Criptografia *by default* na tutela de direitos humanos e condicionantes ao *hacking* governamental

Encryption by default in the protection of human rights and constraints on government hacking

Paulo Rodrigo de Miranda[1]

RESUMO

O presente artigo busca apresentar ponderações a respeito da criptografia *by default* e sua importância para a tutela dos direitos humanos, bem como a necessidade do estabelecimento de condicionantes para se evitar o tecnoautoritarismo na implementação de *hacking* governamental. O trabalho será realizado através de uma abordagem dedutiva com emprego de procedimento bibliográfico. Para alcançar essa finalidade será analisada a importância da criptografia na promoção de direitos humanos. Em seguida, serão abordados a reação das autoridades de investigação com o emprego de *hacking* governamental e os riscos do tecnoautoritarismo. Ao final, são examinadas condicionantes para se evitar o tecnoautoritarismo na implementação de *hacking* governamental. Das conclusões deste trabalho, destaca-se a importância crucial da criptografia na proteção da segurança, privacidade e liberdade de expressão dos usuários de sistemas de comunicação informatizados, bem como a necessidade de promoção um debate público e transparente sobre a imposição de condicionantes à implementação de ações de *hacking* pelo governo brasileiro. Isso inclui a urgente necessidade de promulgar uma legislação específica para regular esse assunto. No sistema republicano, no qual os gestores públicos devem agir com transparência e ser responsabilizados por suas condutas ilícitas, inclusive quando praticado com excesso de poder, a falta de legitimidade popular para orientar o uso de tecnologias invasivas como ferramentas de investigação representa um risco à própria estrutura do Estado Democrático de Direito.

Palavras-chave: criptografia; direitos humanos; *hacking* governamental; tecnoautoritarismo.

ABSTRACT

[1] Mestre em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria (PPGD/UFSM). E-mail: pauulorodrigo@hotmail.com.

This article seeks to present considerations regarding encryption by default and its importance for the protection of human rights, as well as the need to establish conditions to avoid techno-authoritarianism in the implementation of government hacking. The work will be carried out through a deductive approach using a bibliographic procedure. To this end, the importance of cryptography in promoting human rights will be analyzed. Next, the reaction of investigative authorities to the use of government hacking and the risks of techno-authoritarianism will be addressed. Finally, we examine the conditions for avoiding techno-authoritarianism in the implementation of government hacking. The conclusions of this work highlight the crucial importance of cryptography in protecting the security, privacy and freedom of expression of users of computerized communication systems, as well as the need to promote a public and transparent debate on the imposition of conditions on the implementation of hacking actions by the Brazilian government. This includes the urgent need to enact specific legislation to regulate this issue. In a republican system, in which public managers must act transparently and be held accountable for their unlawful conduct, including when practiced with excess power, the lack of popular legitimacy to guide the use of invasive technologies as investigative tools represents a risk to the very structure of the Democratic Rule of Law.

Keywords: *cryptography; human rights; government hacking; techno-authoritarianism.*

1 INTRODUÇÃO

Após as revelações de Edward Snowden, que expuseram as inúmeras técnicas de coleta e análise em grande escala de dados desenvolvidas pelo governo dos Estados Unidos, desencadeou-se uma demanda por soluções que pudessem garantir a segurança e a privacidade dos usuários da rede.

Uma das soluções foi apresentada pelo próprio mercado, com a introdução generalizada da criptografia ponta a ponta em plataformas de comunicação populares, como o iPhone da Apple e o WhatsApp do Facebook. A criptografia representa uma importante salvaguarda do sistema de comunicação, protegendo a privacidade e a liberdade de expressão de todos os usuários.

Como reação à implementação de métodos de acesso excepcionais em sistemas criptografados, surgiu um debate global sobre o uso de técnicas de *hacking*[2] por parte dos governos, com o propósito de obter informações de indivíduos sob investigação, sem comprometer a segurança dos usuários das plataformas digitais de comunicação.

Para o desenvolvimento deste trabalho foi empregado uma abordagem dedutiva. Para tanto, houve a utilização de referências bibliográficas, consulta a estudo realizado pelo Parlamento Europeu e análise da manifestação da Comissão Interamericana de Direitos Humanos (CIDH) no caso *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CCAJAR) vs. Colômbia*.

O objetivo é encontrar argumentos que possam pavimentar um caminho mais equilibrado entre o uso da criptografia e os métodos de investigação baseados em *hacking*, atendendo, ao mesmo tempo, às necessidades essenciais para preservar e proteger a privacidade e a liberdade de expressão de todos os usuários de sistemas informatizados. Para alcançar esse equilíbrio, será dada ênfase à discussão sobre a importância da criptografia *by default* e a necessidade do estabelecimento de condicionantes para se evitar o tecnoautoritarismo na implementação de *hacking* governamental.

O presente trabalho divide-se em três partes. Em um primeiro momento, aborda-se a importância da criptografia na promoção de direitos humanos. Em seguida, propõe-se a análise da reação das autoridades de investigação com o emprego de *hacking* governamental e os riscos do tecnoautoritarismo. Por fim, busca-se estabelecer condicionantes para se evitar o tecnoautoritarismo na implementação de *hacking* governamental.

2 A EXPANSÃO DA CRIPTOGRAFIA *BY DEFAULT* E SUA IMPORTÂNCIA NA PROMOÇÃO DE DIREITOS HUMANOS

[2] Apesar de as autoridades evitarem o termo "hacking", essencialmente, esse mecanismo envolve a aplicação de técnicas semelhantes às utilizadas por hackers, explorando vulnerabilidades técnicas ou humanas dentro de sistemas de tecnologia da informação (GUTHEIL, *et al.*, 2017).

A expansão da criptografia a nível internacional ocorreu apenas na década de 90, quando o setor privado norte-americano começou a desenvolver softwares para uso comercial que empregavam a criptografia (PFEFFERKORN, 2018). Nesse mesmo período o debate político sobre criptografia ganhou dimensão internacional em razão das dimensões do comércio e da globalização impulsionados pelas inovações das redes de comunicação e Internet (SCHULZ; HOBOKEN, 2016).

Apesar de a criptografia ter se tornado acessível comercialmente e ser amplamente empregada para garantir a segurança da Internet, transações online, e atividades bancárias, ela não era comumente adotada pelas pessoas comuns que navegavam na internet, trocavam mensagens ou utilizavam seus laptops e dispositivos móveis (PFEFFERKORN, 2018). Tal quadro mudou drasticamente após as revelações do ex-analista da CIA (Agência Central de Inteligência norte-americana) e da NSA, Edward Snowden, ao expor um panorama de vigilância em massa que era orquestrada pelos órgãos de segurança e inteligência do EUA.

A resposta do mercado diante das revelações de vigilância em massa conduziu que grandes empresas de tecnologia começassem a empregar privacidade em sistemas operacionais e de comunicação desde seu *design* (LIGUORI FILHO, 2018). Como resultado, elas implementaram avanços nos sistemas de criptografia forte como padrão de segurança em seus serviços (criptografia *by default)*[3]. Uma das vantagens dessa criptografia por padrão está na facilidade em garantir ao usuário uma proteção sem exigir qualquer ação para sua ativação (LIGUORI FILHO, 2018).

Tais serviços foram implementados em aplicativos de mensagem instantânea, tais como WhatsApp e Telegram, e até mesmo no em sistemas operacionais, como o iOs8 para o iPhone anunciado pela Apple em setembro de 2014. Este tipo de criptografia, adotada tanto no WhatsApp como no iPhone da Apple, é conhecida como criptografia *end-to-end* (ponta a ponta), que assegura que a

[3] A *privacy by default* consiste na ideia de se estabelecerem padrões mais seguros desde a concepção do produto ou serviço, o qual deve ser arquitetado de forma a proteger as informações pessoais dos seus usuários, agregando esse padrão de segurança de forma automática. Por sua vez, a *privacy by design* consiste em um sistema de informação que garanta um ambiente seguro para a coleta, tratamento e transferência de dados, sempre informando o titular destes, capacitando o usuário ao controle de seus dados por meio de interfaces mais amigáveis (LIMA, 2020).

comunicação entre duas partes não pode ser lida por nenhum intermediário ou provedor de serviço (AMNESTY INTERNATIONAL, 2016).

Porém, enquanto esse tipo de criptografia garanta que nem mesmo o provedor da aplicação pode acessar o conteúdo da comunicação, proporcionando maior proteção e segurança aos usuários, ao mesmo tempo, fragiliza a capacidade técnica das autoridades de investigação para acessar esse conteúdo. Inclusive as próprias autoridades investigativas e jurisdicionais no Brasil demoraram para entender que estes dados protegidos pela criptografia ponta a ponta não poderiam nem sequer ser fornecidos pelos provedores da aplicação.

No ano de 2015 e 2016, o WhatsApp sofreu sucessivas suspensões de seus serviços no Brasil, em razão de ter se recusado a entregar o conteúdo de mensagens veiculadas no aplicativo em razão de não possuir capacidade técnica para o referido acesso por conta da criptografia ponta a ponta.

Esse assunto ganhou relevo com o ajuizamento da ADI nº 5527 e ADPF nº 403, atualmente em curso no Supremo Tribunal Federal (STF). Na ADI nº 5527, de relatoria da ministra Rosa Weber, questiona-se a constitucionalidade de dispositivos do Marco Civil da Internet (Lei 12.965/2014), que supostamente permitiriam a suspensão do WhatsApp conforme mencionado em reiteradas decisões judiciais que determinaram o bloqueio do aplicativo. Por sua vez, a ADPF nº 403, de relatoria do ministro Edson Fachin, foi ajuizada contra decisão judicial que teria determinado o bloqueio nacional do WhatsApp diante da recusa técnica do aplicativo em fornecer dados no âmbito de uma investigação criminal.

Em 19 de julho de 2016, o ministro Ricardo Lewandowski, ao analisar a medida cautelar na ADPF nº 403, determinou o restabelecimento imediato dos serviços de mensagens do aplicativo WhatsApp. O referido Ministro justificou que a suspensão dos serviços, além de parecer pouco razoável e desproporcional, violaria o direito à liberdade de expressão e comunicação, ao mesmo tempo em que representaria uma ameaça à estabilidade, segurança e funcionalidade da rede, o que era uma das preocupações da Lei 12.965/2014 (Marco civil da internet).

Os votos já apresentados pelos Ministros Relatores, Edson Fachin (ADPF 403) e Rosa Weber (ADI 5527), demonstram um reconhecimento abrangente da

relevância da criptografia na preservação dos direitos fundamentais. Além disso, ambos os relatores afirmam de maneira explícita a inconstitucionalidade de qualquer tentativa de impor restrições a esses sistemas de segurança, mesmo quando se trata de investigações criminais. No entanto, é relevante observar que as ações estão atualmente suspensas devido a um pedido de vista, e não é possível antever os votos dos próximos Ministros do STF.

A questão mais delicada que envolve as referidas ações de controle de constitucionalidade trata-se do uso pelos aplicativos de comunicação da criptografia ponta a ponta (SARMENTO, 2020). A audiência pública promovida pelo STF em 2017 foi fundamental para que fosse esclarecido a inviabilidade do cumprimento de decisões judiciais que decretassem a interceptação ou a quebra do sigilo das comunicações realizadas pelo WhatsApp (SARMENTO, 2020).

Em novembro de 2016 a Assembleia Geral das Organizações Unidas (AGNU) aprovou uma "resolução sobre o direito à privacidade na era digital", na qual enfatizou a relevância na ponderação e avaliação da necessidade e proporcionalidade nas práticas de vigilância, interceptação de comunicações e a coleta de dados pessoais. Isso se deve ao fato de que, quando essas atividades são realizadas de forma ilegal ou arbitrária, violam o direito à privacidade, interferem no direito à liberdade de expressão e entram em conflito com os princípios de uma sociedade democrática (*UN GENERAL ASSEMBLY*, 2016).

No âmbito nacional o art. 8º da Lei nº 12.965/2014 (Lei do Marco Civil da Internet) estabelece que a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito do acesso à internet. Somado a isso, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) prevê a necessidade de adoção de medidas de segurança e técnicas aptas a proteger os dados pessoais de acessos não autorizados, o que inclusive deve ser observado desde a fase de concepção do produto ou do serviço até a sua execução (art. 46, "caput" e §2º)[4].

[4] Lei nº 13.709/2018. Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Segundo Laura Mendes (2015) o avanço tecnológico resultou na criação de uma interdependência das pessoas em relação aos sistemas informatizados, onde o indivíduo perde a capacidade de controlar de maneira individual o fluxo e o armazenamento de seus dados pessoais. Nesta perspectiva, a criptografia além de assegurar a confidencialidade nos sistemas, redes e infraestruturas de comunicação, garante sigilo, integridade e autenticidade no conteúdo das mensagens de dados e informações (ABREU, 2017)

Para Danilo Doneda (2020) a criptografia é um elemento central de confiança da internet, pois além de garantir privacidade, propicia comunicações seguras, robustecendo as tecnologias de comunicação e informação. Portanto, observa-se que a criptografia é um mecanismo que garante o direito fundamental de privacidade, o exercício da liberdade de expressão, bem como assegura que as comunicações ocorram com respeito a confiabilidade e integridade do fluxo informacional.

Assim, a criptografia, além de ser uma ferramenta essencial para a preservação dos direitos fundamentais à privacidade, liberdade de expressão e do sigilo das comunicações (CF, art. 5º, IX, X e XII)[5], é essencial para a proteção de dados pessoais e da própria democracia. Por essa razão, qualquer política pública sobre o tema tem implicação direta sobre a proteção e o exercício de direitos humanos essências para a garantia de uma sociedade democrática.

3 REAÇÃO DAS AUTORIDADES: HACKING GOVERNAMENTAL E TECNOAUTORITARISMO

[...]
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

[5] Constituição Federal. Art. 5º [...] IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença [...] 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 [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Após a Apple adotar a criptografia em seu sistema, o ex-diretor do FBI, James Comey (2014), liderou uma campanha contra o uso da criptografia forte como padrão de segurança, argumentando que a capacidade de interceptação e acesso às comunicações estava diminuindo, o que se denominou de *going dark*.

Essa postura das autoridades americanas foi replicada em diversos países, fomentando que as autoridades de investigação dos governos passassem a exigir o acesso aos dados criptografados através da criação de *backdoors* ou de outros mecanismos similares. Além disso, diversos grupos políticos fomentarem a regulamentação da própria criptografia, de modo a inibir ou enfraquecer o seu uso nos mecanismos de fluxo informacional[6].

Com base no relatório de 2015 elaborado por David Kaye, Relator Especial do Conselho de Direitos Humanos da ONU, estabeleceu-se um consenso entre organizações da sociedade civil internacional e países europeus que apoiam o desenvolvimento de criptografia robusta. Essa postura foi reiterada por nações como Alemanha, Holanda, Irlanda, Noruega, Suécia e Eslováquia, que adotaram políticas governamentais pró-criptografia e se posicionaram a favor do uso de criptografia forte, opondo-se à implementação de qualquer forma de mecanismo excepcional (SALVADOR; GUIMARÃES, 2020; GUTHEIL et al., 2017).

O estudo conduzido para o Comitê LIBE (Comitê de Liberdades Civis, Justiça e Assuntos Internos) do Parlamento Europeu enfatiza a necessidade de reiterar perante a sociedade a posição da União Europeia contrária à criação de *backdoors* ou técnicas semelhantes, ao mesmo tempo que apoia o uso de padrões de criptografia forte. Adicionalmente, esse posicionamento recebe respaldo das forças policiais europeias, incluindo a Associação Internacional de Chefes de Polícia (IACP) e a Europol, que emitiram uma Declaração Conjunta em 2016 em colaboração com a ENISA sobre esse tema (GUTHEIL, *et al*., 2017).

[6] Tal como ocorreu na Austrália, França e Reino Unido (SALVADOR; GUIMARÃES, 2020; LIGUORI FILHO, 2020). As legislações destes países ampliaram os poderes de investigação de autoridades frente a sistemas criptográficos, obrigando as empresas de tecnologia a criar mecanismos de acesso excepcional que permitam a interceptação da comunicação de investigados. As referidas legislações são severamente criticadas pela comunidade internacional e infelizmente tem influenciado alguns projetos de lei que circulam perante o poder legislativo do Brasil (SALVADOR; GUIMARÃES, 2020).

Pesquisadores de Harvard questionaram a eficácia da metáfora "*going dark*" das autoridades norte-americanas, argumentando que a ampla adoção de criptografia e tecnologias de ocultação de dados pelos usuários não será generalizada devido à dependência das empresas dos dados do usuário, enquanto o uso crescente de sensores na Internet das Coisas pode alterar a vigilância, deixando a maioria dos metadados desprotegidos. (GASSER, *et al*., 2016). De fato, eles destacaram que o aumento do uso de sensores na Internet das Coisas pode transformar a vigilância ao capturar vídeos e áudios em tempo real, com a maioria dos metadados permanecendo sem criptografia devido à necessidade de acesso aos dados para o funcionamento dos sistemas, como rastreamento de localização de dispositivos (GASSER, et al., 2016).

Por essas razões, há uma tendência na busca de outras ferramentas alternativas à aplicação da lei sem colocar em risco os atuais sistemas de criptografia. Dentre os diversos meios alternativos de investigação para contornar a restrição causada pela criptografia, o *hacking legal* ou *hacking governamental* tem sido um dos mais sugeridos (LIGUORI FILHO, 2020) e atualmente empregados em diversos países conforme estudo realizado para o Comitê LIBE do Parlamento Europeu.

O *hacking* pode ser compreendido como exploração vulnerabilidades (falhas existentes em hardware ou software), bem como uso malware e engenharia social para obter acesso a um sistema, dispositivo ou rede, podendo ser usado para contornar a criptografia e permitir acesso a dados não criptografados no sistema alvo (AMNESTY INTERNATIONAL, 2016). Nesse contexto, 'o "hacking governamental" consiste, no contexto de investigações criminais, na utilização dessas técnicas e suas respectivas ferramentas, para acessar dados em redes e dispositivos a partir da exploração de vulnerabilidades existentes no sistema' (LIGUORI, 2022, p. 76).

Existe uma preocupação de que os governos possam usar ferramentas de *hacking* para aumentar a vigilância no futuro. Isso inclui a capacidade de ativar secretamente microfones, câmeras e tecnologia de localização baseada em GPS, bem como acessar telas, registros de entrada e saída, detalhes de login e senhas, histórico de navegação na internet e documentos e comunicações que os usuários nunca pretendiam divulgar (*PRIVACY INTERNATIONAL*, 2018).

O estudo para o Comitê LIBE do Parlamento Europeu destaca que as técnicas de *hacking* são altamente invasivas em comparação com métodos tradicionais de investigação, como escutas telefônicas e buscas domiciliares. Diferentemente dos mecanismos tradicionais, essas novas técnicas podem resultar no acesso a um extenso conjunto de dados armazenados ou em trânsito (GUTHEIL, *et al*., 2017).

Por essa razão, esse amplo poder investigativo gera preocupações sobre excesso de poder, coleta de dados sem autorização e condutas arbitrárias por parte dos governos, diante possibilidade de manipulação dos sistemas informatizados para encobrir atividades relacionadas a eventuais ilegalidades (*PRIVACY INTERNATIONAL*, 2018).

Conforme avalia André Ramiro *et al.* (2022), a exploração de vulnerabilidades em sistemas informáticos é uma prática que carrega uma dualidade, uma vez que pode ser usada tanto por agentes privados maliciosos quanto por autoridades policiais como uma ferramenta "legítima" para reunir evidências em investigações criminais. Nesse contexto, há uma tendência internacional na utilização de vácuos regulatórios para a implementação da vigilância governamental (RAMIRO, *et al*., 2022), de modo que a utilização de mecanismos de *hacking* percam a sua legitimidade.

Nessa lacuna entre o aumento do uso de ferramentas tecnológicas intrusivas pelo Estado e a ausência de regulamentação, abre-se caminho para o que é denominado como "tecnoautoritarismo". O conceito de tecnoautoritarismo pode ser empregado para compreender os procedimentos de ampliação do poder do Estado através da adoção de tecnologias de comunicação de última geração, visando a reforçar as capacidades de vigilância e controle da população, muitas vezes à custa de violações dos direitos individuais ou do aumento significativo dos riscos relacionados a direitos fundamentais (GROSS *et al*., 2021).

É fundamental destacar que o tecnoautoritarismo não está restrito a regimes políticos autoritários ou ditatórias, também sendo identificado em Estados Democráticos, onde o governo recorre a tecnologias avançadas para ampliar seu controle sobre os cidadãos (SARLET; SARLET, 2022). Esse cenário suscita

preocupações consideráveis relacionadas aos direitos humanos, em especial à preservação da privacidade e da liberdade de expressão.

As práticas de tecnoautoritarismo contribuem para minar os alicerces da democracia, estabelecendo estruturas que têm a capacidade de intensificar a vigilância, repressão e restrição do exercício de direitos fundamentais (GROSS *et al.*, 2021).

Exemplo disso pode ser extraído do escândalo do “dossiê antifascista” orquestrado em junho de 2020 pelo Ministério da Justiça, na gestão do ex-presidente Jair Bolsonaro. Por meio da sua Secretaria de Operações Integradas (Seopi), o Ministério da Justiça e Segurança Pública implementou uma operação confidencial que envolveu um grupo de 579 servidores federais e estaduais de segurança, identificados como pertencentes ao "movimento antifascismo," além de três professores universitários (VALENTE, 2020). Entre eles, havia um ex-secretário nacional de direitos humanos que atualmente atuava como relator da ONU para direitos humanos na Síria (VALENTE, 2020).

Desde julho de 2015, a partir do vazamento de documentos da empresa italiana *Hacking Team* (conhecida por desenvolver e vender softwares espiões e ferramentas de vigilância para governos), foram encontradas diversas menções a órgãos de inteligência do Brasil e autoridades de investigação, como a Agência Brasileira de Inteligência, o Centro de Inteligência do Exército, as polícias civil e militar, o Ministério da Justiça e a Procuradoria Geral da República, que sugeriam negociações e aquisições da "solução" RCS (*Remote Control System*) para um projeto piloto com duração de 3 meses (ANTONIALLI; ABREU, 2015).

O RCS é um sistema discreto, baseado em *spyware*, e desenvolvido para atacar, infectar e monitorar computadores e smartphones, sendo uma ferramenta que permite o monitoramento e controle de dados do dispositivo infectado, permitindo acesso remoto de todas as informações armazenadas no aparelho, as produzidas em tempo real, além de permitir o acionamento da câmera e do microfone para capturar imagens e sons sem qualquer conhecimento do infectado (ANTONIALLI; ABREU, 2015). De fato, é amplamente reconhecido que as autoridades italianas utilizam ferramentas de *hacking* em processos de investigações criminais, sendo que o uso de

malware é o método preferido de escolha dos órgãos de aplicação da lei italianos (GUTHEIL, *et al.*, 2017).

Em 2022, um minucioso relatório elaborado pelo IP.rec apresentou um cenário que revela a capilaridade de ferramentas de *hacking* consideravelmente ampla no Brasil. No referido estudo restou consignado a existência de 228 acordos comerciais realizados desde 2013 entre agências de investigação (federais e estaduais) e empresas privadas (RAMIRO, *et al*., 2022). Esses acordos resultaram em um aumento significativo nos gastos públicos com soluções de *hacking* governamental, que passaram de 6 milhões em 2015 para 55 milhões em 2021, atingindo um pico de 74 milhões em 2020 (RAMIRO, *et al*., 2022).

Não por outra razão, André Ramiro *et al*. (2022, p. 80), afirmam que as "técnicas de extração de dados já compõem o *modus operandi* de agências investigativas em todos o território brasileiro".

O principal desafio reside no fato de que a utilização de tecnologias para acesso remoto a dados, por meio de métodos de *hacking* governamental, ocorre sem uma regulamentação clara que delimite as ações das autoridades estatais. Isso é ampliado quando essas tecnologias são usadas como meio de troca de informações, como no caso do Programa Excel do Ministério da Justiça[7], resultando em sua disseminação indiscriminada e na perda da característica de excepcionalidade da medida.

Nesse cenário, o direito internacional dos direitos humanos assume um papel fundamental ao estabelecer proteções em constante fortalecimento para a proteção dos indivíduos. Como resultado, observa-se um aumento na pressão de órgãos internacionais por maior rigor legal e transparência nas atividades investigativas dos Estados na era da tecnologia.

[7] A esse respeito, o The Intercept Brasil detalhou alguns termos do Programa Excel, política criada no âmbito do Ministério da Justiça que propõe o seguinte arranjo: o Ministério provê às forças policiais estatais MDFTs da Cellebrite (que, em sua maioria, podem variar entre 100 ou 200 mil reais) e, como contrapartida, as polícias alimentariam uma base dados do Ministério composta pelos dados extraídos dos celulares.36 Ou seja, para além de uma finalidade investigativa pontual e demarcada por ordem judicial, dados pessoais são acumulados pela máquina pública com o fundamental auxílio das MDFTs, uma lógica que aprofunda o sistema de vigilância estatal e permite usos colaterais dos dados pessoais. (RAMIRO, *et al.*, 2023, pp. 09-10).

4 VÁCUO LEGISLATIVO E PRESSUPOSTOS CONDICIONANTES PARA EVITAR O TECNOAUTORITARISMO

Em 2008, a Corte Constitucional alemã ao analisar uma lei do Estado de *Nordrhein-Westfalen* que regulamentava e permitia acesso remoto de computadores de indivíduos suspeitos de cometer crimes, reconheceu a importância de preservar a confidencialidade e integridade dos sistemas de informação (MENKE, 2015).

No julgamento o Tribunal alemão entendeu que em situações excepcionais, tal como para fins de persecução criminal, a infiltração nos sistemas informáticos poderia ocorrer, desde que observados os seguintes requisitos: i) edição de lei específica; ii) o texto legal deve estar de acordo com a proporcionalidade em sua tríplice vertente (adequação, necessidade e proporcionalidade em sentido estrito); iii) mediante autorização judicial; iv) o monitoramento deve ser utilizado em *ultima ratio*, em caso de existência de perigo concreto (a ser analisado em cada caso concreto) e que coloque em risco bem jurídico de alta relevância (tais como vida, liberdade da pessoa, bens da coletividade e a própria existência do Estado), e v) que seja possível determinar as pessoas envolvidas, para evitar a violação de direitos de indivíduos inocentes (MENKE, 2015).

No mesmo sentido, o estudo realizado para o Comitê LIBE do Parlamento Europeu revela que da análise dos sistemas legais dos seis estados-membros da EU[8] há a estruturação jurídica de um conjunto de pressupostos condicionantes ao deferimento de medidas de *hacking* legal (denominadas *ex-ante considerations*), bem como de mecanismos posteriores à aplicação da medida investigativa (denominadas *ex-post considerations*), visando a garantir que a utilização das técnicas de *hacking* seja proporcional e necessária (GUTHEIL, *et al.,* 2017).

As considerações *ex-ante* (pressupostos condicionantes ao deferimento da medida) podem ser sintetizadas como: i) necessidade de autorização judicial como regra, salvo circunstâncias excepcionais em que poderia haver uma decisão judicial posterior; ii) limitação do tempo de duração da medida (que nos países da EU tem

[8] França, Alemanha, Itália, Países Baixos, Polônia e Reino Unido (na época do relatório ainda era membro da EU).

variado entre 1 a 6 meses, com possíveis prorrogações), e iii) limitação do uso das ferramentas de *hacking* com base na gravidade dos crimes e/ou na dosagem da pena em abstrato do crime (GUTHEIL, *et al.,* 2017).

Por sua vez, nas considerações *ex-post* (mecanismos posteriores) constata-se que a maioria dos países objeto de estudo prevê: i) notificação dos investigados sobre as práticas de *hacking* (após a implementação da medida), e ii) métodos de controle/fiscalização, as vezes por meio de relatórios nos quais são registradas as atividades *hacking* ou então mediante a existência de órgãos externos de revisão e supervisão (GUTHEIL, *et al*., 2017).

Além desses requisitos básicos, na análise das legislações e projetos de lei, da Alemanha, Itália e Holanda, é possível constatar de maneira uniforme a exigência para que os pedidos de *hacking* legal delimitem quem seriam os investigados, bem como indiquem detalhes da medida que será implementada e do período da ação (GUTHEIL, *et al*., 2017). Sem dúvida esses requisitos permitem maior controle pela autoridade jurisdicional, evitando assim, eventuais abusos pelas autoridades investigativas. Ademais, no novo projeto de lei italiano há expressa previsão que toda a operação deve ser devidamente registrada e documentada, de modo que os resultados da operação possam ser efetivamente contestados pelo réu (GUTHEIL, *et al*., 2017).

Por sua vez, a partir de uma análise do posicionamento do Sistema Interamericano de Direitos Humanos (SIDH) em relação aos riscos de controle e vigilância relacionados a potenciais violações de Direitos Humanos, é possível aferir que a Corte Interamericana de Direitos Humanos recentemente emitiu uma declaração explícita em um caso que envolveu a violação dos direitos à privacidade e à liberdade de expressão de indivíduos por meio de vigilância ilegal.

A Comissão Interamericana de Direitos Humanos (CIDH) levou o caso dos *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CCAJAR) vs. Colômbia* à Corte Interamericana de Direitos Humanos em 08 de julho de 2020 (OEA, 2020). O caso envolve atos de violência, intimidação, assédio e

ameaças contra os membros da CAJAR, que têm defendido os direitos humanos na Colômbia desde a década de 1990[9].

A Comissão destacou que os membros da CAJAR foram alvo de várias ameaças e perseguições, em parte devido a ações de inteligência arbitrárias realizadas pelo Estado e pronunciamentos estigmatizantes de altos funcionários do Governo (CIDH, 2019). A inteligência estratégica, conduzida pelo extinto Departamento de Segurança Administrativa (DAS) do Governo da Colômbia, realizou o monitoramento das atividades da CAJAR, interceptação de comunicações e a criação de arquivos pessoais sem justificação legal ou controle judicial adequado (CIDH, 2019).

Após essas constatações, uma das principais recomendações feitas pela CIDH ao Estado da Colômbia consistiu que este se abstenha de realizar atividades de inteligência que violem os direitos à privacidade e à liberdade de expressão, garantindo que qualquer interferência nesses direitos seja legal, com finalidade legítima, necessária e proporcional (CIDH, 2019).

Ademais, A Comissão recomendou ao Estado da Colômbia a regulamentação precisa da matéria, de modo a evitar poderes excessivamente amplos, exigindo-se a prévia autorização judicial e observância dos princípios da excepcionalidade e da transparência (CIDH, 2019). Além disso, as pessoas afetadas devem ter recursos eficazes para acessar, corrigir, atualizar ou eliminar seus dados pessoais nos arquivos de inteligência (CIDH, 2019).

Assim, de acordo com a relatoria do CIDH no caso *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CCAJAR) vs. Colômbia,* a questão dos trabalhos de vigilância/inteligência do Estado foi submetido ao teste de três partes, no qual qualquer restrição aos direitos de liberdade de expressão e acesso à informação, de acordo com a Convenção Americana, deve atender aos princípios de legalidade, legitimidade, necessidade e proporcionalidade.

Este caso oferece a possibilidade de responsabilizar ações e métodos de inteligência usados pelos Estados de maneira ilegal e arbitrária contra organizações

[9] Para maiores informações: https://confidencialnoticias.com/colombia/lo-mas-confidencial/corte-idh-realiza-audiencia-publica-del-caso-cajar-vs-colombia/2022/05/12/. Acesso em: 22 ago. 2023.

sociais e defensores dos direitos humanos, incluindo o Brasil. Isso se deve à obrigação dos Estados-membros de observar a jurisprudência do Sistema Interamericano de Proteção dos Direitos Humanos (SIDH), conforme estabelecido nos artigos 1º, 2º e 62 da Convenção Americana.

Assim, pode-se afirmar que a orientação firmada pela CIDH no caso *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CCAJAR) vs. Colômbia* possui elementos condicionantes ao tecnoautoritarismo similares ao julgado da Corte alemão de 2008.

Um requisito importante a ser destacado é que, embora seja fundamental obter autorização judicial prévia para avaliar a necessidade e proporcionalidade na implementação de medidas de *hacking* governamental, devido à sua natureza altamente invasiva, essa autorização judicial só será válida se houver legislação específica que regule o tema.

Isso se justifica porque o *hacking* introduz ao sistema jurídico brasileiro novas dimensões de risco que transcendem as legislações tradicionalmente usadas como instrumentos de obtenção de prova na seara processual penal, tal como a intercepção telefônica, a infiltração ou mandados genéricos de busca e apreensão. Esses mecanismos tradicionais não atendem as métricas de risco oriundas de um *hacking* governamental (RAMIRO, *et al*., 2022).

Corroborando esse raciocínio, Laura Mendes (2015) afirma que para essa nova modalidade de investigação, seria requerida não apenas uma ordem judicial específica que autorizasse tal forma de monitoramento, mas também uma legislação específica, uma vez que as Leis 9.296/96 e 12.850/13 não abordam o uso de *softwares* espiões para monitoramento online e acesso remoto a informações em sistemas informáticos pessoais.

Por essas razões, RAMIRO *et al*. (2022), DUTRA *et al.* (2023) e LIGUORI FILHO (2020) sustentam que, embora haja margem para a adoção de *hacking* governamental em investigações legítimas, é fundamental garantir a proteção dos direitos fundamentais e a observância do devido processo legal. Isso se concretizaria por meio do respeito a princípios essenciais, como legalidade, proporcionalidade,

necessidade, transparência e prestação de contas (RAMIRO *et al*., 2022; DUTRA *et al.,* 2022; LIGUORI FILHO, 2020).

Por último, as medidas posteriores ao *hacking* legal também demonstram extrema relevância, não apenas devido à novidade desses mecanismos, cujos efeitos sociais ainda são desconhecidos, mas também para garantir que as autoridades investigativas não atuem com abuso de poder ou coletem provas de maneira ilegal.

Por isso, defende-se a integridade na coleta de informações, com autoridades mantendo um registro detalhado das atividades de *hacking* e possibilitando a verificação por auditorias independentes. Isso inclui a divulgação dos métodos utilizados, a extensão e a duração da medida, permitindo que a pessoa investigada compreenda os dados obtidos e identifique quaisquer modificações que possam afetar a integridade das informações (PRIVACY INTERNATIONAL, 2018). Esse processo visa justamente assegurar uma transparência adequada e um efetivo contraditório e ampla defesa das provas produzidas.

5 CONCLUSÃO

O presente trabalho buscou demonstrar a importância da criptografia ponta a ponta para a tutela dos direitos humanos, bem como a necessidade do estabelecimento de condicionantes para se evitar o tecnoautoritarismo na implementação de *hacking* governamental.

Na primeira parte do artigo foi abordado a expansão do uso de criptografia nos meios de comunicação informáticos, impulsionada pelas revelações de Edward Snowden sobre a vigilância em massa. Internacionalmente, a ONU e a União Europeia reconhecem a importância da criptografia para a privacidade, enquanto no Brasil, o Marco Civil da Internet e a Lei Geral de Proteção de Dados respaldam sua utilização para proteger direitos fundamentais em uma sociedade democrática.

Assim, pode-se afirmar que a criptografia *by default* se tornou crucial para proteger os direitos fundamentais em um ambiente digital, mesmo diante de desafios legais e de investigação. Ela é reconhecida internacionalmente como essencial para

a privacidade e, no Brasil, é respaldada por legislação que a posiciona como uma ferramenta de proteção dos direitos humanos e da democracia.

No segundo tópico verificou-se que o uso generalizado da criptografia forte como padrão de segurança nas comunicações gerou debates globais, com os EUA inicialmente preocupados com a "escuridão" que ela poderia criar, enquanto a comunidade internacional e diversos países europeus, como Alemanha, Holanda, Irlanda, Noruega, Suécia e Eslováquia, a apoiam, destacando sua importância para a privacidade e segurança.

Ademais, pesquisadores alertam para o conceito de "tecnoautoritarismo", destacando como os avanços tecnológicos podem ser usados para ampliar o poder estatal e ameaçar os direitos humanos, incluindo a privacidade e a liberdade de expressão. A utilização de técnicas de *hacking* governamental como alternativa para contornar a criptografia gera preocupações sobre abuso de poder, coleta de dados sem autorização e condutas arbitrárias por parte dos governos. Isso levanta a necessidade de uma regulamentação clara e transparente dessas práticas.

Por último, abordou-se os mecanismos para condicionar o uso de *hacking* governamental partir da análise da decisão da Corte Constitucional alemã de 2008 e da recomendação feita pela CIDH no caso *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CCAJAR) vs. Colômbia*, que revelam a importância de estabelecer salvaguardas rigorosas para proteger os direitos humanos dos indivíduos em um cenário de crescente uso de técnicas de investigação de inteligência.

Nesse ponto, tanto a Corte alemã quanto a CIDH enfatizam a necessidade de observar princípios fundamentais, como legalidade, proporcionalidade, necessidade e transparência ao autorizar e implementar medidas de *hacking* governamental. A autorização judicial prévia é vista como um requisito essencial, garantindo que cada caso seja analisado individualmente, levando em consideração a gravidade do crime e a relevância da medida.

Além disso, é crucial que exista legislação específica que regule o uso dessas técnicas, uma vez que o *hacking* introduz novas dimensões de risco que não estão contempladas nas leis tradicionais de obtenção de provas. A transparência e a

prestação de contas são enfatizadas como meios de garantir a integridade na coleta de informações, com a necessidade de manter registros detalhados das atividades de *hacking* e permitir auditorias independentes.

Com efeito, essas diretrizes buscam equilibrar a necessidade de investigação criminal com a proteção dos direitos humanos ao implementar medidas de *hacking* governamental em conformidade com os princípios do Estado Democrático de Direito. A introdução do *hacking* governamental no Brasil requer uma legislação específica, precedida por estudos aprofundados e debates públicos transparentes, alinhados com pesquisas da União Europeia e recomendações da CIDH para promover e proteger os direitos humanos.

REFERÊNCIAS

ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, 2017, p. 25-42.

AMNESTY INTERNATIONAL. ***Encryption:*** *a matter of human rights*, mar. 2016. Disponível em: https://www.amnesty.org/en/documents/pol40/3682/2016/en/. Acesso em 14 jan. 2023.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. Vigilância das comunicações pelo estado brasileiro: e a proteção a direitos fundamentais. **INTERNETLAB**, 2015. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2015/11/VigilanciaEstado_Diagram_vprova.pdf. Acesso em: 19 jan. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 jan. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoas (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 17 jan. 2023.

BRASIL, Supremo Tribunal Federal. **Medida Cautelar na ADPF nº 403.** Relator Ministro Edson Fachin. Disponível em:

http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403MC.pdf. Acesso em: 17 jan. 2023.

CIDH. Informe Nº. 57/19. Caso 12.380. *Fondo. Miembros de la Corporación Colectivo de Abogados José Alvear Restrepo. Colombia*. 4 de mayo de 2019. Disponível em: https://www.oas.org/pt/cidh/decisiones/demandas2.asp?Year=2020. Acesso em: 22 ago. 2023.

COMEY, James B. *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* ***Federal Bureau of Intestigation (FBI),*** 16 out. 2014. Disponível em: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acesso em: 16 jan. 2023.

DONEDA, Danilo. Criptografia, segurança e confiança em tempos de pandemia: a criptografia é um elemento que praticamente transcreve vários dos valores fundamentais de nossa ordem jurídica. **JOTA**, 06 de mai. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criptografia-seguranca-e-confianca-em-tempos-de-pandemia-06052020. Acesso em: 21 jan. 2023.

DUTRA, Luiza Correa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Hacking governamental:** uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: https://bit.ly/3YdVcIL. Acesso em: 14 ago. 2023.

GASSER, Urs, *et al. Don't panic: making progress on the "going dark" debate*. February 1, 2016. **The Berkman Center for Internet & Society at Harvard University**. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf. Acesso em: 25 jul. 2023.

GROSS, Clarissa; ZANATTA, Rafael; Nuñez; LEITÃO, Clara; SANTOS, Bruna; VICENTE, João Paulo. Retrospectiva Tecnoautoritarismo. **LAUT**, 2021. Disponível em: https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/. Acesso em: 22 ago. 2023.

GUTHEIL, Mirja; LIGER, Quentin; HEETMAN, Aurélie; EAGER, James; CRAWFORD, Max. *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices.* ***EUROPEAN PARLIAMENT'S***, mar. 2017. Disponível em: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)583137. Acesso em: 14 jan. 2023.

LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. *Crypto Wars* e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. **Revista da Faculdade de Direito – UFPR** / Curitiba, Vol. 63, nº 3, set/dez. 2018, p. 135-161. Disponível em: https://revistas.ufpr.br/direito/article/view/59422. Acesso em: 19 jan. 2023.

LIGUORI FILHO, Carlos Augusto. *Exploring lawful hacking as a possible answer to the 'Going Dark' debate.* ***Michigan Telecommunications and Technology Law Review***, Vol. 26, n. 2, 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606601. Acesso em: 15 jan. 2023.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina Brasil, 2020.

MENDES, Laura Schertel. Uso de softwares espiões pela polícia: prática legal? **JOTA,** 04 jun. 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015. Acesso em: 18 jan. 2023.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia de confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In:* MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, Inovação e Tecnologia. Vol. 1**. São Paulo, Saraiva, 2015.

OEA. **A CIDH apresenta caso sobre a Colômbia perante a Corte Interamericana**. Comunicado de imprensa, 28 de dezembro de 2020. Disponível em: https://www.oas.org/pt/cidh/prensa/notas/2020/312.asp. Acesso em: 20 ago. 2023.

PFEFFERKORN, Riana. O debate estadunidense sobre vigilância e criptografia. *In:* ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. **Direitos fundamentais e processo penal na era digital:** doutrina e prática em debate. Vol. 1. São Paulo, InternetLab, 2018.

PRIVACY INTERNATIONAL. ***Government Hacking and Surveillance: 10 Necessary Safeguards***, 2018. Disponível em: https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf. Acesso em: 14 jan. 2023.

RAMIRO, André (Coord.); AMARAL, Pedro; CANTO, Mariana; PEREIRA, Marcos César. **Mercadores da insegurança: conjuntura e riscos do hacking**

governamental no Brasil [livro eletrônico]. Recife: IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife, 2022. Disponível em: https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/. Acesso em 16 ago. 2023.

SALVADOR, João Pedro Favaretto; GUIMARÃES, Tatiane. **Regulação da criptografia ao redor do mundo: um cardápio de possibilidades.** CEPI – FGV DIREITO SP, 03 de nov. 2020. Disponível em: https://medium.com/o-centro-de-ensino-e-pesquisa-em-inova%C3%A7%C3%A3o-est%C3%A1/regula%C3%A7%C3%A3o-da-criptografia-ao-redor-do-mundo-um-card%C3%A1pio-de-possibilidades-76fc6343a6be. Acesso em 16 jan. 2023.

SARLET, Ingo Wolfgang; SARLET, Gabrielle Bezerra Sales. Tecno-autoritarismo, tecno-fascismo societal, democracia e proteção de dados. **Conjur**, 13 de novembro de 2022. Disponível em: https://www.conjur.com.br/2022-nov-13/direitos-fundamentais-tecno-autoritarismo-tecno-fascismo-societal-protecao-dados. Acesso em 11 ago. 2023.

SARMENTO, Daniel. Aplicativos, criptografia e direitos fundamentais em tempos de erosão democrática. **JOTA**, 14 mai 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/aplicativos-criptografia-e-direitos-fundamentais-em-tempos-de-erosao-democratica-14052020. Acesso em: 15 jan. 2021.

SCHULZ, Wolfgang; HOBOKEN, Joris van. **Direitos humanos e criptografia**. Tradução brasileira Por Instituto de Tecnologia e Sociedade do Rio (ITS Rio). França: UNESCO, 2016. Disponível em: https://itsrio.org/wp-content/uploads/2018/10/direitos-humanos-e-criptografia-1.pdf. Aceso em: 14 jan. 2021.

UN GENERAL ASSEMBLY. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, David Kaye, **A/HRC/29/32**, de 22 mai 2015. Disponível em: https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx. Acesso em: 19 jan. 2023.

VALENTE, Rubens. Ação sigilosa do governo mira professores e policiais antifascistas. **Veja**, 24/07/2020. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/07/24/ministerio-justica-governo-bolsonaro-antifascistas.htm. Acesso em: 30 ago. 2023.