteger. Isso foi, inclusive, mencionado pelo ilustre Ministro Edson Fachin em seu voto na ADPF 403, ao argumentar que não seria possível o estabelecimento de *backdoors* apenas para as autoridades ou para as "pessoas boas". Ou seja, criar uma vulnerabilidade nos dispositivos de todos os usuários não apenas permite o acesso por parte das autoridades para os fins considerados "legítimos", mas também expõe esses sistemas ao risco de exploração por terceiros com intenções maliciosas (Real, 2020).

Cabe ressaltar que a Ministra Rosa Weber, em seu voto na mencionada ADI 5527, sublinha, exatamente, o perigo de se adotar uma visão simplista na relação entre segurança pública e privacidade. Para ela, a proteção da privacidade não se limita a um direito individual, mas está diretamente conectada à própria segurança coletiva, especialmente em um cenário de crescente dependência das redes digitais. Ao permitir que autoridades de segurança tenham maior facilidade no acesso a dados privados sob a justificativa de combate às ameaças imediatas, expõe-se a sociedade a riscos mais profundos no longo prazo, como ciberataques e fraudes, enfraquecendo a segurança das redes e dos usuários como um todo.

Ademais, a Ministra alerta que a mesma tecnologia que facilitaria o acesso de autoridades a informações privadas, também poderia ser usada por criminosos para explorar e violar a privacidade de cidadãos. A flexibilização dos mecanismos de proteção pode abrir uma perigosa porta, onde o equilíbrio entre privacidade e segurança é prejudicado, potencialmente resultando em danos futuros mais graves, como o aumento de fraudes, invasão de intimidade e extorsão. Assim, a Ministra destaca a importância de garantir que a defesa da segurança não venha às custas da privacidade, mas sim que ambas sejam tratadas de forma equilibrada e interdependente.

Nesse sentido, a solução não reside em um enfraquecimento da criptografia, mas no fortalecimento de capacidades investigativas que possam operar dentro de um ambiente tecnológico cada vez mais avançado. Buscando, assim, melhorar a eficácia das investigações sem comprometer a privacidade de milhões de usuários.

Portanto, o debate não deve ser sobre a necessidade do sacrifício de um - privacidade - em prol do outro - segurança - (Liguori, 2022), sobre qual direito deve prevalecer, mas sobre como os dois podem coexistir. Haja vista que a criptografia, quando usada corretamente, fortalece ambos.

A criptografia, portanto, transcende a proteção individual de dados, sendo uma peça-chave para a estabilidade e segurança da infraestrutura digital que sustenta tanto o setor privado quanto o público. Ela garante que comunicações, transações e informações sensíveis possam ser mantidas a salvo de acessos indevidos, resguardando tanto os direitos dos cidadãos quanto a integridade de instituições. Ao assegurar a inviolabilidade dos dados, a criptografia se torna um elemento crucial para mitigar riscos como ataques cibernéticos e vazamentos de informações, contribuindo para o funcionamento confiável e seguro da sociedade digital moderna.

A solução para essa aparente contradição está em reconhecer que privacidade e segurança não precisam estar em conflito, mas sim caminhar lado a lado. Em vez de tratar esses valores como mutuamente excludentes, é possível desenvolver abordagens e políticas que garantam ambos. O respeito aos direitos fundamentais, aliado ao uso de tecnologias que protejam a privacidade, permite a criação de ambientes seguros sem abrir mão das liberdades individuais. Inovação tecnológica e proteção de dados podem coexistir, gerando um equilíbrio que atenda às demandas de segurança pública sem comprometer os direitos essenciais dos cidadãos.

5. CONSIDERAÇÕES FINAIS

Na era das tecnologias digitais, os riscos inerentes ao ambiente virtual ensejam a criação e fortalecimento de técnicas aptas a tornar o ciberespaço seguro. O uso de chaves criptográficas consiste em uma dessas, como se logrou demonstrar. A criptografia de ponta a ponta, especialmente, é utilizada nos aplicativos de mensagens instantâneas, a exemplo do WhatsApp. Seu funcionamento rende, nos dias de hoje, sérios questionamentos por parte dos órgãos de segurança pública, o que leva ao debate público a ideia de colisão entre dois direitos fundamentais – privacidade e segurança pública.

Todavia, os estudos na área da segurança de dados são unânimes em considerar que o uso da criptografia permite, na verdade, o exercício seguro de direitos fundamentais, sobretudo, a privacidade. As garantias da confidencialidade, integridade e resiliência dos sistemas de informação são tratadas como instrumentos próprios da segurança.

A permissão para acessos excepcionais para desencriptação – *backdoors* –

não seria um caminho exclusivo aos agentes da segurança pública. Abrir espaço para vulnerabilidades no sistema, na prática, seria uma oportunidade para a delinquência cibernética operar em larga escala. A criptografia, nesse sentido, atua para proteção de todos, incluindo os agentes que atuam na investigação criminal.

Por esses motivos, privacidade e segurança pública não constituem uma dicotomia no que se refere ao uso da criptografia nos aplicativos de mensagens, mas uma relação necessária para a manutenção da segurança no ciberespaço. A título de sugestão para trabalhos futuros, tem-se como proeminente uma investigação que visualize o direito à privacidade com um cariz coletivo na economia dos dados. Reconhecendo o limite deste estudo, percebe-se que inovações tecnológicas, a exemplo da criptografia de ponta a ponta, merecem um estudo aprofundado e com destaque para com as mudanças de perspectivas – individualidade versus coletividade – dos direitos fundamentais.

REFERÊNCIAS

ALIMONTI, Veridiana. Criptografia, direitos e a problemática da polarização entre "privacidade individual" e "segurança coletiva". *In*: DONEDA, Danilo; MACHADO, Diego. **A criptografia no direito brasileiro**. Revista dos Tribunais, 2018. p. 64-65.

ARANHA, Diego F. **O que é criptografia fim a fim e o que devemos fazer a respeito?** Revista dos Tribunais – Caderno Especial, v. 998, p. 27, 2018.

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: 8 dez. 2024.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceitos Fundamentais (ADPF) nº 403.** Reqte.(s): Cidadania. Intdo. (a/s): Juiz de Direito da Vara Criminal da Comarca de Lagarto. Min. Rel. Edson Fachin, julgamento, 28 de maio de 2020. Disponível em https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf. Acesso em: 28 de set. 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 5527.** Reqte.(s): Partido da República - PR. Intdo. (a/s): Presidente da República. Min. Rel. Rosa Weber, julgamento 27 de maio de 2020. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=560715474. Acesso em 29 de set. de 2024.

COSTA, André Barbosa Ramiro. **Políticas de encriptação**: entre a codificação de direitos, regulação pública e o cipher-ativismo. 2021. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Pernambuco, Recife, 2021.

LIGUORI, Carlos. **Direito e Criptografia:** direitos fundamentais, segurança da

informação e os limites da regulação jurídica na tecnologia. São Paulo: Saraiva-Jur, 2022.

LONGHI, João Victor; FALEIROS JÚNIOR, José Luiz; BORGES, Gabriel; REIS, Guilherme. **Fundamentos do direito digital.** Uberlândia: LAECC, 2020.

REAL, Paula. **Fantasmas infiltrados**: preocupantes tentativas de burlar a criptografia e monitorar as comunicações. Instituto de Pesquisa em Direito e Tecnologia do Recife, 5 ago. 2020. Disponível em: https://ip.rec.br/blog/fantasmas-infiltrados-preocupantes-tentativas-de-burlar-a-criptografia-e-monitorar-as-comunicacoes/. Acesso em: 5 out. 2024.

SCHULZ, Wolfgang; van HOBOKEN, Joris. **Human Rights and Encryption**. UNESCO Series on Internet Freedom, 2016.

SOLOVE, Daniel J., **Nothing to Hide: The False Tradeoff Between Privacy and Security**. Yale University Press (2011).

VÉLIZ, Carissa. **Privacidade é poder**: por que e como você deveria retomar o controle de seus dados. Tradução Samuel Oliveira; Ricardo Campos. 1. ed. São Paulo: Editora Contracorrente, 2021.

WESTIN, Alan. **Privacy and Freedom.** New York, 1968.